КОНКРЕТНАЯ ТЕОРИЯ ГРУПП
I. ОСНОВНЫЕ ПОНЯТИЯ

Николай Вавилов

За пределами пассивного наслаждения мы открываем музыку, заставляющую нас активно участвовать в операциях ума, который *упорядочивает, оживляет и творит*. Искусство, собственно говоря, — это способ создания произведений с помощью некоторых методов, либо полученных в результате обучения, либо выдуманных. Эти методы являются *строгими и определенными путями*, обеспечивающими правильность наших операций. Если взять в этой области в качестве гида лишь разум, он приведет нас прямо ко лжи, так как разум в данном случае не освящен инстинктом. Инстинкт же непогрешим. Если он нас обманывает, то это уже не инстинкт. Во всяком случае, в таких вещах живая иллюзия гораздо ценнее, чем мертвая реальность.

Игорь Стравинский. [1]

По мере развития науки нам хочется получить нечто большее, чем просто формулу. Сначала мы наблюдаем явления, затем с помощью измерений получаем числа и, наконец, находим закон, связывающий эти числа. Но истинное величие науки состоит в том, что мы можем найти такой способ рассуждения, при котором закон становится очевидным.

Ричард Фейнман. [2]

То, что наблюдатель, куда бы он ни шел, переносит с собой центр проходимой им местности, — это довольно банальное и, можно сказать, независимое от него явление. Но что происходит с прогуливающимся человеком, если он случайно попадает в естественно выгодную точку (пересечение дорог или долин), откуда не только взгляды, но и сами вещи расходятся в разные стороны? Тогда субъективная точка зрения совпадает с объективным расположением вещей, и восприятие обретает всю свою полноту. Местность расшифровывается и озаряется. Человек видит.

Пьер Тейяр де Шарден. [3]

Одни вещи хороши в каких-то определенных целях, другие — сами по себе, а третьи — и сами по себе, и для чего-то еще. Природа хитроумно устроила так, что большинство полезных вещей вызывают у нас субъективное чувство приятности. И это касается не только питания и размножения, но и познания. Открытие в области фундаментальных исследований, например, доставляет радость вне зависимости от его возможного практического применения. Но любое приобретенное таким образом знание рано или поздно становится полезным тем, что увеличивает нашу власть над Природой.

Ганс Селье. [4]

Приобретение человеком знаний включает в себя три науки. Первая — это наука обычного знания, вторая — наука необычных духовных состояний, часто

называемых экстазом, и, наконец, третья и наиболее важная наука — наука истинной реальности: наука, занимающаяся изучением того, что неизмеримо выше предметов изучения первых двух наук.

Только реальное внутреннее знание составляет знание науки истинной реальности. Первые же две науки лишь отражают, каждая по-своему, третью науку. Они почти бесполезны без нее.

Представим себе кучера. Он сидит на козлах экипажа и управляет лошадью, которая тянет за собой экипаж. Экипаж — это интеллект, высшая форма, в пределах которой мы находимся, когда сознаем свое существование и решаем, что нам делать. Экипаж дает возможность лошади и ездоку действовать. Это то, что мы называем **ташкил**, внешняя оболочка или формулировка. Лошадь, являющаяся движущей силой, символизирует энергию, называемую иногда **эмоциональным состоянием**, а иногда как-нибудь по-другому. Она необходима, чтобы привести в движение экипаж. Человек, в нашей схеме, есть тот, кто воспринимает наилучшим образом цель и возможности ситуации и направляет экипаж в заданном направлении.

Каждый из этих трех элементов, взятый в отдельности, способен выполнять свои функции, причем достаточно правильно. Но общая функция, которую мы называем движением экипажа к цели, не может осуществляться до тех пор, пока действия трех элементов не будут согласованы *правильным образом*[♮].

Идрис Шах. *Сказки дервишей*

Пишущий стихотворение, однако, пишет его не потому, что он рассчитывает на посмертную славу, хотя он часто и надеется, что стихотворение его переживет, пусть не надолго. Пишущий стихотворение пишет его потому, что язык ему подсказывает или просто диктует следующую строчку. Начиная стихотворение, поэт, как правило, не знает, чем оно кончится, и порой оказывается очень удивлен тем, что получилось, ибо часто получается лучше, чем он предполагал, часто мысль его заходит дальше, чем он рассчитывал. Это и есть тот момент, когда будущее языка вмешивается в его настоящее. Существуют, как мы знаем, три метода познания: аналитический, интуитивный и метод, которым пользовались библейские пророки — посредством откровения. Отличие поэзии от прочих форм литературы в том, что она пользуется сразу всеми тремя (тяготея преимущественно ко второму и третьему), ибо все три даны в языке; и порой с помощью одного слова, одной рифмы пишущему стихотворение удается оказаться там, где до него никто не бывал, — и дальше, может быть, чем он сам бы желал. Пишущий стихотворение пишет его прежде всего потому, что стихотворение — колоссальный ускоритель сознания, мышления, мироощущения. Испытав это ускорение единожды, человек уже не в состоянии отказаться от повторения этого опыта.

Иосиф Бродский

[♮]Идрис Шах дает следующий комментарий: “этот открывок записан в дервишском манускрипте на персидском языке. Различные варианты его найдены в таких географически удаленных друг от друга школах, как дамасская и делийская”.

Оглавление

> ... написать задачник, развивающий попутно с навыками счета, моральное чувство и чувство исторической перспективы.
>
> Венедикт Ерофеев. *Из записных книжек*

Глава 4. Гомоморфизмы групп

Раздел II. Действия групп

Глава 5. Симметрическая группа

Глава 6. Действия групп

Hors-d'oeuvres

Аппендикс 1: Set[']s cradle

Содержание следующей части II: Основные конструкции

Содержание дальнейших частей:
Теория конкретных групп

ИНТРОДУКЦИЯ

Творящий Благо сказал Чжуан-цзы:
— Ты говоришь о бесполезном.
— С тем, кто познал бесполезное, можно говорить и о полезном, — ответил Чжуан-цзы. — Ведь земля и велика, и широка, а человек ею пользуется [лишь] в размере своей стопы. А полезна ли еще человеку земля, когда рядом с его стопою роют [ему] могилу вплоть до Желтых источников?
— Бесполезна, — ответил Творящий Благо.
— В таком случае, — сказал Чжуан-цзы, — становится ясной и польза бесполезного.

Чжуан-цзы

При рассмотрении любых важных предметов нет ничего более существенного, чем выяснение основополагающих идей.

Жозеф де Местр

Nothing that is worth knowing can be taught.

Oscar Wilde

Было начало второго, когда я вернулся к себе. На столе в кабинете в пятне света от лампы мирно лежал раскрытый на странице `Опасности поворота` Додерляйн. С час еще, глотая простывший чай, я сидел над ним, перелистывая страницы. И тут произошла интересная вещь: все прежние темные места сделались совершенно понятными, словно налились светом, и здесь, при свете лампы, ночью, в глуши, я понял, что значит настоящее знание.
“Большой опыт можно приобрести в деревне, — думал я, засыпая, — но только нужно читать, читать, побольше . . . читать . . . ”

Михаил Булгаков. *Крещение поворотом*

Важнейшее место в буддийской эпистемологии занимает видение, поскольку видение — основа знания. Знание невозможно без видения; все знание берет свое начало в видении. Таким образом, в учении Будды знание и видение тесно связаны. Поэтому буддийская философия категорически предписывает видеть реальность такой, какова она есть. Созерцание есть переживание просветления.

Дайсэцу Судзуки

Не ищите способ употребления, ищите смысл!

Людвиг Виттгенштейн (slightly updated)

Ведь в человеке не одна только физическая сторона; в нем и духовная сторона есть, и есть — больше того — есть сторона мистическая, сверхдуховная сторона.

Венедикт Ерофеев. *Москва—Петушки*

Математика большого стиля сочетает высочайшую степень эксплицитности с высочайшей степенью суггестивности. Иными словами, она апеллирует не только к рассудку, но и к биологии (зрение, моторика, пространственное чувство, чувство ритма), к эстетическому и религиозному чувству, к духовной и сверхдуховной стороне человека. В работе профессионального математика логика является не только не единственным — как полагают доморощенные мудрецы — но и далеко не главным аспектом. В действительности, она занимает чисто служебное положение по отношению к наблюдательности, **акумену***, воображению, фантазии, движению, эстетике, прагматике, интуиции, остроумию — и, в первую очередь, по отношению к откровению и пониманию, т. е. прямому контакту с миром идей, данному в форме *непосредственного* созерцания истины.

Самым важными сторонами математики являются ее очарование и увлекательность. Для профессионала это очевидно без дальнейших объяснений, но любой учебный текст, который построен без учета этого основополагающего обстоятельства, в мирное время вреден, а в военное — опасен. Тот текст, который Вы видите перед собой, представляет собой фрагмент систематического учебника алгебры для начинающих, написанного с изложенных выше позиций. В отличие от френологических учебников, он обращен не к логической шишке где-то в левом полушарии, а к сознанию, подсознанию и гиперсознанию ученика в их целостности. Этот текст скомпонирован по тем же законам, что *Гептамерон*, *Гаргантюа и Пантагрюэль*, *Тристрам Шенди*, *Жак-фаталист*, *Кот Мурр*, *Винни-Пух*, *Властелин колец*, *Звездные войны*, *Индиана Джонс* и его следует оценивать по тем же критериям.

---

*Акумен — термин Невского диалекта, означающий остроту и/или силу ума, **перспикацию** или проницательность. Если противное не оговорено явно, набранные кириллическим шрифтом \tt **вокабулы** относятся к Невскому диалекту.

§ 1 ♢. Фактический план: контент

> ... in unserem Jahrhundert treten Substitution und Substitutionsgruppe, Transformation und Transformationsgruppe, Operation und Operationsgruppe ... immer deutlicher als *die wichtigsten* Begriffe der Mathematik hervor*.
>
> Sophus Lie

> The theory of groups is a branch of Mathematics in which one does something to something and then compares the result with the result of doing the same thing to something else, or something else to the same thing.
>
> James Newman

> We may as well cut out the group theory. That is a subject that will never be of any use.
>
> James Jeans

Настоящая книга представляет собой систематическое введение в общую теорию групп, начиная с первых определений. В ней излагается — с большим запасом — весь материал, который включается в общие курсы алгебры, и, сверх того, трактуются некоторые темы, которые обычно затрагиваются только в специальных курсах по теории групп. Кроме детальной отработки на многочисленных примерах основных понятий теории групп (гомоморфизмы, подгруппы, смежные классы, нормальные подгруппы, фактор-группы, порождение, сопряженность и т. д.), мы подробно обсуждаем действия групп, основные конструкции над группами, задание групп образующими и соотношениями и основы теории конечных групп. По оглавлению читатель может более подробно ознакомиться с включенными темами. Выбор материала диктуется тем, что по моему мнению должен знать о теории групп любой математик, и вообще любой специалист, которому приходится *серьезно* использовать теорию групп в своей работе. Название книги должно подчеркнуть то обстоятельство, что общая теория групп — `allgemeine Gruppentheorie`, теория групп *для всех* — не только не совпадает с абстрактной теорией групп, но и находится в прямой оппозиции к ней.

---

*В нашем столетии понятия перестановки и группы перестановок, преобразования и группы преобразований, оператора и группы операторов ... все отчетливее выступают в качестве *важнейших* понятий всей Математики.

В этом отношении книга **уникальна*** в русской учебной литературе. Дело в том, что *все*♮ остальные *систематические* учебники теории групп на русском языке написаны ЛИБО специалистами по *абстрактной* теории групп — и рассчитаны на расширенное воспроизводство специалистов по теории групп настолько *абстрактной*, что она не может иметь никаких приложений нигде, включая саму теорию групп!!! — ЛИБО физиками для физиков. Книги Куроша [**118**] и Каргаполова—Мерзлякова [**97**] — а других не было — рассказывают *не о том, не то* и *не так*. Не о том, что реально понадобится *той*, кто учит теорию групп, чтобы использовать ее в своей работе, не то, что *ей* встретится, и не так, как это было *ей* интересно. Дело в том, что ей понадобятся конкретные группы — в 9 случаях из 10 — в 99 случаях из 100 — в 999 случаях из 1000 — группы симметрий (симметрические группы, кристаллографические группы, группы Вейля), группы типа Ли (классические группы, исключительные группы Шевалле, группы Ли, алгебраические группы, конечные простые группы) или связанные с ними группы, такие как группы кос, группы Стейнберга и т. д. А как раз о конкретных группах имеющиеся абстрактные учебники не говорят *ничего*. С другой стороны, учебники для физиков обсуждают конкретные группы — и в этом смысле дают гораздо более адекватное представление о теории групп!!! — но делают это в том духе, теми средствами и на таком языке, что были приняты у математиков лет 70 назад.

В этом тексте я пытаюсь рассказать о конкретных группах и ТО, ЧТО и ТАК, КАК это принято у математиков *сегодня*. Разумеется, чтобы говорить о конкретных группах, нужно вначале овладеть некоторым минимумом общих понятий и простейших фактов. Именно этим объясняется двусмысленность в названии: КНИГА II, КОНКРЕТНАЯ ТЕОРИЯ ГРУПП по-русски значит не совсем то же самое, что КНИГА IIBIS, ТЕОРИЯ КОНКРЕТНЫХ ГРУПП. Несколько первых читателей предлагали назвать Книгу IIB еще более *конкретно*, скажем, ЧИСТО КОНКРЕТНАЯ ТЕОРИЯ ГРУПП. Многие указали на железобетонные парагоны [**220**], [5]. Однако настоящее объяснение названия гораздо проще. Внутренний текст этой книги существует в четырех синхронных версиях, одна из которых английская. А по-английски, как обсужда-

*Разумеется, в **нормативном** Великорусском языке автор не может сказать ничего такого о собственной книге. Но в Невском диалекте вокабула **уникальна** лишена эмоциональной окраски и значит ровно то, что она значит, а именно, `unique`.

♮Это обычное полемическое преувеличение в духе Арнольда, на русском имеются два превосходных учебника, Шмидта [**220**] и Холла [**207**], первый из которых написан 90 лет назад, а второй — 60 лет назад.

ется в книге I,

`Concrete (group theory)` $\neq$ `(Concrete group) theory.`

Дойдя до середины оглавления, англофон снова посмотрит на название CONCRETE GROUP THEORY и переставит в нем скобки. В итальянской версии то же название звучит так: TEORIA DI GRUPPI IN CONCRETO (**Настоящая** теория групп) — `as opposed to` TEORIA DI GRUPPI CONCRETI. Таким образом, название этой книги, как, собственно, и большая часть самой теории групп, представляет собой НЕПЕРЕВОДИМУЮ ИГРУ КЛЮЧЕВЫХ СЛОВ. Из всех непереводимых слов настоящей книги самое ключевое — MORE (= `more`). Больше идей, больше понятий, больше `субстанции`, больше `конкрета`*, больше примеров, больше конструкций, больше методов, больше трюков, больше вычислений, больше фактов, больше деталей, больше объяснений, больше доказательств, больше истории, **больше жизни** — ES IST NICHT RICHTIG ZU SAGEN, DASS DIE CHEVALLEY-GRUPPEN SIND DAS WICHTIGSTE IM LEBEN, WEIL DIE CHEVALLEY-GRUPPEN SIND DAS LEBEN SELBST.

§ 2 ♢. Мистический план: WAS SIND UND WAS SOLLEN DIE GRUPPEN

> Die Begriffe Invariante und continuierliche Gruppe sind so alt wie die Mathematik selbst*.
>
> Sophus Lie

> Lange bevor man sich mit Permutationen beschäftigte, wurden mathematische Figuren konstruiert, die auf das engste mit Gruppentheorie zusammenhängen und nur mit gruppentheoretischen Begriffen erfaßt werden können, nämlich die regulären Muster, welche durch Bewegungen und Spiegelungen mit sich selbst zur Deckung gebracht werden können. Insbesondere bestand die von Griechen viel bewunderte ägyptische Mathematik zweifellos in der Auffindung solcher Figuren. In der arabischen und persischen Kunst erlebte die ägyptische Ornamentik einen neuen gewaltigen Aufschwung und schuf Gebilde von unerhörter Vollendung und mathematischer Tiefe. In der

*Тот, кто читал *Das Parfüm* Зюсскинда , знает, что `конкретом` называется `эссенция`, используемый в парфюмерии экстракт эфирных масел. Я думаю, это тот нюанс в названии книги `Concrete mathematics`, который ускользнул от большинства комментаторов. `Concrete mathematics` значит еще `Essential mathematics`.

*Понятия инварианта и непрерывной группы такие же старинные, как сама Математика.

gotischen Architektur trifft man sogar komplizierte Raumgruppen*.

Andreas Speiser. **[347]**

В настоящей книге мы начинаем изучение первой из фундаментальных классических структур алгебры — групп. Формально определение группы чрезвычайно незатейливо: это просто множество с одной ассоциативной бинарной операцией, для которой существует всюду определенная обратная операция. Однако эта простота обманчива. Уже на уровне конечных групп за последние два века возникли красивейшие и глубочайшие математические теории, потребовавшие для своего создания десятилетий вдохновенного изобретательного труда сотен блестящих математиков. Все это время развитие теории групп вдохновлялось и инспирировалось п(р)оявлением понятия группы и групповых идей в **сотнях** самых различных математических и экстраматематических контекстов. В целом важность понятия группы для математики сопоставима только с важностью таких понятий как категория, множество, отображение, кольцо, модуль, топологическое пространство, многообразие, мера, ...

Официально теория групп возникла в начале XIX века из трех основных источников:

- теории чисел,
- теории алгебраических уравнений,
- геометрии.

Эта получившая широкое распространение в советской литературе точка зрения пропагандировалась Вуссингом: "Почти всегда утверждается, или по крайней мере прямо подразумевается, что абстрактное понятие группы возникло в конце XIX века из понятия группы подстановок, которое в свою очередь обязано своим возникновением теории алгебраических уравнений. По мнению автора, при изучении математических источников выясняется, что абстрактная теория

*Задолго до того, как люди начали заниматься перестановками, они конструировали математические фигуры, которые теснейшим образом связаны с теорией групп и которые можно выразить *только* в теоретико-групповых терминах, а именно, регулярные орнаменты, которые переводятся в себя движениями и отражениями. В частности, египетская математика, которой столь восхищались греки, несомненно состояла именно в поиске таких фигур. Египетская орнаментика пережила новый мощный взлет в арабском и персидском искусстве, где она создала образцы *неслыханного* совершенства и математической глубины. В готической архитектуре встречаются даже сложные пространственные группы.

групп имеет исторически три корня. Конечно, теория решения алгебраических уравнений является одним из них, — достаточно, прежде всего, назвать имена Лагранжа, Руффини, Гаусса, Абеля, Коши, Галуа, Серре и К.Жордана, — но не единственно определяющим, и уж, конечно, не единственным. Два другие источника, оказавших столь же плодотворное влияние, как и теория решения алгебраических уравнений, — геометрия и теория чисел XIX века — до сих пор не осознавались как таковые в значительной степени потому, что теоретико-групповые формы мышления применялись в этих областях неявно, вовсе без употребления термина `группа` и вначале без связи с параллельно развивающейся теорией групп подстановок", [6], **[368]**.

Эварист Галуа (Évariste Galois, 25 октября 1811, Бург Ла Рен — 31 мая 1832, Париж) — один из самых удивительных математиков во всей истории нашей науки, оказавший громадное влияние на ее дальнейшее развитие, тем более поразительное, что он был убит на дуэли в возрасте 20 лет.

Первая его работа, посвященная непрерывным дробям, была опубликована в апреле 1829 года. Его самое замечательное достижение состоит в том, что (в возрасте 16–18 лет!) он получил полный ответ на вопрос о разрешимости уравнений в радикалах. Однако ни Коши, ни Фурье, ни Пуассон не смогли понять его работ и "потеряли" рукописи статей, представленных им в Comptes Rendus (впрочем, потом Коши опубликовал ту часть этих работ, которую все же смог понять, под своим именем).

Среди прочего Галуа ввел понятия поля, группы, подгруппы, смежного класса, нормальной подгруппы, простой и разрешимой группы, композиционного ряда, etc. Много важнейших понятий алгебры названы в его честь: теория Галуа, группа Галуа, поля Галуа, соответствие Галуа, когомологии Галуа. Не надеясь более на честность французских математиков в предсмертном письме своему другу Огюсту Шевалье Галуа просит сообщить свои результаты об алгебраических функциях Гауссу и Якоби.

Работы Галуа были переоткрыты в 1843–1846 годах Лиувиллем, а широкое признание получили только в 1870-х годах. Все сохранившиеся математические рукописи Галуа собраны в **[271]**, и их чтение производит совершенно ошеломительное впечатление. В этих рукописях можно найти формулировки десятков теорем, которые обычно связываются с именами Коши, Жордана, Гельдера, Мура и других математиков, доказавших эти факты десятилетия спустя. Часть этих текстов переведена на русский язык **[65]**.

Широкой публике Галуа известен главным образом по романтической легенде, порожденной тем, что он погиб в столь юном возрасте, два раза не был принят в *l'Ecole Polytechnique* и исключен из *l'Ecole Normale*, провел несколько месяцев в тюрьме, и т. д. Литература, посвященная этой легенде, совершенно необъятна, см., в частности, [7], [8].

Сам термин **группа** впервые употребил в 1830 году Эварист Галуа, правда он обозначал так как собственно группы, так и смежные классы по подгруппе. Этот термин происходит от **grouper les permutations** — **группировать перестановки**. А именно, Галуа связал с каждым алгебраическим уравнением группу перестановок его корней — **группу Галуа** — и доказал **спектакулярный**, или, как сказали бы сегодня, сенсационный результат, утверждающий, что уравнение тогда и только тогда разрешимо в радикалах, когда его группа Галуа разрешима. В течение нескольких лет было осознано, что этот результат объясняет неразрешимость классических геометрических проблем (трисекция угла, удвоение куба, ...) — и что его легко обобщить с тем, чтобы доказать несуществование интегралов от элементарных функций, невозможность интегрирования дифференциальных уравнений в квадратурах и т. д. В качестве типично шпенглеровского совпадения отметим, что в том же самом 1830 году, когда Галуа впервые употребил термин **группа**, Гессель нашел все 32 кристаллографические класса.

Однако я склонен верить, что в действительности понятие группы является *древнейшим* математическим понятием, не только более древним, чем алгебраические уравнения, но даже более древним, чем само понятие числа, и неотделимым от человеческой цивилизации. Группы п[р]оявляются всюду, где возникают симметрии, автоморфизмы, обратимые преобразования. Иными словами, всюду, где есть повторяющиеся и самовоспроизводящиеся узоры (**patterns**). А человеческая культура, подобно природе и жизни, состоит в составлении узоров. Группы — уже конечные группы — дают нам неисчерпаемый материал для упражнения нашего остроумия и изобретательности. Именно этим объясняется вездесущность идеи группы, универсальность этого понятия и огромное разнообразие его приложений в самой математике, а также в искусстве, физике, химии, кристаллографии, теории передачи информации, криптографии, ...

§ 3 ✠. Мистический план: пригоршня философем с оргвыводами

> Как часто в науке начинаешь понимать, что абстракции бывают в такой же или даже в большей степени реальны, чем осязаемые конкретные факты.
>
> Ганс Селье. [4]

Here are my principles. If you don't like them, I have

OTHERS.

Groucho Marx

Для более квалифицированного читателя отметим несколько принципиальных идеологических соображений, объясняющих выбор и освещение материала.

• В приложениях теории групп в математике и за ее пределами, как правило, возникают не группы сами по себе, а **действия** групп, будь то перестановочные действия конечных групп, линейные действия групп Ли и алгебраических групп или непрерывные действия топологических или дискретных групп на многообразиях, графах и других геометрических объектах. В математике группа чаще всего (но не всегда!) возникает как **группа автоморфизмов** какой-то структуры точно так же, как алгебра Ли чаще всего возникает как **алгебра Ли дифференцирований**. Поэтому целью начального этапа изучения теории групп должна быть подготовка к изучению **теории представлений**, в первую очередь перестановочных и линейных. Это значит, что изучение теории групп должно начинаться с двух примеров: **симметрической группы** S_n и **полной линейной группы** $\mathrm{GL}(n, K)$.

• В действительности, S_n и $\mathrm{GL}(n, K)$ это **один и тот же пример**. С одной стороны, векторные пространства это множества с дополнительной структурой. С другой стороны, множества являются **частным случаем** векторных пространств. А именно, множество — это просто векторное пространство над полем из одного элемента, совпадающее со своим базисом. Подлинный смысл этого утверждения становится понятен только **после** изучения теории представлений и теории инвариантов, но обозначения, терминология и сама постановка вопросов должны с самого начала приучать к аналогии между перестановками и матрицами. Например, множество k-элементных подмножеств следует рассматривать как k-ю внешнюю степень множества и т. д. Формальным воплощением этой идеи является теория **λ-колец** [**80**], [**209**].

• Центральным объектом **всей** математики XX века является понятие группы **с дополнительной структурой**: топологические группы, вещественные и комплексные группы Ли, алгебраические группы[♮], p-адические аналитические группы, проконечные группы, адельные группы, etc. A *topological group* IS PERHAPS *the* MOST IMPORTANT CONCEPT IN MODERN MATHEMATICS, [**324**], с. 125. Это понятие лежит в основе не только алгебры и топологии, но и римановой геометрии, алгебраической геометрии, теории комплексных аналитических пространств, теории чисел, теории автоморфных функций, функционального и гармонического анализа, теории специальных функций, теории интегрирования, теории дифференциальных уравнений, эргодической теории (не говоря уже о приложениях в физике!).

[♮]Я помню свое удивление, когда первый раз увидел выражение **алгебраические группы** — по наивности я тогда считал, что **алгебраические группы** это *абстрактные* группы. В действительности, как мы впервые услышим уже в главе I, алгебраическая группа — это группа, которая одновременно является алгебраическим многообразием, причем отображения, определяющие структуру группы, являются морфизмами многообразий.

Софус Ли (Sophus Lie, 17 декабря 1842, Nordfjordeid, поселок недалеко от Бергена, — 18 февраля 1899, Кристиания, ныне Осло) — гениальный норвежский математик, основатель теории групп и алгебр Ли, внесший основополагающий вклад в геометрию, теорию дифференциальных уравнений и математическую физику. По общему признанию XX век в математике был веком теории Ли, в том же смысле, в котором XVIII век был веком вещественного анализа, а XIX век — веком комплексного анализа.

Преподавателем математики в школе, где учился Ли, был Людвиг Силов и Ли посещал его лекции по теории групп. Его первые работы конца 1860-х годов относятся к геометрии. О его выносливости и физической силе в то время ходили легенды. Например, однажды он решил навестить своих родителей в Моссе, пройдя 60 километров и не застав их дома, он тут же развернулся и направился обратно в Осло.

В 1869–1870 годах Ли получил стипендию для стажировки в Берлине и Париже, где близко подружился с Клейном. Французская стажировка чуть не закончилась для Ли трагически. Когда началась франко—германская война, Клейн вернулся в Германию, а Ли отправился *пешком* в Италию. По дороге он был арестован как немецкий шпион, так как полицейские приняли его математические записи за шифр. И уж, конечно, особенно подозрительным было письмо от Клейна на немецком языке! Его даже хотели расстрелять, но после вмешательства Гастона Дарбу все же освободили. Во время этой поездки Ли понял основополагающее значение теории групп для математики. С тех пор основной темой его исследований стали непрерывные группы и их приложения в геометрии, теории дифференциальных уравнений и механике.

После возвращения Ли в Норвегию в 1871 году он защитил докторскую диссертацию и начал искать университетскую позицию за границей, но в 1872 году его назначили (экстраординарным) профессором университета в Кристиании. Что касается научной работы, следующие 10 лет были самыми продуктивными в его жизни. За эти годы он и создал то, что сегодня носит имя **теории Ли**, и получил фундаментальные приложения этой теории в теории дифференциальных уравнений. Кстати, многие из его работ того периода написаны на норвежском языке!

Однако, в 1886 году Клейну предложили позицию в Геттингене и Ли перебрался на освободившуюся позицию в Лейпциге. Судя по дальнейшему развитию событий, это было ошибкой. Ли страдал от необходимости много преподавать на иностранном языке слабым студентам, крайне болезнено воспринимал вопросы приоритета и остро конфликтовал с немецкими коллегами — как в Лейпциге, так elsewhere, в том числе с Клейном и Киллингом. Уже в 1889 году это привело к тяжелейшему нервному расстройству и бессоннице, так что Ли был даже вынужден длительное время лечиться в психиатрической клинике под Ганновером, все время мечтая вернуться на родину. Однако фактически вернулся он только в 1898 году, уже абсолютно больным человеком, и на следующий год умер от злокачественной анемии.

В нашем курсе упоминаются алгебры Ли, скобка Ли, группы Ли, теория Ли, несколько теорем Ли, теорема Ли—Колчина, etc. На русском языке имеется достаточно основательная биография Ли [9].

• Наиболее интересные группы — это **конкретные** группы: группы симметрии геометрических конфигураций, простые конечные группы, простые алгебраические группы, классические группы, группы движений, группы типа Ли, группы Шевалле, группы Стейнберга, группы Кокстера, группы Вейля, группы, порожденные специальными элементами (отражениями, псевдоотражениями, корневыми элементами, квадратичными элементами, etc.), кристаллографические группы, спорадические группы, etc. Именно к изучению этих групп относится **подавляющая** часть наиболее содержательных, глубоких, трудных и полезных результатов теории групп.

• Изучение **абстрактных бесконечных групп** алгебраическими методами чрезвычайно сложно, в большинстве случаев не очень интересно, а зачастую просто совершенно бессодержательно. Теория бесконечных групп является разделом **геометрии**, а не алгебры. Даже в тех случаях, когда чисто алгебраическое изучение абстрактных групп возможно и плодотворно (свободные группы, свободные произведения, амальгамы, группы Бернсайда, etc.) **только** геометрическая реализация может дать настоящее понимание. Например, свободная группа является **фундаментальной группой графа** и **все** относящиеся к ней результаты естественнее всего доказывать именно на этом языке.

• Понятие **конечной группы** содержательно как само по себе так и, в особенности, в связи с ролью конечных групп в алгебраической теории чисел, комбинаторике, теории кодирования, теории решеток, классификации многообразий, и т. д. Конечные группы являются линейными и алгебраическими, в классе конечных групп можно проводить чисто алгебраические доказательства **индукцией по порядку** точно так же, как в классе связных алгебраических групп можно проводить **индукцию по размерности**[♮]. Конечные группы устроены гораздо сложнее, чем алгебраические группы над алгебраически замкнутым полем (если, конечно, интересоваться только замкнутыми подгруппами, рациональными представлениями и т. д.!) и гораздо проще, чем алгебраические группы над произвольным полем. Первым шагом к решению любого вопроса о конечных группах является решение соответствующего вопроса об алгебраических группах над алгебраически замкнутым полем. Классификация дает возможность получать чисто алгебраические ответы на многие *естественно* возникающие вопросы, относящиеся к конечным группам. Тем не менее, даже при анализе конечных групп значительно продуктивнее пользоваться геометрическими реализациями связанными с соответствующей алгебраической группой, либо, если с группой не связано никаких классических геометрий, строить комбинаторную геометрию исходя из самой группы (билдинги, диаграммные геометрии и т. д.).

• С каждой группой связано **групповое кольцо**. Описание линейных представлений группы эквивалентно описанию модулей над ее групповой алгеброй. Тем самым, теория представлений групп вкладывается в более общую **теорию представлений ассоциативных колец**. Тем не менее, отдельное изложение классической — **полупростой** — теории представлений конечных групп вполне оправдано, по следующим причинам. Во-первых, это случай, представляющий наибольший интерес для подавляющего большинства приложений за пределами

[♮]С точки зрения **теории моделей** порядок и размерность — это одно и то же, и то и другое являются частными случаями **ранга Морли**, [10].

алгебры. Во-вторых, это модель гармонического анализа — конечномерная, но **некоммутативная**! В силу конечномерности здесь не происходит отвлечения внимания на второстепенные вопросы сходимости, с другой стороны, в силу некоммутативности возникает гораздо лучшее понимание действительно важных структурных вопросов. В-третьих, понимание современной теории представлений ассоциативных колец — и даже понимание гораздо более простой теории модулярных представлений конечных групп — на принятом в общем курсе уровне абстракции в принципе невозможно. Дело в том, что в этих теориях мы должны переосмыслить язык, технику и саму проблематику теории представлений, по сравнению с классическим случаем. В неполупростом случае полностью или в значительной степени утрачивают свое значение такие классические понятия, как неприводимое представление, и попытка изложить неполупростую теорию на классическом языке приводит к нагромождению технических деталей и полному непониманию. С другой стороны, любая попытка ввести на начальном уровне современные понятия, для которых студент не обладает ни опытом, ни мотивацией, ни набором мысленных образов, может привести только к формализму и полному непониманию.

• Понятие группы **аналогично** понятию **алгебры Ли**: в группе умножение играет роль сложения, а коммутирование — роль скобки Ли. Использование групп автоморфизмов полностью параллельно использованию алгебр Ли дифференцирований. Однако понятие группы **значительно** сложнее понятия алгебры Ли, так как умножение в группе некоммутативно, поэтому прежде, чем браться за какую-то задачу о группах, полезно вначале решить соответствующую задачу для алгебр Ли. Эта аналогия чрезвычайно плодотворна и как руководящая идея, и как точное математическое утверждение (в тех случаях, когда ее **удается** превратить в точное утверждение, как, например, в теории Ли или в теории Магнуса). Эта аналогия получает полное развитие в теории **алгебр Хопфа** (или, как теперь принято говорить, **квантовых групп**), где выясняется, что группы и алгебры Ли являются частными случаями одного и того же объекта и все относящиеся к ним результаты допускают единую формулировку. Любое современное изложение теории групп должно учитывать параллелизм групп и алгебр Ли на уровне языка, техники и постановки вопросов.

• **Самым важным** из всего, что произошло до сих пор в конечной математике, является **классификация конечных простых групп**. Она открывает возможность к получению доказательств результатов о конечных объектах, основанных на переборе случаев (case by case analysis). Следствия классификации [11] для таких областей математики, как теория чисел, комбинаторика, теория Галуа, теория решеток, теория римановых поверхностей, теория особенностей, теория кодирования, и т. д. не говоря уже о самой теории конечных групп и теории представлений, не только не продуманы, но и не начинали всерьез продумываться. Симметрии платоновых тел гипнотизируют математиков на протяжении 25 веков. Можно думать, что и симметрия конечных простых групп и извлечение ее непосредственных следствий будет одной из важнейших задач математики на несколько столетий. Поэтому курс теории групп, в котором не сформулирована теорема классификации конечных простых групп, не является курсом теории групп.

• Теория алгебр Ли есть теория **простых алгебр Ли**. Нильпотентные и разрешимые алгебры Ли рассматриваются не сами по себе, а лишь постольку, поскольку это необходимо для классификации или изучения простых алгебр. Точно так же

теория групп должна быть теорией простых групп. То, что это не так, и в XX веке было написано громадное число работ по группам, близким к разрешимым, представляется мне аберрацией, связанной с тем, что простые группы были классифицированы исторически очень поздно — даже предположение о возможности полной классификации конечных простых групп не высказывалось всерьез до начала 1960-х годов.

• Теория абелевых групп по своей идеологии и используемой технике вообще не является частью теории групп, а относится к **линейной алгебре**. Конечно, модули над кольцом $\mathbb{Z}$ можно изучать и сами по себе, но действительно интересный вопрос состоит в том, какие из свойств кольца $\mathbb{Z}$ при этом на самом деле используются. Таким образом, результаты об абелевых группах, за исключением классификации **конечно порожденных абелевых групп**, вообще не следует включать в курс теории групп. Классификация же конечно порожденных абелевых групп настолько важна для изучения конечных групп и с точки зрения приложений в теории чисел и комбинаторике, а ее доказательство настолько просто, что включение его в курс теории групп оправдано.

• Классификация **с точностью до изоморфизма** сколь-нибудь широких классов групп в терминах явных инвариантов (аналогичная классификации конечно порожденных абелевых групп) как правило **невозможна**. Например, невозможна уже никакая разумная классификация конечных метабелевых p-групп. Дело в том, что такая классификация включала бы в себя задачу о паре матриц и, тем самым, отвечала бы вообще на **все** вопросы жизни. Кроме того, в большинстве случаев такая классификация не является даже желательной. Например, даже когда в некотором классе групп известны полные наборы инвариантов с точностью до изоморфизма (скажем, для некоторых классов бесконечных абелевых групп), на большинство конкретных вопросов проще отвечать непосредственно, чем пользуясь такой классификацией.

• Доказательство большинства результатов о группах (в особенности о конечных группах!) разбивается на рассмотрение **массового случая** и анализ **маленьких исключений**. При этом именно анализ маленьких исключений обычно представляет наибольшие трудности, однако именно эти исключения, а не массовый случай чаще всего возникают в приложениях. С этой точки зрения методически неправильно — как это часто делается в элементарных руководствах — опускать анализ исключительных случаев. Построение внешнего автоморфизма S_6 столь же важно (и *по крайней мере* столь же интересно!), как доказательство того, что все автоморфизмы остальных симметрических групп внутренние. Воспитание привычки и вкуса к подобного рода тщательности имеет, среди прочего, громадное значение для формирования здорового профессионального рефлекса **полноты анализа**.

• Самым важным экстра-математическим феноменом последних десятилетий является распространение **компьютеров**. За последние 10 лет наши возможности проведения математического эксперимента выросли на несколько порядков. Представляется в высшей степени правдоподобным, что роль компьютеров будет возрастать и дальше. Уже сегодня во многих областях математики, в том числе (и, может быть, в первую очередь!) в **теории конечных групп**, математик, не вооруженный компьютером, не может успешно конкурировать с математиком, который кроме своей области владеет еще и техникой

символьных вычислений. В связи с этим мне представляется, что любой современный курс алгебры должен учитывать возможность **имплементации** излагаемых в нем методов. Кроме того, компьютерный эксперимент позволяет отвечать на конкретные вопросы, которые были вне досягаемости предшествующих поколений математиков.

• На группу можно смотреть как на **групповой объект** в категории множеств. В действительности, групповые объекты можно определить в любой категории, имеющей финальный объект e и допускающей конечные произведения. Наиболее известны групповые объекты в гомотопической категории, называемые **H-пространствами**, и групповые объекты в категории схем, называемые **групповыми схемами** (group scheme, употребляется также французский термин **схема в группах**, schéma en groupes), но, в действительности, можно рассматривать и групповые объекты в других категориях. Ясно однако, что это представляет следующий уровень абстракции по сравнению с теорией групп, *систематический* переход на который на элементарном уровне невозможен. Тем не менее, любое современное изложение теории групп должно учитывать *возможность* такого перехода. В действительности, многочисленные симптомы показывают, что над алгеброй нависла следующая неотвратимая смена парадигмы, при которой утратят свое значение используемые сегодня точные понятия такие, как, скажем, изоморфизм, точные тождества типа ассоциативности, etc. Все эти понятия заменятся на соответствующие понятия и тождества, понимаемые с точностью до гомотопии.

• Онтогенез является рекапитуляцией* филогенеза. В применении к интересующей нас теме это значит, что развитие индивидуального математика должно резюмировать (recapitulate) развитие математики. С этой точки зрения **кристаллографические группы** являются *идеальным* материалом для изучения групп на начальном этапе. Во-первых, это сюжет, история которого насчитывает *десятки тысяч лет*, непосредственно апеллирующий к человеческой любознательности и эстетическому чувству. Во-вторых, это раздел теории групп, который никогда не терял своей роли в истории человеческой культуры и сегодня сохраняет свое значение с точки зрения **реальных** приложений в науке и искусстве. Наконец, в-третьих, уже в случае размерностей 2 и 3 возникающие при этом математические вопросы совершенно небанальны и были полностью решены только в конце XIX — начале XX века. Все это позволяет проиллюстрировать такие понятия как нормальный делитель, фактор-группа, расширения, сопряженность, когомологии на настоящих, а не учебных примерах.

§ 4 ◇. Практический план: для всех и ни для кого

> Главным побудительным мотивом было желание сказочника испробовать свои силы в действительно длинной сказке, которая удержала бы внимание читателей, развлекла их и доставила им радость, а иногда, может быть, и тронула. В качестве проводника мне служило лишь мое собственное чувство, а многих такой проводник подводил. Некоторые из читателей нашли книгу скучной, нелепой или недостойной внимания, и я не собираюсь с ними

*Существенно, что именно **рекапитуляцией**, а не *повторением*, как иногда переводят!

> спорить, ибо испытываю аналогичные чувства по отношению к их книгам или книгам, которые они читают. Но даже с точки зрения тех, кому понравилась моя книга, в ней есть немало недостатков. Вероятно, невозможно в длинной сказке в равной мере удовлетворить всех читателей: я обнаружил, что те отрывки или главы, которые одни мои читатели считают слабыми, другим очень нравятся. Наиболее критичный читатель — сам автор — видит теперь множество недостатков, больших и малых, но так как он, к счастью, не обязан пересматривать книгу или писать ее заново, то пройдет мимо них в молчании, отметив лишь один недостаток, отмеченный некоторыми читателями: эта книга слишком коротка.
>
> Джон Рональд Руэл Толкин. *Властелин колец*

> Самые острые разногласия между суфиями и обычными схоластами вызывает суфийская теория, гласящая, что идеи суфиев могут изучаться только в соответствии с особыми принципами, один из которых: время, место, люди ... Утверждают, что любой отрывок в Коране имеет семь смыслов, каждый из которых соответствует состоянию читателя или слушателя.
>
> Идрис Шах. *Сказки дервишей*

1. Архитектоника: горизонтальное членение. Выбор материала в настоящей книге и ее композиционные особенности определяются следующими обстоятельствами. С одной стороны, она представляет собой **вторую** часть **тетралогии**, части которой срифмованы по схеме ABBA:

Книга I. Не совсем наивная теория множеств

Книга II. Конкретная теория групп

Книга III. Конкретная теория колец

Книга IV. Не совсем наивная линейная алгебра

С другой стороны, она представляет собой **первую** часть **дилогии**, более продвинутая вторая часть которой

Книга IIbis. Теория конкретных групп

посвящена изложению основ теории групп типа Ли и связанных с ними групп.

2. Кому и зачем. Курс рассчитан, в первую очередь, на следующие категории читателей:

• Как **современный базовый учебник** для всех, кто впервые *серьезно* знакомится с алгеброй, скажем на младших курсах университета, в рамках таких специальностей, как прикладная математика,

программирование, теоретическая физика, квантовая химия, теория управления, кристаллография или криптография и кодирование.

• Как **вспомогательный элементарный учебник** для студентов 1-го курса в области чистой математики. Однако с точки зрения профессионального математика этот учебник в целом слишком консервативен и аналитически ориентирован. Для математика его чтение должно сопровождаться изучением более продвинутых источников, подчеркивающих теоретико-категорные, топологические и геометрические аспекты рассматриваемых понятий.

• Как **дополнительный задачник** средне высокого уровня. Я не пытаюсь конкурировать с такими задачниками, как [**82**] и привожу очень мало стандартных однотипных задач. Кроме того, многие задачи жестко привязаны к месту их появления и не могут быть решены начинающим сами по себе, в отрыве от антуража. Это связано с тем, что в основном это задачи предлагавшиеся в `ПОМИ-группах`[♮], где практика не отделяется от лекций.

• Как **справочник** для математиков-неспециалистов, ученых — физиков, химиков и кристаллографов, инженеров, в первую очередь специалистов по теории кодирования, теории информации и теории управления, программистов, — словом тех, кто в принципе уже когда-то что-то слышал об алгебре, но забыл слова **`идеал`** и **`гомоморфизм`**, хочет освежить свои знания или быстро получить справку по конкретному вопросу.

• Как **Schatzgrube** (=`treasure-trove`) для всех, кто преподает алгебру на университетском уровне и продумывает различные возможности построения курса, или просто ищет новые примеры и вычисления, новые образы, новые задачи или более простые доказательства основных фактов.

• Как **развернутое введение** к Книге IIbis, адресованное студентам старших курсов и аспирантам, занимающимся алгебраической K-теорией, алгебраической геометрией, алгебраической теорией чисел,

---

[♮]Петербургская реалия. Несколько упрощая, можно сказать, что `ПОМИ-группа` представляет собой **`пролонгацию`** системы математических кружков еще на два года. Каждый год среди студентов мат-меха отбирается 8–20 человек, которых пытаются *по-настоящему* учить *настоящей* математике. Они сдают два комплекта экзаменов: два экзамена по анализу, два экзамена по алгебре, два экзамена по геометрии и т. д., один по общей, второй по полной программе. Название связано с тем, что занятия `ПОМИ-групп` происходят не на мат-мехе, а в здании ПОМИ, набережная Фонтанки 27. Подробное описание истории и теории `ПОМИ-групп` можно найти на сайте Санкт-Петербургского Математического Общества.

теорией Галуа, классическими группами, квадратичными формами, группами типа Ли, алгебраическими группами, группами Шевалле, простыми конечными группами в направлениях, близких к научным интересам **фаддеевской школы**, которые хотят быстро узнать концептуальные объяснения *уже известных* им фактов или углубить *понимание* нужных им фрагментов общей теории.

• Как **книгу для чтения** дли широких кругов образованных читателей обладающих некоторым досугом: "пенсионеров, школьников старших классов и способных аспирантов" (Сан Саныч Кириллов, [**99**] предисловие к изданию 1972 года, стр. 5, из последующих изданий эта блистательная **локуция*** исключена).

• Как **памятник русской словесности** для Василеостровских автохтонов и приравненных к ним, для тех, кто интересуется доктринальными, мистическими, психологическими и историческими аспектами математики, для всех, кто увлекается духовной жизнью, мифологией и культурой Санкт-Петербурга, и вообще для всех, кто может, умеет и хочет читать по-русски.

3. Copyleft notice. Разумеется, это не исключает возможности использования этой книги другими категориями читателей, или для других целей: как цитатника и словаря **квотаций***, с намерением плагиата, интеллектуального пиратства и нелицензионного использования содержащихся в ней мыслей и мыслей, которые приходят в голову при ее чтении, в качестве pillow-book, подставки под ножку стола, и тому подобное.

Я считаю своим долгом предупредить, что не несу *никакой* юридической, нравственной или интеллектуальной ответственности за прямые и косвенные риски, проистекающие из подобного несанкционированного использования моей книги. Большая часть цитат и эпиграфов придуманы лично мною — *You think it's easy for me to misconstrue all these misquotations*?!? — и тот, кто захочет использовать их без

---

*`Локуция` — оборот речи, фраза, устойчивое словосочетание, идиоматическое выражение. Эта **вокабула** поддерживается большим количеством однокоренных диалектных терминов: **локутор** (=конферансье, ведущий, диктор, тамада, культуртрегер, массовик-затейник, мастер церемоний), **интерлокутор**, **интерлокуция**, **циркумлокуция** и т. д.

*`Квотация` — *явная* цитата, воспроизводимая `verbatim` чужая речь, выделенная из основного текста специальными техническими средствами наподобие `\quote` ... `\unquote`; сегодня известно широкой публике главным образом в специфическом биржевом значении **котировка**. **Мисквотация** — неправильное цитирование; приписывание человеку слов, которых он не произносил.

ссылки на данную книгу, может впоследствии сильно удивиться. Например, я всюду использую Рассела и Виттгенштейна в качестве мифологических знаковых фигур, наподобие Будды или Христа, выражающих некоторую *позицию*. Ясно, что они не только никогда фактически не говорили, но и *не могли* сказать ничего из того, что я им здесь приписываю. С другой стороны, многие фрагменты авторского текста, в частности, **все** фразы, набранные *курсивом* `\it` и КАПИТЕЛЬЮ `\smc`, являются *почти* дословными цитатами, введенными для любителей шарад и развлечений. В большую часть доказательств сознательно внесены опечатки, столь оживляющие чтение математического текста. Эти опечатки являются моей электронной подписью и делают доказуемым каждый случай прямого несанкционированного включения текста этой книги в другие произведения.

Все мысли, которые могут прийти в голову при чтении данной книги, являются интеллектуальной собственностью автора и объектом авторского права. Их нелицензированное обдумывание запрещается.

§ 5 ♢. Технический план: кулинарный путеводитель

> Причиной для таких различных уровней сложности является то, что люди изменяются по мере привыкания к некоторому мощному инструменту. Когда Вы впервые пытаетесь пользоваться TEX'ом, Вы обнаружите, что некоторые части его очень просты, в то время как к другим надо привыкнуть. Через день или немного позже, после успешного набора нескольких страниц, Вы станете другим человеком, понятия, которыми Вы пользовались с трудом, теперь покажутся естественными, и окажется, что можно в уме представить конечный результат прежде, чем он будет получен машиной. Но тогда, вероятно, Вам захочется большего. После следующей недели работы Ваши горизонты раздвинутся еще шире и Вы подрастете и т. д. С годами Вы столкнетесь с набором многих видов текста и обнаружите, что Ваше обращение с TEX'ом по мере накопления опыта претерпело изменения. Так всегда при освоении мощного инструмента: всегда есть, чему учиться и всегда есть лучший способ делать то, что делал раньше. На каждой стадии развития Вам будет нужен чуть отличающийся тип руководства. Обращая внимание на знаки в этой книге, можно лучше сосредоточиться на уровне, который интересует Вас в настоящее время.
>
> Дональд Кнут. [12]

Суфий, познавший Высшую Истину, действует и говорит, учи-

тывая понимание, ограничения и господствующие скрытые предубеждения своих слушателей. Способность истолкования означает, что человек способен легко читать то, что сказано мудрецом, пятью совершенно различными способами.

Идрис Шах. *Путь суфиев*

Самый большой грех по отношению к ближнему — говорить ему то, что он поймет с первого раза.

Венедикт Ерофеев. *Из записных книжек*

1. Архитектоника: вертикальное членение. В соответствии с этим изложение **эксплицитно** разделено на **пять** МАРКИРОВАННЫХ *четко различающихся* уровней:

- для инженеров ♢,
- для физиков ♡,
- для математиков ♠,
- для алгебраистов ♣,
- для любознательных школьников и пенсионеров ✠

Маркировка первых четырех уровней отвечает рангам мастей в скате. Начинающий должен иметь в виду, что внутри любого параграфа ему могут встретиться фрагменты или комментарии профессионального и/или любительского уровня, которые никак отдельно не выделяются! Если при первом чтении ей непонятно что-то напечатанное мелким шрифтом, это нормально, нужно просто ДВИГАТЬСЯ ДАЛЬШЕ, понимание придет: THE FOCUS IS ON GOING FORWARD, BECAUSE MATHEMATICS IS **only** LEARNED IN HINDSIGHT [**256**]. В этой книге нет **ничего** находящегося на более глубоких уровнях, в частности, ничего адресованного специалистам по теории *конечных* — или, тем более, бесконечных — групп.

Вопросы, маркированные ♢ и ♡, обычно входят в общий курс алгебры на математико-механическом факультете СПбГУ, при этом вопросы с меткой ♢ рассказываются детально и их знание необходимо для получения удовлетворительной оценки, в то время как вопросы с меткой ♡ часто освещаются менее подробно или только упоминаются. Студенты-математики ПОМИ-группы, которым читается более продвинутый курс алгебры, должны *полностью* владеть уровнем ♡ и большинством тем с меткой ♠, хотя точный список может от года к году слегка меняться. Наконец, темы с меткой ♣ обычно включаются *только* в специальные курсы для студентов, специализирующихся по кафедре алгебры и теории чисел.

В действительности различие между ♢ и ♡ не столько в уровне сложности, сколько в уровне **императивности**. Некоторые темы маркированы ♡ не потому, что они труднее или менее важны, а только потому, что они меньше связаны с другими темами в этом курсе или других курсах, читаемых на математико-механическом факультете. То же самое относится к ♠ и ♣, но, конечно, между ♢ и ♡ с одной стороны и ♠ и ♣ с другой, в целом происходит **зримый** рост требований к зрелости, мотивации и/или настойчивости потенциального читателя. Все фрагменты параграфов с **красной меткой**, набранные мелким шрифтом (eightpoint), выходят за пределы общего курса и во многих случаях гораздо сложнее окружающего текста.

Все доказательства в параграфах помеченных ♢ и ♡ носят рутинный характер и любой компетентный алгебраист, допущенный к чтению лекций, должен быть в состоянии придумать любое из этих доказательств у доски в реальном времени (это относится только к основному материалу, но не к задачам, в параграфах с **красной меткой** полно задач с **черной меткой**). В действительности, именно это является для меня критерием для включения доказательства в общий курс. Я исхожу из того, что если я не в состоянии придумать доказательство за 2–3 минуты, то средний студент окажется не в состоянии воспринять такое доказательство. С другой стороны, студенты ПОМИ-групп (≈ студенты, специализирующиеся по кафедре алгебры и приравненные к ним) отнюдь не рядовые студенты, ни по степени таланта, ни по объему подготовки, ни по уровню мотивации. *Им* можно рассказывать доказательства таких не совсем банальных результатов, как теоремы Фробениуса, Бернсайда, Шура, Диксона, Шура—Цассенхауза или Холла. Чтобы состряпать *какое-нибудь* работающее (и, тем более, элегантное!) доказательство *таких* теорем профессиональному алгебраисту (не являющемуся специалистом по конечным группам!) может понадобиться часа два. Независимо от тщательности и продуманности изложения понимание этих доказательств может потребовать от студента некоторого интеллектуального усилия.

Относительно параграфов с меткой ✠, конечно, абсолютно не требуется, чтобы студент 1-го курса их прочел, и не предполагается, что он должен понять, *о чем* в них говорится. Однако студент 3-го курса мат-меха должен быть уже вполне в состоянии проследить не только за тем, *о чем*, но и за тем, *что* в них говорится. Вместе с тем, я не утверждаю, что студент 1-го курса *не может* понять эти параграфы. Более того, в последние годы мне посчастливилось встретить дюжину школьников, из хороших петербургских школ, которые были в состоянии полностью воспринять все, что в них сказано.

В ответ на замечания некоторых коллег на тему, что все эти уровни не могут быть одномоментно восприняты *начинающим*, и не лучше было бы написать *более короткий* учебник, содержащий только два первых уровня, я могу ответить следующее. О том, что может быть, а что не может быть воспринято *начинающим*, лучше спросить самого *начинающего*. Первой книгой по алгебре, которую я прочел летом с 9-го на 10-й класс, и которая уж совсем никак не адресована *начинающему*,

была *Алгебра* Сержа Ленга. В книге Ленга нет никаких удачных педагогических приемов, но есть владение материалом, увлеченность, полнота сознания и личность автора. Относясь с презрением к педагогике *как науке*, я старался написать такую книгу, которая по моим воспоминаниям могла бы заинтересовать меня самого в старших классах школы или на младших курсах университета и которая может быть интересна моим сегодняшним студентам. О том, удалось ли это, судить не мне, но, во всяком случае, за последние 5 лет большинство студентов смогли понять предмет `in parte`, а несколько десятков студентов ПОМИ-групп *творчески* овладели этим курсом `in toto`. С другой стороны, я, несомненно, согласен с тем, что для тех, кто интересуется алгеброй **ровно** в том объеме, что позволяет сдать экзамен *на положительную оценку*, следовало бы написать более короткий учебник — только мне самому делать это было бы не слишком интересно. В действительности, с моей собственной точки зрения самый крупный недостаток этой книги состоит в том, что она слишком коротка.

2. Рекомендации по чтению. Новичку, чтобы начать ориентироваться в предмете и увидеть хотя бы часть внутренних связей, нужно прочесть книгу *дважды*.

• Первый раз так:

◦ прочесть все параграфы всех глав, помеченные ♢,

◦ вернуться к § 6 и прочесть все параграфы всех глав, помеченные ♡,

◦ вернуться к § 2 и прочесть все параграфы всех глав, помеченные ♠.

• Второй раз — не менее, чем через 3–4 месяца, лучше через 6–8 месяцев после первого чтения, когда многие детали уже забылись, но общее впечатление еще осталось — можно читать подряд, включая формулировки, но пропуская доказательства в параграфах, помеченных ♣.

Вообще, начинающий должен иметь в виду, что определения, примеры, конструкции и методы важнее, чем подавляющее большинство доказательств и формулировок. Доказательства нужны главным образом для того, чтобы выяснить новые детали и проверить, правильно ли Вы понимаете смысл и пафос того, что говорится.

• Однако сам я предпочитаю читать книги с *произвольного* места, обращаясь к предшествующему по мере необходимости. Эта книга задумана и скомпонирована♯ именно для такого чтения, чему должны способствовать детальное оглавление, подробные указатели,

♯Я компонировал **Тристана** под влиянием большого чувства и после трех лет теоретической работы — Рихард Вагнер.

большое количество **реприз***, **трассировок***, **реитераций***, **тавтегорий***, и внутренних ссылок.

Тот, кто *легко* понял § 2 Главы 1 при первом чтении, решив в уме упражнения, скорее всего уже имеет университетское образование по специальности **математика** или сопоставимый уровень квалификации и не нуждается в моих советах. Он может далее читать или не читать книгу с любого места и в любом порядке.

§ 6 ♡. Мистический план: о математике и ее изучении

> To be a scholar of mathematics you must be born with talent, insight, concentration, taste, luck, drive and the ability to visualize and guess.
>
> Paul Halmos. *I want to be Mathematician*

> Итак, вопрос: откуда в общественном мнении появляются порочащие нравственный облик митьков сведения? Ответ: из митьковской мифологии. Сознание неразвитого слушателя выхватывает из мифа не суггестивные слои, и даже не мораль, а то, что это неразвитое сознание принимает за факты.
>
> Владимир Шинкарев. *Митьки*

А вот несколько мыслей, которые адресованы усердному и амбициозному начинающему. То, что я говорю, не следует воспринимать буквально — и не следует пытаться сразу этому поверить. Мне понадобилось года 2–3 на то, чтобы согласиться с утверждением Юрия Ивановича Манина о том, что доказательство важнее, чем результат, и лет 10–15, чтобы понять, что определения важнее, чем доказательства.

• **Формулы и вычисления.** Для непосвященного наиболее характерной чертой математики являются **формулы** и **вычисления**. Действительно, в математических текстах часто встречаются формулы некоторых специальных типов, но использование формул по крайней мере столь же характерно для многих других дисциплин, скажем, для химии и музыки, а в математических текстах кроме формул встречаются слова и картинки, причем некоторые виды слов и картинок столь же характерны для математики, как некоторые виды формул. Имеется

---

*Репри́за — возвращение к той же теме или фразе в новом контексте или с новой точки зрения.

*Трассировка или трассирование — регистрация, отслеживание, мониторинг; в особенности запись или фиксация пройденного пути.

*Реитерация — многократное возвращение в одно и то же место или к одному и тому же сюжету. В отличие от репризы, которая подразумевает творческое подхватывание идеи, наличие вариаций и определенный артистизм, реитерация часто является чисто механической, назойливо **репетитивной** и даже маниакальной.

*Тавтегория — повторение того же самого примерно теми же словами, в противоположность **аллегории** — иносказанию, повторению того же самого *другими* словами.

много типов *псевдоматематических* формул, встречающихся в текстах по социальным наукам, экономике, психологии, военному делу и т. д., которые не имеют **ничего общего** с тем, как формулы понимаются в математике и которые для профессионального математика выглядят совершенно анекдотически. Это **ритуальное** использование формул, *громкая музыка, призваная соблазнять глупых людей*. Математики *редко* пользуются формулами в ритуальных целях, а многие математики стараются вообще не использовать формул для передачи тех мыслей, которые легко выразить словами или рисунками.

• **Вычисления и рассуждения.** Что же касается вычислений, то математикам действительно иногда приходится что-то вычислять, однако в целом математики проводят **значительно** меньше вычислений, чем, скажем, физики, астрономы, химики, инженеры или экономисты. В любом случае это совсем не те вычисления, которым учат в школе. Однако действительно характерным для работы математика являются не вычисления, а построение цепочек рассуждений, **заменяющих вычисления**. С точки зрения профессионала, математика не есть искусство **проводить** вычисления, а искусство **избегать** вычислений. На самом деле, виртуозный счет редко является самоцелью или предметом особой гордости математика, это просто элемент его профессии, побочный продукт навыка проведения **рассуждений**. Целью математика и его главным инструментом являются не вычисления, а ясное мышление.

• **Доказательства.** Еще одной бросающейся в глаза чертой математики является наличие **доказательств**. Собственно, математик — это тот, кто умеет находить доказательства. Так, трактат Никола Бурбаки начинается со следующей констатации: "Со времен греков говорить **математика** — значит говорить **доказательство**. Некоторые сомневаются даже, что вне математики имеются доказательства в том точном и строгом смысле, какой получило это слово у греков и какой мы хотим придать ему здесь". Действительно, в течение многих столетий за пределами математики не было ничего хотя бы отдаленно приближающегося по степени убедительности к математическим доказательствам. Аргументация, приводимая обычно в подтверждение своих концепций специалистами в области *естественных* наук, обычно не выдерживает **никакой** критики с точки зрения принятых в математике стандартов, а то, что называется **аргументацией** у философов и представителей *общественных* наук, с этой точки зрения вообще не заслуживает обсуждения.

Впрочем, в последние десятилетия достаточно убедительные — а иногда и просто почти безупречные — математические доказательства встречаются во многих работах по теоретической физике, скажем, по квантовой теории поля, гравитации, статистической физике, и т. д., а также по теории управления, теории связи и некоторым другим областям знания. Впрочем, Бурбаки мог бы возразить на это, что эти разделы науки являются скорее математикой — или, точнее, математической **деятельностью**, чем собственно физикой или инженерными дисциплинами в традиционном понимании.

• **Определение — формулировка — доказательство.** Однако, профессиональный математик знает, что характеристикой математики являются не доказательства сами по себе, а триада **определение — формулировка — доказательство**, причем основой этой триады являются именно **определения**. Ни одна другая область человеческой деятельности не знает ничего подобного математическому доказательству по степени убедительности именно пото-

му, что она не знает ничего подобного математическому определению[♮]. Слегка перефразируя Рассела, можно констатировать, что

○ в математике мы знаем, верно ли то, что мы говорим.

○ Более глубокая причина того, что мы знаем, верно ли то, что мы говорим, состоит в том, что в математике мы знаем, что мы говорим.

○ В свою очередь причина того, что мы знаем, что говорим, состоит в том, что, в отличие от большинства остальных областей человеческой деятельности, в математике мы знаем, о чем мы говорим.

Поэтому начинающий должен прежде всего контролировать, понимает ли он, **о чем** говорится; затем, понимает ли он, **что** именно говорится; и *только* после этого можно начинать задумываться над тем, **верно ли** то, что говорится. Разумеется, по мере овладения предметом он начнет задумываться над другими вопросами: **почему** это верно, **почему** это говорится, почему говорится **именно это** и, наконец, **что еще** можно было бы сказать.

• **Face value.** Самая значительная трудность для нематематика состоит именно в том, чтобы понять, что математические понятия выражают ровно то, что говорится в их определении. Что такое квадратный корень из -1? — это просто квадратный корень из -1! — allez en avant et la foi vous viendra. Трудно дать сколь-нибудь удовлетворительное определение таких понятий, как **мышление** или **человек**, или даже таких простейших понятий, как **электрон** или **стул**. Дело в том, что вещи или явления, описываемые этими понятиями, существуют до и, по всей видимости, независимо от этих определений. В то же время, смысл, в котором существуют математические понятия, уже не столь очевиден.

Однажды после лекции ко мне подошла студентка первого курса и спросила: "Что такое кольцо?" — "Ну как же, — ответил я — это множество с двумя бинарными операциями [...]" — "Это я помню, а все-таки, что это такое?" — "Ну посмотрите на примеры, вот целые числа образуют кольцо относительно обычных операций сложения и умножения, многочлены, матрицы, [...]" — "Это я тоже помню, а все таки, **что такое кольцо?**" Первый навык, которым должен овладеть каждый, всерьез желающий понять математику, является умение воспринимать все буквально. Второй навык, которым он овладеет с необходимостью — это умение воспринимать все **метафорически**.

• **Контролируемая точность.** Еще одним эпитетом, традиционно характеризующим математику, является ссылка на ее **точность**. Действительно, мате-

---

[♮] "Verworrenheiten in Begriffen und Definitionen sind nirgends mehr zu Hause, als bei Philosophen, *die keine Mathematiker sind*. Sehen Sie sich doch nur bei den heutigen Philosophen um, bei Schelling, Hegel, Nees von Esenbeck und Consorten, stehen Ihnen nicht die Haare bei ihren Definitionen zu Berge. Aber selbst bei Kant steht es oft nicht viel besser; seine Distinctionen sind meines Erachtens solche, die entweder nur auf Trivialitäten hinausläufen, oder falsch sind." — "Путаница в понятиях и определениях нигде не так пышно не разрастается, как у тех философов, *которые не являются одновременно математиками*. Посмотрите хотя бы на сегодняшних философов, всяких там Шеллингов, Гегелей, Нееса фон Эзенбека и их прихвостней, — разве у Вас не встают волосы дыбом от их определений? Но даже с Кантом дела часто обстоят немногим лучше; все его разграничения по моему мнению либо сводятся к полным тривиальностям, либо ложны." [13]

матика предполагает значительно большую точность, чем почти все остальные виды человеческой деятельности и на протяжении многих веков ее единственными соперниками в этом отношении были лишь естественный язык и музыка. Заметим, впрочем, что ориентальная культура породила такие правополушарные занятия, как китайская каллиграфия или японские боевые искусства, требующие точность, сопоставимую с точностью обычной в математике.

Однако в настоящее время точность математики не является чем-то исключительным. В действительности в настоящее время имеется несколько областей деятельности, которые требуют точности **большей**, иногда **значительно** большей, чем математика. Речь идет не только о таком достаточно экзотическом занятии, как математическая логика (которую *при желании* можно считать разделом математики, хотя с моей личной точки зрения она гораздо дальше от основного русла математических исследований, чем, скажем, физика или лингвистика), но и о таких относительно массовых профессиях, как computer science или криптография. Как заметил один специалист по программированию, `the problem with you mathematicians is that you are so imprecise`. Особенностью математики является не точность как таковая, а **контролируемая** точность. Чем лучше мы понимаем то, что происходит, тем менее точными мы можем позволить себе быть.

• **Простота математики.** Есть еще одна нетривиальная параллель между каллиграфией, боевыми искусствами и математикой. Как каллиграфия, так и искусство меча основаны на использовании 5–6 фундаментальных принципов, причем суть состоит не в **знании** этих принципов — их знает каждый, кто взял 2–3 урока, а в **умении** их применять, т. е. собственно в **мастерстве**. Конечно, число фундаментальных принципов в математике больше, но оно совсем не так велико, как думает начинающий. Число *действительно* фундаментальных принципов, на которых построено подавляющее большинство математических доказательств, вряд ли превосходит несколько десятков. Но профессионал может применять эти простые соображения с изощренностью (или, как говорит Литтлвуд, **виртуозностью**) недоступной для начинающего или любителя и в состоянии образовывать из них сколь угодно длинные цепочки рассуждений. Математика основана на простых, но могущественных идеях. Самая могущественная идея, которой учит математика, — это идея о могуществе простых, но могущественных идей — the power of powerful ideas.

§ 7 ♣. Мистический план в фактических аспектах: доказательства

> Среди всех искавших истину в науках только математикам удалось найти некоторые доказательства, т. е. некоторые точные и очевидные соображения.
>
> Декарт. *Рассуждение о методе*

> Every proof is a one-line proof, if you start sufficiently far to the left.
>
> *Cambridge Mathematical Quotes*

> It is to accept that a theory can be used, and its applications understood, without a complete mastery of the detailed structure of the

proof on which it rests. This is not to say that such mastery is of little value or that it need never be attempted, but that there is nothing sacrosanct about any traditional order and sequence in the work of learning and using a theory.

H.R.Pitt. [14]

Proof is beautiful when it gives away the secret of the theorem, when it leads us to perceive the actual and not the logical inevitability of the statement that is proved.

Gian-Carlo Rota [15]

Всеобъемлюще, незыблемо и достоверно.

Венедикт Ерофеев. *Из записных книжек*

1. Роль доказательств в учебной литературе. Традиционно считается, что **все** высказываемые в элементарном учебнике утверждения должны сопровождаться полными доказательствами. Эта норма представляется мне **безнадежно устаревшей, нереалистичной и лицемерной**. В действительности, в большинстве случаев наличие или отсутствие доказательства не влияет на уверенность студентов в справедливости результата. С моей точки зрения, роль доказательств в учебной литературе состоит в следующем:

• Убедить студента в том, что он правильно понимает формулировку.

• Прояснить смысл доказываемого утверждения и его связи с другими утверждениями.

• Отработать общие методы проведения математических рассуждений (индукция, редукция, разбиение на случаи, общее положение, специализация, ...) и стандартные приемы в изучаемой области.

• Выработать привычку к точным рассуждениям вообще и, в первую очередь, вкус к построению сколь угодно длинных цепочек импликаций.

• Воспитать умение отличать предположения от доказательств и правдоподобные догадки от твердо доказанных утверждений.

• Как принято говорить в Кэмбридже†, to illustrate some of the tedium, т. е. создать правильное чувство перспективы и выработать ощущение того, какие доказательства можно провести за несколько минут, а какие могут потребовать нескольких недель.

Ясно, что всем этим целям (кроме, быть может, последней) могут служить только **короткие** и **ясно организованные** доказательства, вскрывающие суть дела. Большинство длинных плохо структурированных или чисто калькулятивных доказательств не только не способствуют этим целям, но *дезориентируют* студента и лишь затемняют смысл доказываемых утверждений. Например, с моей точки зрения, полный абсурд и прямое вредительство приводить в первом семестре чисто вычислительное доказательство теоремы Лапласа о разложении

†*Cambridge Mathematical Quotes*.

определителя на трех страницах, в то время как используя внешнюю алгебру эту теорему можно будет доказать в несколько строк.

2. Общая политика. В настоящем курсе я придерживаюсь следующей политики в отношении доказательств.

• Есть несколько десятков ключевых классических теорем, без которых **невозможно** понимание духа, стиля или исторического развития алгебры и/или которые чрезвычайно важны для ее приложений (теорема Артина—Веддербарна, основная теорема теории Галуа, теорема Гильберта о нулях, теорема Томпсона—Фейта, теорема Оре о кольцах частных, лемма Нетера о нормализации и т. д.) Я придерживаюсь мнения, что все эти результаты должны быть *сформулированы* в **любом** элементарном учебнике алгебры, *независимо от того*, собирается автор их там доказывать, или нет.

• Я стою на точке зрения Бурбаки, что не бывает трудных теорем, а бывают теоремы, которые мы плохо понимаем. Величие математики и залог ее прогресса состоят в том, что для большинства действительно интересных утверждений удается найти такую систему понятий и такой способ рассуждений, при котором они становятся **очевидными**.

• Для многих ключевых теорем, которые традиционно считаются слишком трудными для включения в элементарные курсы (квадратичный закон взаимности, теорема Руффини—Абеля, теорема Фробениуса, ...), в действительности имеются доказательства, занимающие от 5 строчек (для квадратичного закона взаимности) до одной страницы текста. В тех случаях, когда такие доказательства мне известны, я их воспроизвожу.

• В тех случаях, когда мне не известно *короткое* доказательство, доступное пониманию начинающих, или такое доказательство носит чисто технический характер и мне *не хочется* воспроизводить его, я, тем не менее, формулирую результат и сопровождаю его интуитивными соображениями в пользу его справедливости, примерами и приложениями. Впрочем, часто то, что я называю **`интуитивными соображениями`**, в других текстах было бы названо **`доказательствами`** (теорема д'Аламбера).

В том, что касается настоящей книги, это означает следующее. Я формулирую, но не пытаюсь доказывать *десятки* ключевых теорем, существенных для выработки интуиции и правильной перспективы,

• доказательства которых **заведомо** слишком трудны для включения в *любой* элементарный учебник теории групп — таких, скажем, как классификация конечных простых групп, теоремы Томпсона—Фейта, Холла—Хигмена, Новикова—Адяна, Кострикина—Зельманова, Ольшанского;

• которые в принципе вполне могли бы быть доказаны на элементарном уровне, но либо слишком техничны (pq-теорема Бернсайда), либо уводят в сторону от основной линии изложения, так что их включение заметно нарушило бы равновесие;

• которые требуют для своего доказательства соображений, хотя и элементарных, но выходящих за рамки развитого в настоящей книге понятийного аппарата, скажем, привлечения топологии, геометрии или теории представлений (pq-теорема Бернсайда).

С другой стороны, я доказываю не только все стандартные результаты элементарной теории групп, но и много таких, которые обычно в учебниках не доказываются. Как выясняется, для большинства классических результатов, в том числе таких, которые традиционно считаются достаточно трудными, таких как теорема Фробениуса, Anzahlsatz, теорема Шура—Цассенхауза, теоремы Холла, придуманы простые доказательства, занимающие страницу или полторы. В некоторых случаях я привожу даже два или три различных доказательства — а для первой теоремы Силова **пять** различных доказательств — если я считаю, что они вводят новые идеи или иллюстрируют важные технические приемы. В поисках этих доказательств я проштудировал большинство стандартных текстов по теории групп на английском, немецком, французском, итальянском и польском языках, American Mathematical Monthly за последние 50 лет, все выпуски Mathematical Intelligencer, и некоторые другие источники.

§ 8 ♣. Мистический план: текст, контекст и гипертекст

Любой текст — в том числе, конечно, и данный текст — включен в различные более широкие контексты. Особенностью настоящего учебника является попытка **эксплицировать*** возможно большую часть не только чисто математического, но и интеллектуального, технологического, духовного, культурного, исторического, общенаучного, эстетического, магического, мистического, мифологического, религиозного, философского контекстов, в которых происходило — и происходит — развитие математических концепций, и без понимания которых никакое *подлинное* овладение математическими идеями, не только в доктринальных, но даже в простейших фактических, технических и прагматических аспектах невозможно. Поэтому читатель найдет в этой книге необычно большую дозу фольклора, истории, мистики, экзегетики, герменевтики, эсхатологии, оккультизма, — Панург без труда продолжил бы этот список — а также явных и скрытых цитат, намеков, суггестий, реминисценций и заимствований. В отличие от **псилософов*** и

*Тот, кто хочет и дальше читать эту книгу, должен как можно раньше выучить следующие два слова. **Эксплицитный** — явно выраженный или сказанный; **эксплицирование** — уточнение и проговаривание (очевидных) деталей; **эксплицировать** — излагать, объяснять, явно формулировать; **экспликация** — объяснение (процесс и результат); пояснение или разъяснение; развертывание, детальный план. “А я, чтобы избегнуть встречи и экспликаций с нею, чем спуститься с лестницы перестиля, повернул круто направо мимо колонн фасада” — Записки графа М. Д. Бутурлина. **Имплицитный** — содержащийся в скрытом или латентном виде, неявно подразумеваемый, но не произнесенный; **импликация** — логическое следование; следствия, выводы, последствия или результаты высказываний или действий (**все импликации**); подтекст; **имплицировать** — логически влечь; подразумевать, но не произносить, инсинуировать.

*Псилософия — глубокомысленная болтовня с претензией на знание; поверхностное формальное философствование, состоящее в хаотическом повторении плохо переваренных банальностей. В последнее время широкие народные массы интерпретируют термин **псилософия** как сокращение выражения **психоделическая философия**. Все написанное о математике нематематиками, включая Рассела и Витгенштейна, представляет собой типичную псилософию — в любом из указанных смыслов.

большинства логиков, я исхожу из представления, что математика является не просто игрой, состоящей в переписывании значков по определенным правилам, а свободным творением человеческого духа и высшим достижением трезвого человеческого разума. Иными словами, я утверждаю, что математика имеет смысл[♮] не сводящийся к последовательности символов на бумаге.

Никакое обучение математике без раскрытия этого смысла, без формирования соответствующей **ментальности*** и приобщения к трехтысячелетней математической традиции невозможно. Однако математическое сообщество до сих пор **строжайшим образом** придерживается пифагорейского предписания не излагать математические идеи непосвященным. Именно поэтому до сих пор широкая публика считает математику либо напастью и докукой (каковой большая часть школьной математики в той форме, как ее традиционно излагают, конечно, и является), либо разделом теологии, либо — *в лучшем случае* — игрой в бисер. Часто математические книги написаны плохо не потому, что их авторы сами не понимают того, что говорят; не потому, что их авторы не уверены в своем понимании, и не потому, что они демонстрируют чрезмерное глубокомыслие в коммерческих или рекламных целях. Все это, *несомненно*, встречается, и нередко, но в большинстве случаев математические книги написаны плохо все же **абсолютно сознательно** в угоду традиции математической стеганографии: их цель состоит вовсе не в том, чтобы очистить и передать, а в том, чтобы закодировать и скрыть информацию.

Между тем, сегодня нет никакой необходимости *искусственно* поддерживать разделение математики на эзотерические и экзотерические слои. За последние 100–150 лет отрыв не только широких народных масс, но и *так называемых* **образованных людей** от развития математики и математического естествознания приобрел угрожающий и необратимый характер, и сейчас именно этот разрыв, а вовсе не **дивульгация*** математических знаний, представляет собой основную угрозу развитию нашей науки. Философы и псилософы **всех деноминаций*** до сих пор ведут себя так, как будто в математике нет ничего актуальнее теоремы Геделя (или, в рецидивных случаях, парадокса Рассела). Овладеть математическими идеями

[♮]Die Mathematik hat ihren Zweck in Inhalt; ihre Form ist nebensachlich und muss nicht notwendig diejenige sein, die sie historisch geworden ist — Суть математики в ее смысле; ее форма вторична и совсем не обязана оставаться такой, какой она исторически сложилась, [16].

*`Ментальность` — совокупность общих характеристик психики, или более специфично склад ума и умонастроение (= `frame of mind`), определяющие все основные психологические реакции на перцептивном, когнитивном, интеллектуальном, эмотивном и психомоторном уровне. Люди, нечуткие к слову или просто недостаточно владеющие русским языком, часто путают паронимы **ментальность** и **менталитет**. Соотношение между этими словами такое же, как между словами **нейтральность** и **нейтралитет**. Второе из них является юридическим термином и может использоваться только в соответствующих контекстах.

*`Дивульгация` — разглашение, обнародывание, профанация, популяризация.

*`Всех деноминаций` — всевозможные. `Деноминация` — нарицание, акт именования или обозначения; класс, тип или категория объектов, обладающих общим названием и обозначением; религиозная или идеологическая конфессия или секта.

трудно, но не потому, что трудны или недоступны эти идеи — наоборот, математика фундаментально проста!!! С одной стороны, имеется объективная причина, состоящая в том, что наиболее могущественные из этих идей *настолько* глубоки и **версатильны***, что приобщение только к наиболее важным их аспектам даже при самых благоприятных обстоятельствах требует многолетнего упражнения. Но еще большую роль, **имхо**, играет то, что в математической литературе основополагающие идеи, которые являются душой нашего учения, либо вообще не обсуждаются, либо сообщаются в закодированном виде, и могут быть экстрагированы только тем, кто уже полностью владеет предметом. С моей точки зрения, сегодня барьер, преграждающий доступ в мир математических идей, и вступительный взнос для желающего войти в него *настолько* высоки, что продолжать создавать искусственные препятствия абсолютно деструктивно.

Поэтому я абсолютно сознательно отхожу от пифагорейской традиции — *в этой ее части*. Главное, что я стараюсь объяснить в этой книге — генезис и смысл рассматриваемых понятий и результатов. Некоторые мои коллеги полагают, что эти объяснения идут поверх голов начинающих, но я так не считаю. Даже в период острого увлечения позитивизмом я не верил самонадеянному заявлению Виттгенштейна о том, что начинающему не следует говорить то, что он не в состоянии понять. По этой логике с младенцем вообще не следует разговаривать. Если мы и можем чему-то научить наших студентов, так это **только** говоря им вещи, которые они *с нашей точки зрения* пока не в состоянии понять. Поэтому даже новичок (после того, как он овладел некоторым минимумом языка и техники!!) должен смотреть на отступления и комментарии как на неотчуждаемую часть текста, — притом наиболее интересную и важную: *это не отступление его, но само произведение*. Многие из них станут ему понятными — и очевидными!!! — в процессе дальнейших размышлений над предметом и/или знакомства с остальными частями настоящего *произведения* и с другими произведениями на ту же тему.

§ 9 ◇. Практический план: пререквизиты

> Что знаешь, то и считай, что знаешь; что не знаешь, то и считай, что не знаешь. Это-то и есть знание.
>
> *Луньюй*, гл. *Вэйчжэн*

Формально мы не предполагаем, что читатель имеет какую-нибудь подготовку в области математики, включая школьную математику, кроме знания следующих трех платоновских вещей:

- основных алгебраических операций над целыми и рациональными числами;
- декартовых и полярных координат;

---

*Версатильный — пригодный для достижения самых различных целей, гибкий, разносторонний, универсальный; обладающий многими разными аспектами, многосторонний, многогранный; не имеющий постоянной природы, меняющий свой вид и форму, непостоянный, переменчивый, изменчивый.

• основных теоретико-множественных обозначений.

Все остальные понятия, включая вещественные числа, "элементарные" функции и т. д. *где-то* в настоящем курсе нами определяются.

Конечно, **фактически** мы предполагаем у студента некоторый уровень **математической культуры**, который вырабатывается в результате 5–6 лет изучения математики и обычно достигается к окончанию *хорошей* петербургской школы, ну, скажем, такой, как 239, АГУ, ФТШ, 30, 610, АЛ. Предполагаемые нами элементы математической культуры это в первую очередь:

• готовность воспринимать новые понятия;

• способность замечать аналогии между понятиями и утверждениями;

• умение отличать сказанное от подразумеваемого и принимать вещи по номиналу (face value);

• первоначальное знакомство с аксиоматическим методом;

• автоматизм в применении простейших законов логики (если $A \Longrightarrow B$, то $\neg B \Longrightarrow \neg A$; если A и $A \Longrightarrow B$, то B; etc.);

• владение стандартными приемами доказательства (индукция, разбиение на случаи[♭], доказательство от противного, etc.)

• умение строить цепочки из двух–трех импликаций;

• навык следить за длинными цепочками рассуждений;

• умение отличать доказанное от недоказанного;

• привычка к полноте анализа;

• автоматизм алгебраических преобразований[♭];

• умение подставлять выражения в другие выражения[♭]!!!

Никаких других знаний, умений и навыков не предполагается. Основная сложность изучения алгебры на начальном этапе состоит в принципиально более высоком уровне абстракции, необычности языка, весьма значительном количестве определений, которые нужно запомнить, и понятий, которыми нужно овладеть, прежде чем удается сформулировать первые действительно содержательные и волнующие

[♭]Если $A \ \& \ B \Longrightarrow C$ и $A \ \& \ \neg B \Longrightarrow C$, то $A \Longrightarrow C$.

[♭]С точки зрения алгебры речь здесь идет о вычислениях в коммутативных ассоциативных кольцах с 1. Одна из основных целей настоящего курса как раз и состоит в выработке *автоматизма* в проведения вычислений в **некоммутативных** кольцах, таких, как кольца матриц, и в *первом знакомстве* с вычислениями в **неассоциативных** кольцах.

[♭]Важнейший навык! Стандартной для большинства школ является ситуация, когда ученик помнит формулу для решения уравнения $ax^2 + bx + c = 0$, но не в состоянии решить уравнение $pz^2 + qz + r = 0$. Впрочем, эта ситуация типична не только для наших школ: "a simple instance of failing in this is provided by the poll-man at Cambridge, who learned perfectly how to factorise $a^2 - b^2$ but was floored because the examiner unkindly asked for the factors of $p^2 - q^2$" [17].

результаты. Большинство начинающих пытаются запомнить то, что нужно понять, и понять то, что нужно запомнить. Первые 5–6 месяцев студент должен просто верить своим учителям и пытаться переварить **все**, что ему скармливают, понимание придет позже: ALLEZ EN AVANT, ET LA FOI VOUS VIENDRA[♮].

§ 10 ♢. Технический план: COMPUTERS AND TYPESETTING

Artificial intelligence is no match for natural stupidity.

Американская пословица

1. Средний брат. Почти все действующие сегодня учебники алгебры написаны в докомпьютерную эпоху и не учитывают произошедшего за последние 10–15 лет коренного изменения роли компьютеров. Появление в 1940-е и 1950-е годы больших компьютеров мало повлияло на характер и стиль работы большинства математиков, но вот распространение PC изменило их *самым* радикальным образом — раньше математики проводили большую часть рабочего дня мечтательно лежа на диване с листком бумаги и карандашом, теперь они все время что-то сосредоточенно печатают.

Имеются два программных продукта *абсолютно* необходимых для профессиональной работы в области математики и ее приложений, свободное владение которыми стало de facto такой же неотъемлемой частью *ремесла* математика (кроме тех избранных счастливчиков, у которых есть персональные секретарши!), как свободное владение английским языком:

• Системы компьютерного набора, в первую очередь TEX и его диалекты. Я сам привык пользоваться AMS-TEX'ом[♭], но многие из моих

[♮] "On raconte qu'un jeune homme abordant le calcul différentiel y rencontrait des contradictions qui, s'il est mal enseigné, peuvent réelement s'y trouver. Il osa consulter d'Alembert, illustre déjà et, comme disait Diderot, coriphée admiré des sciences mathématiques. La réponse est restée célèbre: allez en avant, la foi vous viendra. Il se réserve d'éclairer chaque page par la lecture de la suivante." — "Рассказывают, что один молодой человек, только начавший изучать математический анализ, столкнулся с противоречиями, которые в анализе действительно встречаются, особенно если его плохо преподавать. Он осмелился обратиться к д'Аламберу, уже весьма известному в то время и, как говорил Дидро, признанному корифею математических наук. Ответ стал знаменит: Идите вперед и вера к Вам придет. Сам он писал так, что каждая страница становится понятной *только* после чтения следующей." [18].

[♭] Читается амстех.

коллег, кто в свое время пожалел потратить месяц на чтение книги Кнута 'Все про TEX', вынуждены ограничиться LaTEX'ом[b].

• Системы компьютерной алгебры, как специализированные: GAP, CoCoA, SINGULAR, MAGMA, Lie, Chevie, etc., так и, в первую очередь, general purpose: AXIOM, Mathematica, Maple.

Настоящая книга полностью набрана в AMS-TEX'е, а *большая часть* примеров в ней вычислена в Mathematica 4 и Mathematica 5 на компьютере по имени Средний Брат. В некоторых случаях я пользовался Maple 9, в дополнениях к которому имплементировано вычисление основных теоретико-групповых функций (порядок группы, центр, коммутант, нормализатор и т. д.) Всюду, где я считал это уместным, я привожу TEX'овские названия математических и типографских символов и короткие программы в Mathematica и Maple, показывающие, как фактически порожден текст настоящего *произведения*. Разумеется, это чисто учебные примеры до порядка 10^5 или 10^6. Вычисления в группах порядка $> 10^9$ проводятся на других компьютерах с использованием профессиональных программных средств.

2. Кегль. В разделах, набранных мелким шрифтом (eightpoint), могут упоминаться концепции и факты, которые не обсуждаются в настоящем курсе, в частности, понятия и теоремы геометрии, топологии, анализа, теории дифференциальных уравнений, теории вероятностей и других разделов математики, а также (реже!) других наук (физики, computer science, кристаллографии, лингвистики, химии, инженерных наук). Части текста, набранные мелким шрифтом, обычно обладают (по крайней мере) одним из следующих достоинств:

• они адресованы квалифицированному читателю,

• они опираются на понятия, которые не обсуждаются в настоящем курсе,

• они носят мировоззренческий, чисто иллюстративный или развлекательный характер.

Эти фрагменты *не используются* в основном тексте набранном шрифтом tenpoint, не входят в обязательную программу и ДОЛЖНЫ БЫТЬ ПРОПУЩЕНЫ начинающим ПРИ ПЕРВОМ ЧТЕНИИ!!

3. Фонт. В *тексте* настоящей книги используются 6 фонтов:

• roman, \rm — для набора основного текста;

---

[b] Читается **латекс**. Кроме того, **латексом** (от итальянского latte — молоко) называется материал, из которого делаются *резиновые изделия*, соски and the like.

• **boldface**, \bf — для набора подзаголовков, рубрик, выделения определяемых **понятий** и **динамического** эмфазиса;

• *slanted*, \sl — для противопоставления различающихся фрагментов формулировок (для *конечной* группы ... для *бесконечной* группы ...) и *смыслового* эмфазиса, особенно внутри выделенного текста;

• *italics*, \it — для выделения формулировок, *интонационного* эмфазиса и — вместо кавычек — как указание на то, что выделенный текст является *названием*, *чужой речью* или *феромоном*;

• typewriter, \tt — для выделения компьютерных команд и программ, торговых марок, диалектных слов и — вместо кавычек — для указания на то, что выделенный текст следует рассматривать as is как факт предметного языка;

• SMALL CAPITALS, \smc — для заголовков разделов, глав и параграфов, колонтитулов, ТЕКСТУАЛЬНОГО эмфазиса (текст, читаемый поверх текста) и — вместо кавычек — как указание на то, что выделенный текст является СЛОГАНОМ, МАГИЧЕСКОЙ ФОРМУЛОЙ или ЗАКЛИНАНИЕМ.

4. Ссылки. В Аппендиксе 3 приведены *две* библиографии, ссылки на которые оформлены по-разному.

• ОСНОВНАЯ БИБЛИОГРАФИЯ адресована студенту и содержит исключительно учебники алгебры и книги по теории групп. В этой библиографии вначале приведены книги на русском (и украинском!) в алфавитном порядке, потом книги на других европейских языках, также в алфавитном порядке. Ссылка на позицию 13 в этом списке производится полужирным шрифтом [**13**].

• РАБОЧАЯ БИБЛИОГРАФИЯ адресована преподавателю и содержит ссылки на другие книги, а также статьи, диссертации, доклады, письма, etc., фактически использованные при работе над книгой. Поскольку большинство этих источников цитируются ровно один раз, они приведены в порядке их появления в тексте. Ссылка на позицию 17 в этом списке производится обычным шрифтом [17].

Ясно, что в тексте такого объема невозможно пользоваться сквозной нумерацией определений, теорем, лемм и пр. С другой стороны, при использовании в электронном виде постраничные ссылки также чрезвычайно неудобны. Технически книга скомпонирована следующим образом.

◦ Текст глубоко структурирован: книги — части — разделы — главы — параграфы — пункты — **айтемы**.

○ Нумерация глав внутри данной части и параграфов внутри данной главы сквозная.

○ Большинство параграфов довольно короткие, обычно всего две–три страницы.

С учетом этих композиционных особенностей ссылки на вводимые понятия и используемые результаты организованы следующим образом. Чтобы сослаться на теорему 7, приведенную в параграфе 103 главы 23 части B книги XII, я пишу что-нибудь в духе `XIIB.23.103, теорема 7`. Разумеется, в пределах одной части указываются только номера главы и параграфа, а в пределах главы — только номер параграфа.

Для удобства навигации в левом колонтитуле указывается номер и название главы, а в правом колонтитуле — номер и название параграфа.

§ 11 ♠. Мистический план в фактических и технических аспектах: Невский диалект

> "And how's the horse doing, that you got from me?" — asked father Hely,
>
> "Ah, he's all right, your reverence," said the farmer, "but for a touch of vernacular."
>
> Lord Dunsany. *My Ireland*

> Я родился и вырос в балтийских болотах, подле
> серых цинковых волн, всегда набегавших по две.
> В этих плоских краях то и хранит от фальши
> сердце, что скрыться негде и видно дальше.
> Это только для звука пространство всегда помеха:
> глаз не посетует на недостаток эха.
>
> Иосиф Бродский. *Часть речи*

1. Невский диалект. Настоящий учебник написан на русском языке, *как я его понимаю*. Кроме нормативного великорусского языка знающий глаз и тренированное ухо легко зарегистрируют в моем **дискурсе*** **пласты** петербургского **койне***,

---

*`Дискурс` — связный текст вместе с сопутствующими экстралингвистическими (психологическими, культурными, прагматическими, доктринальными) аспектами; речь, рассматриваемая как социальный акт или агент коммуникации.

*`Койне` — общий язык, систематически используемый для коммуникации между людьми, принадлежащими к разным культурам, носителями разных языков или диалектов.

шихты василеостровского **вернакуляра***, **формации** математического **арго***, **страты** университетской **кафаревусы*** и спорадические **интарсии** германо-паданского **идиолекта***.

Я родился и учился *между выцветших линий* Васильевского острова и язык, которым я говорю, — это **городской** язык, **Невский диалект***. На диалекте написано *почти* все, что известно как Русская литература. Будучи *фактической* записью моих лекций, эта книга сохраняет большую часть особенностей Василеостровской *разговорной* речи — в том числе непринужденную **инкорпорацию** фрагментов на основных европейских языках: el estilo que tengo me es natural y sin afectación ninguna: escribo come hablo*, wir loben uns wohl den, der so schreibt, daß man ihn sprechen hört, nicht aber den, der so spricht, daß man ihn schreiben sieht*. Разумеется, мой текст *значительно* беднее, чем разговорная речь: от систематического использования китайских, японских, санскритских, арабских, персидских, ивритских слов и речений по типографским и прагматическим причинам пришлось отказаться.

2. Фонетика, морфология, синтаксис. Читатель, не являющийся **автохтоном**, но *до некоторой степени* понимающий русский язык, должен иметь в виду, что большая часть того, что может показаться *ей* ошибкой, в действительности представляет собой Петербургскую норму, **узус***, **токен***, **витц*** или — как в данном случае — **феромон***. Например, я позволяю себе использовать правильные Петер-

---

*Вернакуляр — родной язык, просторечье, разговорный язык или диалект, свойственный данной местности.

*Арго — специальный язык, присущий некоторой культурной, социальной или профессиональной группе, жаргон.

*Кафаревуса — ученый язык, язык образования и науки, в противоположность **димотике** — народному языку.

*Идиолект — индивидуальный язык, присущий отдельному человеку, полностью понятный лишь его непосредственному окружению.

*Город — Санкт-Петербург в границах 1917 года, включающий в себя Васильевский остров, Петроградскую сторону и Центр. **Диалект** — Невский диалект. Уроженцы Города, говорящие на Диалекте, и приравненные к ним называются **автохтонами**. Двое автохтонов, встречаясь в Москве, Хельсинки или Париже: “Ты давно из Города?”, “Скоро обратно в Город?”, “Что нового в Городе?”.

*Мой стиль для меня натурален и лишен какой-либо аффектации: я пишу точно так же, как говорю.

*Мы приветствуем того, кто пишет так, что слышно, как он говорит, а вовсе не того, кто говорит так, что видно, как он пишет.

*Узус — обычай, обыкновение, привычка, традиция; в особенности *общепринятое* употребление слова или выражения, в противопоставлении как нормативному, так и окказиональному использованию. **Узуальный** — использованный в общепринятой форме или значении.

*Токен — символ, знак или метка; указатель, опознавательный знак, бирка, жетон. Нечто, использованнное в символическом, а не прямом значении.

*Витц — bon mot: острота или короткая шутка, состоящая из одного-двух передернутых слов, использованных в необычном значении или неожиданном окружении.

*Феромон — химическая **субстанция**, испускаемая животным (чаще всего на-

бугские формы *множественного* числа (**скаляры**, **векторы**, **тензоры**, **реперы**, **спиноры**, **твисторы**, **профессоры**, **доценты**, **ассистенты**, **лекторы**, **докторы**, **кандидаты**, **аспиранты**, **студенты**, и т. д.), там, где многие **ошибочно** употребляют формы *двойственного* числа (**скаляра́**, **вектора́**, **тензора́**, **репера́**, **спинора́**, **твистора́**, **профессора́**, **доцента́**, **ассистента́**, **лектора́**, **доктора́**, **кандидата́**, **аспиранта́**, **студента́**, и т. д.). Разумеется, я отказался от наиболее **пезантных** морфологических особенностей диалекта таких, как использование латинских и греческих падежных окончаний или иврит-ского множественного числа в заимствованных словах, смысловое согласование, дублирование морфологических показателей, etc. С другой стороны, **иногда -- обыкновенно -- всегда** (вариант: **иногда/обыкновенно/всегда**) я использую петербургскую *интонационную* пунктуацию, в которой тире, двоеточие, скобки и **слэш** используются в десятки раз чаще, чем в академической чисто позиционной манере.

В то же время я, **конечно**, не пытаюсь воспроизвести на письме характерные особенности петербургской **фонации** даже в том, что касается консонантизма: редуп(п)ликация согласных (**серебрянный**, **оффициальный**, **литтература**, **конкурренция**), отсутствие палатализации в иностранных словах (**коррэктный**, **энэргия**, **контэнт**), отсутствие регрессивной ассимиляции, интерполяции (**гластность**, **престный**) и прочее. Что касается особенностей вокализма, таких, как schwa в безударной позиции (там где москвичи произносят *долгие* а или **и**), более сильное динамическое ударение, пролонгация ударных гласных, дифтонгизация, другая степень подъема (закрытое а, открытое о), то их, конечно, вообще невозможно передать средствами стандартного русского письма, без специальных фонетических знаков.

Кстати, это полностью опровергает мнение московских **филолухов** о какой-то особой роли орфографии в выработке петербургской нормы, что, мол, склонные к педантизму петербургские чиновники **европейской национальности** произносили русские слова буква в букву. Географически, антропологически, культурно, идеологически, астрально — и уж, конечно, лингвистически — Санкт-Петербург есть продолжение, или, если угодно, **реинкарнация** Новгородской республики, а Петербургская речь в своих существенных чертах есть сплав севернорусских диалектов. Мы здесь не потому так говорим, что так пишем, а потому так пишем, что *всегда* так говорили.

Но ведь и москвичи, насколько мне известно, не всегда скрупулезно придерживаются на письме норм МХАТ'овского **старамаськовскыва** Bühnenaussprache с его *монструозными артефактами*: **призьма**, **лишность**, **дажьжи**, **вь детьсьтьве**, **каньсьтърюкция**, **булашная**, **дерьматолах** и прочей **сисьтемой Станисьлавскыва**. К счастью, следование нормативной русской орфографии не потребовало от меня *слишком* больших жертв, так как мы и так пишем петербургское **бесконечные**, а не московское **бесканешныя**, петербургское **кто**, а не московское **хто**, петербургское **ходят**, а не московское **ходють**. Непетербуржцу полезно попрактиковаться в том, что при чтении настоящей книги вслух **идемпотент** произносится как **идэмпотэнт**.

3. Лексика. Есть однако область, в которой я гораздо менее склонен идти на

секомым) для того, чтобы воздействовать на других животных *того же вида*: привлечь их внимание, отпугнуть, замедлить их развитие и т. д. Расширительно, любой признак или **дивайс**, работающий по принципу **свой-чужой**, проверяющий реакцию на некоторый раздражитель — или ее отсутствие!! Любая метка, позволяющая *мгновенно* идентифицировать члена какой-то этнической, культурной, языковой, профессиональной или конфессиональной группы или касты, **шибболет**.

компромиссы. Невский диалект является самым богатым языком мира, с **зафиксированным** словарным составом около 6 000 000 слов. **Все** немецкие, латинские, греческие слова **по природе** — и десятки тысяч английских, французских, итальянских, польских, ивритских, шведских, финских, японских, санскритских, персидских, арабских слов **по факту** — вовлекаются в орбиту диалекта и им ассимилируются. Никто не владеет всеми этими 6 000 000 слов **in toto**, но выпускник СПбГУ должен точно, компетентно, стильно, элегантно и *осмысленно* пользоваться *хотя бы* 500 000 из них — which is the master, that's the question. Конечно, я не настаиваю, чтобы все студенты пользовались техническими чисто петербургскими словечками типа **укийо-э**, **моно-но-аварэ**, **дзиммон-кагаку**, **югаке** или **кана-кандзимадзирибун** — или, на другом *версанте*, **шлюсс**, **шмельц**, **ферзихерунг**, **фортраг**, **вельтаншауунг**, **гештальт**, **культурворт**, **уеберзетцунг**. Однако в последние годы я с удивлением обнаружил, что приехавшие из других мест студенты не понимают или неправильно истолковывают *тысячи* простейших слов, — причем не только собственно диалектных, но и таких, которые основательно вошли в конституцию русского языка, слов **витальных** для точного выражения **визии** и спекулятивной мысли. Таких, скажем, как аватара, инкарнация и реинкарнация, референтный и автореферентный, релевантный и иррелевантный, инверсный, латеральный и коллатеральный, инволютивный, транспозиция, трансверсальный, эксплицитный и имплицитный, экстенсиональный и интенсиональный, алиас, альтернатива, гетерогенный, робустный, драстичный, брутальный, дихотомия и трихотомия, аддитивный и мультипликативный, инфиксный, префиксный, постфиксный и циркумфиксный, анафорический и катафорический, эзотерический и экзотерический, парафраз и перифраза, оксюморон, суггестивный, энантиоморфизм, эмулировать, эссенциальный, циркумспекция, инкремент и декремент, имманентный†, etc., etc., etc. Отказаться от использования *таких* слов как терминов или как неотъемлемых элементов авторской речи иногда — обыкновенно — всегда значило бы выхолостить язык, отступить от **аутентичности**, художественности, точности и правды. Это разрушило бы саму ткань повествования. Поэтому, чтобы облегчить чтение этой книги друзьям степе[не]й *по всей Руси великой*, я сопровождаю некоторые слова **маргинальными*** **глоссами***. В то же время в процессе редактировании конспекта я сознательно, хотя и не без некоторого сожаления, **элиминировал** большую часть **квели**, т. е. собственно диалектных слов немецкого, скандинавского, польского и финского происхождения, которые вне конкретной языковой ситуации и соответствующих **кинем*** могут быть поняты *исключительно* автохтоном.

4. Чужая речь. В большинстве учебников **вся** речь чужая, поэтому их авторам не нужны какие-то особые средства для выделения *чужой речи*. В предлагаемой

---

† ... мандрагоры имманентные зашуршали в камышах ...

***Маргинальный** — написанный на полях книги или рукописи, не интегрированный в основную тематику, находящийся на краю сознания или культуры.

***Глосса** — перевод или толкование **вокабулы**, редкого, специального, диалектного или устаревшего слова или выражения, помещенные непосредственно в основном тексте книги или на полях.

***Кинема** — жест, движение, поза, гримаса, сопровождающие речь с целью усиления, дополнения, замены или пояснения какого-то ее фрагмента; невербальная часть коммуникации.

книге вся речь моя. Чтобы избежать **аподиктичности***, я гораздо чаще, чем это принято в математической литературе, обращаюсь к явному и *неявному* цитированию. Его роль, в частности роль эпиграфов, состоит в следующем:

• поставить изложение в более широкий культурный, исторический или научный контекст;

• создать иронический фон, парадоксальный контрапункт или яркий контраст, способствующие лучшему пониманию и/или запоминанию;

• выразить точку зрения противоположную, альтернативную или **комплементарную** моей собственной;

• выразить точку зрения **синтоничную** моей собственной, входящую с ней в резонанс или усугубляющую ее.

Согласно митьковской эстетике ХОРОШАЯ КНИГА МОЖЕТ СОСТОЯТЬ ИЗ ОДНИХ ТОЛЬКО, С УМОМ ПОДОБРАННЫХ, ЭПИГРАФОВ, *так точно они выражают первоначальные намерения автора*.

5. Языковая политика. Большая часть математической литературы сегодня — вероятно процентов 80 или 85 — печатается на английском языке. ТОМУ, КТО НЕ ЗНАЕТ АНГЛИЙСКОГО, НЕЗАЧЕМ УЧИТЬСЯ МАТЕМАТИКЕ. Поэтому я не только не делаю никаких попыток переводить *что бы то ни было* с английского, но и систематически знакомлю читателя с английской алгебраической терминологией. При этом я всюду придерживаюсь исключительно нормативной БРИТАНСКОЙ орфографии♮.

Труднее решить, до какой степени уместно предполагать, что все потенциальные юзеры этого трактата бойко шпарят по-немецки. Почти вся классическая алгебраическая литература конца XIX и начала XX века — когда была доказана большая часть результатов, вошедших в настоящий курс — написана на немецком. Большая часть традиционной русской математической терминологии калькирована с немецкого. БЕЗ РАБОЧЕГО ЗНАНИЯ НЕМЕЦКОГО НЕВОЗМОЖНО НИКАКОЕ ПОНИМАНИЕ КЛАССИЧЕСКОЙ АЛГЕБРЫ В ЕЕ ИСТОРИЧЕСКОМ РАЗВИТИИ. Поэтому в электронной версии этой книги все немецкие тексты тоже были оставлены без перевода. Однако в ответ на неоднократные обращения **пациентов** в настоящей публикации воспроизводятся как немецкий оригинал, так и русский перевод. Кроме того, многие классические теоремы приводятся под традиционными немецкими названиями, в особенности, в тех случаях, когда они систематически цитируются под этими названиями в англоязычной литературе: `Isomorphiesatz`, `Nullstellensatz`, `Basissatz`, `Freiheitssatz`, `Indexsatz`, `Anzahlsatz`, usw.

---

*__Аподиктичный__ — не допускающий возражений, категоричный, навязывающий свои взгляды, мнения и вкусы как единственно правильные или возможные; **аподиктический** — категорический, обладающий характером (или видимостью!) необходимости.

♮Это сделано не потому, что сам я ориентируюсь в своей речи на Кэмбридж и Уорик, а из прагматических соображений. Получить из правильной английской формы `centre`, `colour`, `analogue`, `through`, `you`, ... ее американский каунтерпарт `center`, `color`, `analog`, `thru`, `u`, ... обычно довольно просто. Обратное преобразование не всегда очевидно.

Как правило, без перевода даются *короткие* фразы на французском, итальянском, испанском и латыни, — **скерцы**, **экскламации**, стишки, оперные арии, проклятия, ecc. — которые **смешно** переводить (типа *allez en avant*, *brutta ora il mattino*), так как они понятны сами по себе. Все остальные тексты приводятся исключительно в русском переводе.

§ 12 ♠. Практический план: генезис

Нет, в Петербурге институт
Пе-да-го-гический, так, кажется, зовут:
Там упражняются в расколах и в безверьи
Профессоры!!

А. С. Грибоедов. *Горе от ума*

I feel quite certain now that had it not been for the two hundred and fifty bed patients whom he was obliged to visit twice a day at the hospital of Lyons, Rabelais would never have been so boisterously gay, I'm sure of it.

Henry Miller. *Black spring*

Ни одна книга не была написана усилиями одного человека. Я не могу перечислить всех поименно — *слишком* многие относились ко мне с расположением.

Carl Faith. **[185]**

1. Wo kommen wir her. Самуил Давидович Берман вспоминал, как он после войны, вместе с другими фронтовиками, вернулся в МГУ. На первый студенческий вечер они пришли в чем было: в гимнастерках и сапогах. На том же вечере Есенин-Вольпин в галстуке-бабочке читал стихи под названием "Шизофрения". "На нас, со здоровой фронтовой психологией, это произвело большое впечатление".

Я родился и рос в среде физиков и инженеров. Фляжки Дьюара с жидким азотом, в которые можно было засунуть палец — или кусок пластилина.

В возрасте пяти лет между мной и незнакомым дядей состоялся следующий диалог: Ты физик? — нет. Ты химик? — нет. Ты инженер? — нет. Так что же ты делаешь???

Как известно, история имеет тенденцию повторяться. Когда среди наших друзей появились врачи, художники, юристы, музыканты, продуценты вина и люди других профессий, этот диалог повторился один в один, но взрослым дядей на этот раз был я: Ты танцуешь? — нет. Ты поешь? — нет. Ты играешь на рояле? — нет. Так что же ты делаешь???

Без всякой фанаберии и озорства, а просто для полноты сформулирую несколько очевидных фактов. Разумеется, с опытом преподавания я утратил иллюзию, что все очевидное мне очевидно всем остальным: ce que l'un voit, l'autre ne le voit pas.

• У человечества не было и нет ничего более полезного и ценного, чем математика и математическое естествознание.

• Открытие квантовой механики, наряду с изобретением письма, является самым важным из всего до сих пор произошедшего в истории человечества.

• Уровень развития общества измеряется уровнем его математики. Полезность любых этических, религиозных, социальных, политических или экономических взглядов и систем следует оценивать исключительно по этому параметру.

• Мы живем в мире, который создан математиками и физиками.

• Математика *только* потому полезна физикам и другим ученым, что она не является физикой.

Если бы заявление Арнольда о том, что математика есть часть физики, не было задумано как эпатаж, оно было бы чудовищной глупостью. Математика организована как наука. Однако, математика не является наукой, поскольку ее установки, процедуры верификации и фальсификации, критерии ценности ближе к искусству или религии, чем к науке. Конечно, *изначально* тождество Якоби есть экспериментальный факт. Но математик преобразует этот экспериментальный факт в нечто, перестающее быть экспериментальным фактом.

Для того, чтобы продолжать оставаться по-настоящему полезной, математика должна сохранять свою специфику. Однако, я абсолютно не понимаю, каким образом сохранение специфики математики требует написания плохих, ужасных, чудовищных — и откровенно монструозных — учебников.

"Нет ничего более отталкивающего для нормального человека, чем клиническая последовательность определений, аксиом и теорем, порождаемая трудами чистых математиков." [19].

Ричард Фейнман [2]

Ашкрофт—Мерман **[15]**

Андронов— Витт—Хайкин [20]

Ватсон, Бесселевы функции [21]

Янг [22]

Арнольд [23]

Дубровин—Новиков—Фоменко **[81]**

Эта книга возникла из желания, чтобы математические учебники было бы так

2. Мои университеты. Фактически книга основана на следующих основных источниках, в порядке убывания их влияния на характер изложения.

• (Слегка) расширенный конспект общего курса алгебры для студентов (1-й, 2-й и 3-й семестры) ♢, ♡, которые я читал на математико-механическом факультете Санкт-Петербургского Университета начиная с 1981 года. Основная часть книги является фактической записью лекций по алгебре для специальности **прикладная математика** 1997/1998, 1999/2000, 2001/2002 и 2003/2004 годов. Начиная с 1999 года различные версии этого конспекта циркулировали среди студентов в электронном виде. Кроме того, включены фрагменты из конспекта моих лекций 2001 и 2002 годов по истории математики (4-й семестр) ♡.

• Записи нескольких чуть более специальных тем, которые не входили в общий курс, но рассказывались дополнительном интенсивном курсе алгебры ♡, ♠, который я в 1998–2000 и 2002–2004 годах читал в **ПОМИ-группе** математико-механического факультета по специальности **математика** (2-й и 3-й семестры). В

курсе для ПОМИ-группы производилось осторожное, но консеквентное переключение с теоретико-множественного языка на теоретико-категорный.

• Записи специальных курсов ♠, ♣, ✠ по конечным группам, линейным группам, классическим группам, алгебраическим группам, группам Шевалле, группам Ли, группам отражений, арифметическим группам, теории представлений, образующим и соотношениям, и т. д. для студентов старших курсов, специализирующихся в **алгебре и теории чисел**, которые я читал в Санкт-Петербургском университете начиная с 1979 года (кроме тех лет, когда я читал курсы по алгебрам Ли, алгебрам Хопфа, теории колец, алгебраической геометрии, полилинейной алгебре, алгебраической K-теории или неассоциативным алгебрам), и *в особенности* курсов 1979, 1982/1983, 1999 и 2003/2004 годов, посвященных теории конечных групп, представлениям конечных групп и классификации конечных простых групп.

• Записи аспирантских курсов ♡, ♠, ♣, ✠ по теории алгебраических групп, теории групп Шевалле, алгебраической K-теории, копредставлениям групп, теории представлений, классификации конечных простых групп и т. д., которые я последние 15 лет читал в различных университетах, включая Notre Dame, Университет Крита в Ираклионе, Университеты Милана (Città Studi и La Bicocca) и Падуи, Universitaire Instelling Antwerpen, SISSA, Northwestern, Харбинский технологический институт и другие.

• Тексты миникурсов ♣, ✠ colloquium talks ♠, ♣ и обзорных докладов ♣, ✠ на семинарах в различных университетах и научных учреждениях, в особенности в ПОМИ, Московском ун-те, Киевском ун-те, ИМ АН Белоруссии, Нижегородском ун-те, Uni Bielefeld, Uniw. Wrocławskim, Uniw. Warszawskim, Politechnice Śląskiej, Warwick Univ., ун-те и Ньютоновском ин-те Cambridge, Penn State, Yale, Caltech, U. Chicago, U. Virginia, U. Oregon, Univ. California at Santa Cruz, Univ. Zürich, ун-те Цукуба (Токио), Paris VII и Paris XIII, Бар Илане (Рамат-Ган), ун-те Бен Гуриона (Беер-Шева), Еврейском ун-те Йерусалима, ин-те Вайцмана (Реховот), Технионе (Хайфа), ун-те Тель Авива, Univ. Libre Bruxelles, Univ. Roma I La Sapienza, Univ. Roma II Tor Vergata, Univ. Firenze, Scuola Normale Superiore (Pisa), Univ. Siena, Univ. Brescia, Univ. Trento, Univ. l'Aquila, Univ. Trieste, Univ. Napoli, Univ. Genova, Univ. Birmingham, Univ. Southampton, Univ. Manchester, Univ. Newcastle/Tyne, UEA Norwich, Univ. Utrecht, TU Eindhoven, Univ. Amsterdam, Univ. Limburg, Univ. Trondheim, Univ. Bergen, Uni Heidelberg, Uni Giessen, RWTH Aachen, Uni Essen, Humboldt Univ. Berlin, Max-Planck AG Berlin, Uni Frankfurt, Uni Halle, Uni Mainz, Uni Erlangen—Nürnberg, Uni Regensburg, Uni Würzburg, Uni Hamburg, TU München, Academia Sinica в Пекине, Нормальном ун-те Шанхая и многих других, а также обзорных лекций и докладов на различных конференциях и школах.

Почти все представленные здесь доказательства (кроме, кажется, теоремы Ландау о группах с m классами сопряженных элементов и теоремы Диксона) за последние 25 лет хотя бы однажды рассказывались мной в аудитории. Я благодарен всем слушателям — студентам, аспирантам и коллегам — в особенности тем, кто предоставлял мне конспекты лекций (часто с небанальными дополнениями и/или комментариями!), без чего написание этой книги было бы невозможным.

3. Friends and relations. В 30-й школе у меня были лучшие учителя, о которых можно мечтать, особую любовь, благодарность и восхищение я испытывал тогда — и испытываю сейчас — к Иосифу Яковлевичу Веребейчику и Михаилу Льво-

вичу Шифману. Если я не пошел по предначертанному пути, а стал вместо этого математиком, то главным образом под влиянием Иосифа Яковлевича и Николая Григорьевича Чудакова.

Я был очень ленивым студентом и прослушал всего два общих курса, курс алгебры Дмитрий Константинович Фаддеев, и курс топологии Владимир Абрамович Рохлин.

Зенон Иванович Боревич,

Анатолий Николаевич Андрианов, Марк Иванович Башмаков, Борис Борисович Венков, Анатолий Моисеевич Вершик, Сергей Владимирович Востоков, Александр Васильевич Малышев, Александр Иванович Скопин, Анатолий Владимирович Яковлев,

Александр Генералов, Николай Гордеев, Сергей Евдокимов, Владимир Койбаев, Вячеслав Копейко, Сергей Крупецкий, Александр Меркурьев, Сергей Нагорный, Иван Панин, Евгений Плоткин, Александр Смирнов, Андрей Суслин,

Олег Ижболдин, Марат Туленбаев,

Много старших Самуил Давидович Берман, Лев Аркадьевич Калужнин, Алексей Иванович Кострикин, Дмитрий Алексеевич Супруненко,

Энест Борисович Винберг, Александр Ефимович Залесский, Александр Васильевич Михалев, Борис Исаакович Плоткин,

Сергей Иванович Адян, Артамонов, Юрий Бахтурин, Леонид Аркадьевич Бокуть, Валентин Евгеньевич Воскресенский, Юрий Анатольевич Дрозд, Борис Анатольевич Дубровин, Владимир Васильевич Кириченко, Латышев, Виктор Данилович Мазуров, Людмила Александровна Назарова, Александр Юрьевич Ольшанский, Владимир Петрович Платонов, Андрей Владимирович Ройтер, Альфред Львович Шмелькин

В советское время нас не пускали за границу, зато мы довольно часто ездили внутри страны.

так и моим коллегам и друзьям из Москвы, Минска, Киева, Екатиренбурга, Новосибирска, Омска, Кемерово и Риги, в первую очередь Евгений Башкиров, Бондаренко, Александр Боровик, Михаил Волков, Самуил Вовси, Виктор Герасимов, Игорь Голубчик, Зархин, Ефим Зельманов, Борис Зильбер, Александр Иванов (Лондон), Александр Иванов (Вроцлав), Михаил Клин, Анатолий Кондратьев, Игорь Кострикин, Красильников, Борис Кунявский, Василий Логинов, Григорий Маргулис, Александр Махнев, Михаил Милованов, Мясников, Геннадий Носков, Овсиенко, Александр Премет, Андрей Рапинчук, Николай Романовский, Виталий Романьков, Алексей Рудаков, Сергейчук, Григорий Сойфер, Ирина Супруненко, Виталий Сущанский, Сергей Сыскин, Василий Устименко, Виктор Уфнаровский, Владимир Черноусов, Сергей Царанов, Сергей Шпекторов, Вячеслав Янчевский.

Вальдемар Голубовский, Алексей Степанов, Владимир Нестеров, Алексей Бондаренко, Максим Всемирнов, Александр Панин,

Олег Богопольский, Евгений Вдовин, Ваган Микаэлян,

Я слушал доклады и обсуждал разные аспекты теории групп с сотнями коллег. Часто мне трудно судить, что из оценок Особенно большое влияние оказало на меня общение с Эйичи Абе, Герберт Абельс, Амберг, Шимшон Амицур, Хеннинг Андерсен, Майкл Ашбахер, Ева Байер, Энтони Бак, Франческо Бальдассарри, Хельмут Бер, Роджер Брайант, Рональд Браун, Франсис Бюкенхаут, Томас Вайгель, Фред Ван Ойстайен, Питер Габриэль, Норберто Гавиоли, Марсель Герцог, Карл Грюнберг, Роберт Гуральник, Франческа Далла Вольта, Джованни Дза-

кер, Коррадо Де Кончини, Кит Деннис, Димитрис Деризиотис, Дональд Джеймс, Франческо де Джованни, Гарет Джонс, Лино Ди Мартино, Драгомир Дьокович, Гари Зейтц, Йоханнес Зимонс, Дэвид Зингерман, Поль Жерарден, Карло Казоло, Вильберд ван дер Каллен, Уильям Кантор, Андреа Каранти, Роджер Картер, Макс Каруби, Отто Кегель, Оливер Кинг, Джон Конвей, Дуглас Коста, Мауро Костантини, Арье Коэн, Хельмут Кох, Валентино Кристанте, Брюс Куперстейн, Ли Шангчжы, Мартин Либек, Александр Любоцкий, Андреа Луккини, Кей Магаард, Томас Майкснер, Гунтер Малле, Авиноам Манн, Федерико Менегаццо, Йенс Меннике, Герхард Михлер, Джун Морита, Франко Наполетани, Майкл Ньюмен, Иоахим Нойбюзер, Питер Нойман, О.Т.О'Мира, Антонио Пазини, Крис Паркер, Клаудио Педрини, Черил Прегер, Клаудио Прочези, Мохан Путча, Амитай Регев, Ульф Реман, Герхард Рёрле, Клаус Рингель, Джофри Робинсон, Герхард Розенбергер, Марк Ронан, Маркус Рост, Луи Роуэн, Ян Сакс, Йов Сегев, Джордж Селигман, Луиджи Серена, Кристиан Скау, Карло Скоппола, Леонард Скотт, Стив Смит, Рональд Соломон, Майкл Стейн, Эйвинд Стенсхольт, Кьяра Тамбурини, Танг Гуопинг, Франц Тиммесфельд, Жак Титс, Джон Уилсон, Роберт Уилсон, Эндрю Уолдар, Уоррен Уонг, Уолтер Фейт, Бернд Фишер, Шмуэль Фридланд, Эрик Фридландер, Роозбех Хазрат, Хайнекен, Александер Хан, Брайан Хартли, Хайнц Хеллинг, Джонатан Холл, Роберт Хоулетт, Пьер Витторио Чеккерини, Чен Ю, Анер Шалев, Рудольф Шарлау, Лионель Шварц, Бернд Штелльмахер, Гернот Штрот, Эрнест Шульт, Брент Эвериттт, Эрих Эллерс, Ю Хонг, Янцен. Во время прогулок по улицам Кембриджа, Милана и Парижа, в поездах и самолетах, во время поездки по автобану Милан—Венеция, в пабах, барах, кафе и ресторанах.

Андре Вейль, Например, в Уорике я делил офис с Джорджем Люстигом, Я говорил один-два раза, Хайман Басс, Арман Борель, Джон Милнор, Бернард Нойман, Жан-Пьер Серр, Тонни Спрингер,

Значительную часть 3-го тома рассказал мне Джон Конвей во время наших прогулок по Милану и Брессаноне, в холлах гостиниц, ресторанах и закусочных, и записана на упаковках от пиццы. Во время прогулок по Киото мы с Мичио Судзуки говорили в основном о японской истории и искусстве (хотя и о математике тоже), а с Бертрамом Хуппертом вообще обсуждали исключительно итальянскую живопись и Гриммельсхаузена ("zum Heldentod war ich nicht bereit"). Тем не менее, после знакомства с ними я стал вдруг гораздо лучше понимать их книги.

При подготовке этой книги я использовал конспекты моих коллег и учеников, слушавших мои курсы в разные годы, в частности, Иоанниса Антодиадиса, Алекса Факиоласа, Карлы Бардини, ..., Виктора Петрова, Николая Дурова, Леонида Полторака, Николая Харчева, Евгения Горячко,

Несколько моих питерских друзей и коллег внимательно прочли весь текст книги, заметили сотни опечаток и предложили десятки улучшений. В первую очерель это Максим Всемирнов, Елизавета Дыбкова, Борис Бениаминович Лурье, Виктор Петров, Константин Пименов, Алексей Степанов и Роберт Шмидт, предлагавшие исправления в текст в процессе его возникновения, а также Николай Гордеев и Иван Панин, рецензировавшие окончательный текст книги.

Особую роль в появлении этой книги сыграли два человека, Владимир Халин, который много лет убеждал меня превратить записки моих лекций в серию книг, и Андрей Семенов, который как редактор этой книги предложил сотни математических, методических, лингвистических и типографских улучшений. Единственное, в чем он пока не смог меня убедить — в преимуществах LaTeX'а перед AMS-TeX'ом.

Поэтому при подготовке макета этой книги я использовал написанный Алексеем Степановым пакет `alexei.ref`, который моделирует обычные LaTeX'овские **гаджеты** и **виджеты**, но при этом полностью сохраняет привычный AMS-TeX'овский синтаксис и возможность контроля над форматированием текста на микроуровне.

И, конечно, я благодарен Оле и Саше за терпение, с которым они ...

§ 13 ♢. Астральный план: smile of smiles

> Всякое суждение должно обладать тремя измерениями. Что же называется тремя измерениями? Учитель Мо Ди так отвечает на этот вопрос: "Три измерения суть обоснованность, проверяемость и применимость".
>
> Мо-цзы. *Фэймин*, ч.1

> Три вещи, познание которых уничтожает Зло и Смерть и дает победу над ними: Знание сущности вещей; Знание их причин; Знание способа их действия. И это знание будет достигнуто в Гвинфиде.
>
> Триады бардов.

> Probability is a mathematical discipline whose aims are akin to those, for example, of geometry or analytical mechanics. In each field we must carefully distinguish three aspect of the theory:
> (a) the formal logical content,
> (b) the intuitive background,
> (c) the applications.
> The character, and the charm, of the whole structure cannot be appreciated without considering all three aspects in their proper relation.
>
> William Feller. [24]

> Всякий предмет (неодушевленный и созданный человеком) обладает четырьмя рабочими значениями и пятым сущим значением. Первые четыре суть: 1) начертательное значение (геометрическое), 2) целевое значение (утилитарное), 3) значение эмоционального воздействия на человека, 4) значение эстетического воздействия на человека. Пятое значение определяется самим фактом существования предмета. Оно вне связи предмета с человеком и служит самому предмету. Пятое значение — есть свободная воля предмета. Человек, вступая в общение с предметом, исследует его четыре рабочих значения. При помощи их предмет укладывается в сознании человека, где и живет. Если бы человек натолкнулся на совокупность предметов только с тремя из четырех рабочих значений, то перестал бы быть человеком.
>
> Даниил Хармс. *Предметы и фигуры, открытые Даниилом Ивановичем Хармсом*

Изложение в этой книге несколько необычно. Чтобы быть математиком, нужно понимать, знать, уметь и мочь. Иными словами, математика существует одновременно на четырех уровнях: **мистическом**, **фактическом**, **техническом** и **практическом** — или, как сказали бы древние, в четырех стихиях (началах alias элементах): плане огня, плане земли, плане воды и плане воздуха. Профессиональный математик знает, что только гармония всех планов приводит к математике большого стиля.

В то же время подавляющее большинство учебных текстов концентрируются исключительно на фактическом плане, сообщают не знания, а информацию, притом неточную и устаревшую! Я бы охарактеризовал это занятие как exercise in futility. Математика, как говорит ее название, является доктриной и корпусом знаний (body of knowledge) — но вовсе не владение доктриной и корпусом знаний делает человека математиком. Нельзя знать математику, но можно **быть** математиком. Быть математиком означает, в первую очередь, видеть, обладать сверхзрением, позволяющим смотреть сквозь стены и поверх барьеров — *E chi ha gli occhi nella fronte e nella mente*.

Основными инструментами понимания являются аналогия и метафора, контраст и сопоставление. При этом явления в простой и полностью понятной нам области, такой, скажем, как квантовая механика (квантование, туннельный эффект, принцип неопределенности, принцип дополнительности, воздействие наблюдателя на объект и т. д.) могут служить метафорой параллельных им явлений в психологии или лингвистике. Общекультурная роль математики и ее прикладное значение основаны на том, что математика в силу общности, гибкости, точности, широты и экспрессивности своего языка, может служить метафорой всему на свете. Но это можно прочесть и в обратном направлении: **все на свете** — любое явление, любой предмет, любое понятие, встречающиеся в природе, быту, науке, искусстве, игре — может служить материалом для мотивации, кристаллизации или объяснения математических идей и конструкций.

Нельзя заставить понять, как нельзя научить видеть. Можно, однако, подвести ученика к перекрестку, где путь неба сходится с путем земли и путем человека, и сказать — **смотри!** Красота в глазу смотрящего.

Erwirb es, um es zu besitzen.

Goethe. *Faust* I

Раздел I. ОСНОВЫ ТЕОРИИ

$\Big\{$Groups, Groups, {and more Groups}$\Big\}$

Michael Doob. *A gentle introduction to TEX*

В настоящем разделе, занимающем примерно 2/5 всего текста книги, вводятся основные понятия теории групп: группы, абелевы группы, подгруппы, смежные классы, двойные смежные классы, трансверсали, порядок и индекс, порождения, системы образующих, циклические группы, порядок элемента, классы сопряженных элементов, нормальные и субнормальные подгруппы, фактор-группы, гомоморфизмы, образ и ядро, изоморфизмы, автоморфизмы, характеристические подгруппы, внутренние автоморфизмы, нормализаторы и централизаторы, нормальные и субнормальные ряды. Все эти понятия носят общий характер и *неизбежно* возникают даже при самом поверхностном обсуждении групп. Кроме того, мы доказываем некоторые фундаментальные факты. Здесь — в отличие от дальнейших разделов! — нет ни одной действительно трудной теоремы. Впрочем, тут доказано несколько *исключительно важных* простых теорем: теоремы о гомоморфизме и изоморфизме, теоремы о соответствии, классификация циклических групп и их подгрупп, теоремы Лагранжа и Пуанкаре, формула произведения и формула индекса Фробениуса, теоремы Шрайера и Жордана—Гельдера и т. д., все эти результаты *постоянно* используются в дальнейшем.

Наряду с абсолютным минимумом основных понятий и простейших фактов здесь приводится изрядное количество примеров и иллюстративного материала — вероятно, раз в десять больше, чем принято в учебниках сопоставимого уровня — а также, начиная с главы 2, большое количество несложных задач. Значительная часть этих примеров носит факультативный характер, и совершенно не обязательно разбирать их все. Важно однако, чтобы новичок детально продумал хотя бы *некоторые* из них. Это абсолютно необходимо для выработки мысленных образов, при помощи которых он мог бы отчетливо осознавать смысл вводимых в дальнейшем более сложных понятий.

В целом изложение этого материала в общем курсе занимает обычно 3–4 лекции и, соответственно, даже самый слабо подготовленный

студент должен быть в состоянии прочесть первые 4 главы — пропуская параграфы с метками ♠, ♣ и ✠ и не решая задачи — за день или два. Однако если материал этих глав является для него новым, после этого, прежде чем переходить к дальнейшим разделам, следует потратить еще день или два на `рекапитуляцию`, разбор примеров и решение задач.

Глава 1. ГРУППЫ

> На вопрос "Что такое животное?" лучше всего отвечает прогулка по зоопарку.
>
> Джордж Гретцер. [25]

В этой главе мы вводим понятие группы и приводим первые примеры групп. Не предполагается, что начинающий поймет все эти примеры при первом чтении, они служат только для того, чтобы показать, что группы возникают в математике в **сотнях** различных контекстов и по самым разным поводам. Кроме того, эта глава служит миниатюрной моделью всей книги в целом. Здесь нам впервые встретится несколько тем (действия групп, конструкции над группами, образующие и соотношения, классификация различных типов групп), которые потом будут сопровождать нас на протяжении всей книги и которым посвящены большие главы или разделы. Несколько параграфов носят чисто ознакомительный характер, их цель — показать роль групп в алгебре и за ее пределами и указать на различные обобщения понятия группы. Содержание этих параграфов будет раскрыто в книгах III и IIbis.

§ 1◇. Группы

Здесь мы введем одно из центральных понятий всей математики.

1. Группы. Моноид, все элементы которого обратимы, называется группой. Ввиду крайней важности этого понятия повторим это определение в деталях.

Определение. *Непустое множество G называется* **группой**, *если на нем задана*[♮] *бинарная операция $G \times G \longrightarrow G$, $(x, y) \mapsto xy$, обладающая следующими тремя свойствами:*

[♮]Здесь у нас с Робертом Шмидтом каждый раз возникает одна и та же долгая метод(олог)ическая дискуссия на тему `множество на котором` versus `множество вместе с`. С моей точки это не имеет никакого значения и я давно не обращаю внимания на подобные пустяки: того, кто не в состоянии по одному углу предмета составить представления об остальных трех, не следует учить.

G1. Ассоциативность: $(xy)z = x(yz)$ *для любых* $x, y, z \in G$;

G2. Существование нейтрального элемента: *существует* $e \in G$ *такой, что* $xe = x = ex$ *для любого* $x \in G$;

G3. Существование обратного элемента: *для любого* $x \in G$ *существует обратный элемент* $x^{-1} \in G$ *такой, что* $xx^{-1} = e = x^{-1}x$.

Бинарная операция на G, превращающая G в группу, называется **групповым законом**. Мощность $|G|$ группы G обычно называется ее **порядком**. Группа G, содержащая конечное число элементов, называется **конечной**. В противном случае группа G называется **бесконечной**.

Определение. *Говорят, что элементы* x *и* y *группы* G **коммутируют**[♮], *если* $xy = yx$. *Группа, в которой любые два элемента коммутируют, называется* **коммутативной** *или* **абелевой**.

Иными словами, в абелевой группе в дополнение к аксиомам G1 – G3 выполняется аксиома

G4. Коммутативность: $xy = yx$ *для любых* $x, y \in G$.

Абелевы группы названы так в честь Нильса Абеля, который доказал разрешимость в радикалах уравнений с абелевой группой Галуа. Абелевы группы обычно записываются аддитивно, так что вместо xy

---

Как учат великие мудрецы древности, передача математических знаний возможна только от сердца к сердцу (**син-син-мей**), слова здесь играют чисто служебную роль. Студент должен слушать, то, что я думаю, а не то, что я говорю. При этом он либо понимает то, что я *хочу* сказать, либо не понимает. Это не зависит ни от того, что говорится, ни от того, как это говорится, а только от наличия или отсутствия ментального контакта, синхронизации наших сознаний, подсознаний и гиперсознаний. Ничто не в состоянии изменить этот фундаментальный факт. Поэтому *никакие* методические ухищрения и просчеты не в состоянии повлиять на уровень не/понимания в ту или другую сторону. Роберту кажется, что *ритуальные пляски* могут изменить это положение, но я так не считаю. Кроме того, если уж называть группу парой, то нельзя обозначать группу и множество, на котором она задана, одной и той же буквой, а нужно писать что-нибудь в духе $\mathfrak{G} = (G, \cdot)$ — разумеется, наиболее буйные общие алгебраисты именно так и поступают! Запись $G = (G, \cdot)$ явно противоречит аксиоме регулярности. Кроме того, дальше мы все время говорим об **элементах группы**, а какие уж там у группы элементы, если она является упорядоченной парой! Ну и, в конце концов, если уж **вместе с**, то вместе с **тремя** операциями, о чем следующий параграф. Поэтому я без колебаний сохраняю свою первоначальную редакцию.

[♮]Специалисты по комбинаторной теории групп в этом случае используют обозначение $x \quad y$, однако нам оно не кажется настолько более удобным, чем обычная запись $xy = yx$ или $[x, y] = e$, чтобы оправдать введение специального символа.

пишется $x+y$, 0 вместо e и $-x$ вместо x^{-1}. Термин **абелева группа** в этом смысле был впервые употреблен в 1882 году Генрихом Вебером [26]. Тем не менее, следуя Жордану, Диксон и многие другие авторы начала XX века еще несколько десятилетий использовали термин **абелева группа** как название **симплектической группы**. Если это не приводило к недоразумениям, то, видимо, потому, что симплектические группы редко бывают абелевыми.

Нильс Хенрик Абель (Niels Henrik Abel, 05 августа 1802, Финдё – 06 апреля 1829, Кристиания, ныне Осло) — гениальный норвежский математик, основные работы которого относятся к теории алгебраических уравнений, теории рядов и теории алгебраических функций. Наряду с Якоби Абель был одним из основателей теории эллиптических функций.

Абель происходил из бедной семьи (его отец, как положено священнику, все пропивал). В том, что касается математики, был полным самоучкой, так как никаких математических курсов в университете Кристиании в то время вообще не читалось! В 1821–1823 годах он упорно пытался решить алгебраические уравнения степени 5 в радикалах и ему *показалось*, что нашел такое решение. Однако, он нашел ошибку в своем рассуждении и в 1824 году получил первое полное доказательство теоремы о неразрешимости в радикалах общего уравнения степени ≥ 5 (теорема Руффини—Абеля). За это достижение он получил стипендию, которая позволила ему совершить поездку в Германию, Италию и Францию. За полгода, проведенные в Берлине, он подружился с Крелле и написал шесть статей, которые были опубликованы в первом томе только что созданного *Journal für die reine und angewandte Mathematik*. После этого Абель провел несколько месяцев в Венеции и затем поехал в Париж. Там он пытался вступить в контакт с французскими математиками, но был принят *крайне* недоброжелательно. Коши, как водится, "потерял" его большой мемуар, представленный в Парижскую Академию наук. Однако, когда в 1830-м году Коши бежал из Франции, рукопись нашли. Grand Prix Парижской академии был присужден Абелю **посмертно**.

Абелю было несколько раз отказано в преподавательской позиции на родине на том основании, что во-первых, он *постоянно ездит за границу*, а во-вторых, *все равно не сумел бы приспособить свое изложение к уровню понимания студентов младших курсов*. Вынужденный содержать семью и не имея постоянной должности, Абель зарабатывал на жизнь частными уроками и умер от чахотки в бедности за несколько дней до того, как ему пришло приглашение на должность профессора в Берлинский университет.

Кроме абелевых групп и абелианизации в нашем курсе встречается трюк Абеля, несколько теорем Абеля и теорема Руффини—Абеля, громадную роль в математике играют абелевы функции, абелевы многообразия, ... На русский переведена подробная биография Абеля, написанная одним из лучших норвежских математиков XX века Ойстеном Оре [27].

2. Изоморфизм. Абстрактная теория групп изучает свойства групп **с точностью до изоморфизма**. А именно, две группы H и G называются **изоморфными**, если между ними можно установить биекцию

$\phi : H \longrightarrow G$ сохраняющую операцию, т. е. такую, что $\phi(hg) = \phi(h)\phi(g)$ для двух любых элементов $h, g \in H$. Такое отображение ϕ называется **изоморфизмом**. Вообще, любое сохраняющее операцию отображение одной группы в другую называется **гомоморфизмом** и мы детально изучим гомоморфизмы в главе 4. В случае, когда две группы H и G изоморфны, пишут $H \cong G$. Мы вернемся к детальному обсуждению этого понятия в главе 4.

Комментарий. Традиционная точка зрения состоит в том, что природа элементов группы при этом не важна. Это действительно так, если мы интересуемся *тривиальными* вопросами. При изучении всех более глубоких вопросов конкретная геометрическая реализация группы играет существенную роль: различные вычисления проще производить в различных моделях, именно в этом состоит основная идея теории представлений. Именно поэтому, кстати, у многих несложных — но *глубоких* — классических теорем теории групп есть совсем простые геометрические, матричные или арифметические доказательства, но нет никаких теоретико-групповых доказательств, либо есть только такие доказательства, которые *сам не посмотришь и другим не покажешь*. Кроме того, в большинстве приложений обычно возникают *значительно* более тонкие отношения эквивалентности, чем изоморфность. Поэтому уже в этой главе мы, как правило, будем стоять на точке зрения КОНКРЕТНОЙ теории групп, которая рассматривает группы не с точки зрения изоморфизма, а с точки зрения их сопряженности в некоторой объемлющей группе, обычно в группе изоморфизмов некоторого геометрического объекта.

3. Свойства обратных элементов. Приведем два простейших свойства обратных элементов, которые в дальнейшем постоянно используются без явных ссылок:

$$(x^{-1})^{-1} = x, \qquad (xy)^{-1} = y^{-1}x^{-1}.$$

Обратите внимание на порядок множителей во втором выражении. Если две операции не коммутируют, то он весьма существен. Надевают обычно сначала пиджак, а потом пальто, а снимают, соответственно, наоборот, сначала пальто, и только потом пиджак. С другой стороны, если два преобразования коммутируют, как, например, надевание левой и правой перчаток, то коммутируют и обратные к ним преобразования, так что снимать их можно в произвольном порядке.

Коан. Как фокуснику удается снять пиджак, не снимая пальто?

5. Деление в группе. Как мы знаем, любой обратимый элемент регулярен, так что на него можно сокращать. В действительности, в группе разрешимы все уравнения вида $gx = h$, достаточно умножить это равенство слева на g^{-1}, что дает $x = g^{-1}h$. С другой стороны, решением уравнения $yg = h$ является $y = hg^{-1}$. Если g и h не коммутируют, то эти два решения не совпадают, так что нужно различать

левое частное $g^{-1}h$ от **правого частного** hg^{-1}. Поэтому в группах обычно избегают пользоваться записью h/g для деления, а предпочитают писать явно $g^{-1}h$ или hg^{-1}.

Из однозначности деления вытекает, что в группе можно сокращать на любой элемент справа и слева. Возможность **левого сокращения** означает, что равенство $gx = gy$ влечет $x = y$. Аналогично, возможность **правого сокращения** означает, что если $xg = yg$, то $x = y$.

§ 2♠. Сколько операций в группе?

> Группу можно все же рассматривать как алгебру типа $\langle 2\rangle$, т. е. с одной основной бинарной операцией, только не с операцией умножения, а с операцией деления.
>
> Анатолий Иванович Мальцев. [28]

> В конце концов, если нас обвинят в снобизме, пусть их. Все равно нас в чем-нибудь обвинят.
>
> Иосиф Бродский

1. Группа как множество с одной операцией. По словам Владимира Игоревича Арнольда♮, преступные алгебраисты определяют группу как множество с *двумя* операциями. Алгебраисты **никогда** не определяют группу как множество с двумя операциями. Группа определяется либо как множество с

♮В соответствии с общим принципом биографии современников не приводятся и никакие прямые оценки их роли и влияния не даются — это та слишком чувствительная часть лекций, которая не может быть воспроизведена в печатном тексте: *ходить бывает склизко по камешкам иным*. Вероятно, даже мои высказывания о Куроше или Мальцеве, которые отделены уже от нас некоторой дистанцией, могут *многих* покоробить. Что же говорить о наших современниках, кто из них должен быть назван гениальным, кто замечательным, а кто просто великим? Хотя, конечно, в ответ на прямые вопросы студентов я давал столь же прямые *непечатные* оценки. Тем не менее, я хочу воспользоваться случаем пропагандировать сочинения Арнольда: все, что он пишет, талантливо, увлекательно и безумно смешно, независимо от того, издевается он над математиками, физиками, военными, авторами школьных учебников, французскими чиновниками, американскими эдукационистами, экологистами или правозащитниками. Вот несколько его проникновенных высказываний: математика есть раздел теории особенностей; математика — это такой раздел физики, эксперименты в котором дешевы; вся математика делится на три раздела: небесная механика, гидродинамика и теория кодирования; тождество Якоби — это экспериментальный факт. Арнольд написал несколько блистательных книг, в том числе [23], [29]–[34]. В последние годы Издательство МЦНМО издает цитатники Арнольда — маленькие зеленые книжечки: ‘Что такое математика?’, ‘Нужна ли математика в школе?’ и т. д.

тремя операциями, о чем ниже, либо как множество с *одной* операцией. Причем в последнем случае это операция правого деления.

Упражнение. Обозначим через $g/h = gh^{-1}$ операцию *правого* деления. Убедитесь, что все три операции, входящие в сигнатуру группы выражаются через операцию / следующим образом: $e = g/g$, $g^{-1} = (g/g)/g$, $gh = g/((h/h)/h)$. Проверьте, что, кроме того, $g = g/(g/g)$ и $(f/f)/(g/h) = h/g$.

Хиллел Фюрстенберг [35] показал, что группа может быть определена как множество с одной бинарной операцией $G \times G \longrightarrow G$, $(g, h) \mapsto g/h$, удовлетворяющей двум следующим аксиомам:

- для любых $f, g, h \in G$ выполняется равенство $(f/h)/(g/h) = f/g$,
- для любых $g, h \in G$ уравнение $g/x = h$ разрешимо.

Упражнение. Попробуйте вывести из этих аксиом, что умножение в G, определенное равенством $gh = g/((h/h)/h)$, ассоциативно.

2. Группа как множество с двумя операциями. В порядке мелкого подхалимажа заметим, что вот как раз некоторые **топологи** действительно определяют группу как множество с **двумя** операциями, см., например, **[164]**, с.23–25. А именно, группой называется множество G с отмеченной точкой e и определенными на нем операциями **умножения** $m : G \times G \longrightarrow G$, и **обращения** $i : G \longrightarrow G$, такими, что следующие три диаграммы коммутативны[♮]:

G1. Ассоциативность:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \mathrm{id}} & G \times G \\ {\scriptstyle \mathrm{id} \times m}\downarrow & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow[m]{} & G \end{array}$$

G2. Существование нейтрального элемента:

$$\begin{array}{ccccc} G & \xrightarrow{(e,\mathrm{id})} & G \times G & \xleftarrow{(\mathrm{id},e)} & G \\ & & \downarrow{\scriptstyle m} & & \\ & & G & & \end{array}$$

G3. Существование обратного элемента:

$$\begin{array}{ccccc} G & \xrightarrow{(i,\mathrm{id})} & G \times G & \xleftarrow{(\mathrm{id},i)} & G \\ & & \downarrow{\scriptstyle m} & & \\ & & G & & \end{array}$$

Легко видеть, что коммутативность этих диаграмм представляет собой переформулировку условий G1 — G3, так что это определение эквивалентно определению приведенному в пункте 1. Рассмотрим теперь операцию $\tau : G \times G \longrightarrow G \times G$,

[♮]Вообще-то начинающий не должен был это читать!! Однако наиболее настырные начинающие могут найти определение коммутативной диаграммы в последнем параграфе первого аппендикса и в первом аппендиксе второй части.

переставляющую множители: $\tau(x,y) = (y,x)$. Тогда аксиома коммутативности может быть выражена следующим образом.

G4. Коммутативность:

$$\begin{array}{ccc} G\times G & \xrightarrow{\ \tau\ } & G\times G \\ & \searrow \quad \swarrow & \\ & G & \end{array}$$

Это определение хорошо всем, но в современных алгебраических текстах — например, в книгах по алгебраическим группам **[34]**, **[62]**, **[195]** — и нейтральный элемент e тоже часто рассматривается как *отображение*.

3. Ужасы нашего (Академ)городка. Конечно, произнесенное в первом пункте утверждение, что алгебраисты **никогда** не определяют группу как множество с двумя операциями — это чисто пропагандистское заявление в духе самого Арнольда. В действительности, Анатолий Иванович Мальцев, ВЕЛИКИЙ И УЖАСНЫЙ, определяет группу [28], с. 97 как трипель $\mathfrak{G} = \langle G, \cdot, {}^{-1}\rangle$. При этом он предполагает, что умножение ассоциативно и, кроме того, выполняются тождества $y^{-1}(yx) = x$ и $(xy)y^{-1} = x$.

> **Анатолий Иванович Мальцев** (27 ноября 1909, Московская область — 07 июля 1967, Новосибирск) — великий русский алгебраист и логик. После окончания в 1930 году Московского университета Мальцев с 1932 по 1960 год преподавал в Ивановском педагогическом институте, где он с 1943 года заведовал кафедрой алгебры. С 1939 по 1941 год Мальцев проходил докторантуру в МИАН, а с 1942 по 1960 год по совместительству был там старшим научным сотрудником. В 1953 году он был избран членом-корреспондентом, а в 1958 году (еще до переезда в Новосибирск!) — академиком АН СССР. В 1960 году Мальцев переезжает в Новосибирск, где становится заведующим отделом алгебры ИМ СОАН и заведующим кафедрой алгебры и математической логики. Основные ранние работы Мальцева относятся к теории групп Ли, топологической алгебре, теории линейных групп и теории колец. В этот период им получено несколько великолепных результатов, которые стали классическими: теорема Леви—Мальцева; примеры колец без делителей 0, не вложимых в тело; существование точного линейного представления; метод финитной аппроксимируемости, и т. д. В последний период своей жизни он полностью переключился на очень общую алгебру, теорию алгебраических систем и математическую логику. Кроме уже цитированного монструозного сочинения *Алгебраические системы*, Мальцев написал очень тяжеловесный и архаичный курс линейной алгебры [36] и вполне удачный учебник [37]. Все основные статьи Мальцева собраны в издании [38], [39].

Акарологический комментарий. Влияние Мальцева на развитие алгебры в нашей стране огромно, но неоднозначно. Именно он ввел зловещее словосочетание **алгебра и логика**, которое стало девизом сибирской школы — почему тогда не **алгебра и теория чисел**, как в Петербурге, не **алгебра и алгебраическая геометрия**,

как в Москве, **алгебра и топология**, **алгебра и геометрия**, **алгебра и анализ**, **алгебра и дифференциальные уравнения** или даже **алгебра и теория вероятности**, как у Чебышева и Линника!! Сам Мальцев был, несомненно, **крупным** математиком (*всякое тело вкладывается в тело Мальцева*). Однако те идеи, которые он вдохновлял чуть не привели алгебру в нашей стране к гибели. Чтобы уточнить свою позицию, замечу, что я не отрицаю деятельность в области очень общей алгебры, я только решительно против того, чтобы называть "общую алгебру" алгеброй (а не логикой, каковой она в действительности является!) — и уж *абсолютно* против того, чтобы отождествлять **всю** алгебру с общей алгеброй, как это de facto произошло на определенном этапе в Новосибирске. Кроме того, такое понимание навязывалось всей остальной стране административно-террористическими методами.

Упражнение. Покажите, что определение Мальцева эквивалентно обычному.

Разумеется, философски определение Мальцева является неправильным. То, что он определяет, в действительности есть группа, рассматриваемая в сигнатуре **инверсной полугруппы**. Он объясняет, что так можно поступать потому, что любая *инверсная* подполугруппа группы автоматически является подгруппой. Но ведь любой полугрупповой гомоморфизм одной группы в другую автоматически будет гомоморфизмом групп, что же тогда Анатолий Иванович не определяет группу как **дупель** $\mathfrak{G} = \langle G, \cdot \rangle$? Он объясняет это тем, что "операцию обращения можно определить (но не выразить) через операцию умножения" — в то же время третья операция в группе, взятие нейтрального элемента, **выражается** через умножение и взятие обратного и *поэтому* ее нужно исключить из рассмотрения! Я *полностью* солидарен с Арнольдом в том, что подобные инсинуации трудно квалифицировать иначе как насилие над всеми здоровыми математическими инстинктами, совершаемое во имя логического **делюзионизма***.

4. Группа как множество с тремя операциями. Как мы знаем из предыдущей главы, нейтральный элемент e и элемент, обратный к данному элементу $x \in G$, определены однозначно. С точки зрения общей алгебры нейтральный элемент и обратный элемент входят в **сигнатуру** группы. Это значит, что на самом деле группа представляет собой множество с **тремя** операциями: обычной бинарной операцией умножения $\mathrm{mult} : G \times G \longrightarrow G$, унарной операцией взятия обратного элемента $\mathrm{inv} : G \longrightarrow G$, $x \mapsto x^{-1}$, и нульарной операцией $e \in G$. Чтобы подчеркнуть это, иногда обозначают группу как $(G, \mathrm{mult}, \mathrm{inv}, e)$. Такой педантизм оказывается *весьма* полезен при изучении групп с заданными на них дополнительными структурами, но мы, разумеется, будем обычно говорить о группе как о множестве с одной бинарной операцией, удовлетворяющей свойствам, перечисленным выше.

Преимущество данного в предыдущем пункте функториального определения состоит в том, что оно сразу же переносится на все категории, в которых существуют конечные прямые произведения и финальный объект. На русском языке это можно найти, например, в [40]. На этом пути мы получаем определение **группы в категории**. При этом то, что мы называем просто группой — есть *группа*

---

*Делюзия — сознательное введение в заблуждение, обман; галлюцинация, иллюзия или заведомо ложное представление, возникшие в результате мистификации, сознательной дезинформации или болезненного состояния психики; бредовые или маниакальные состояния (мания преследования, мания величия, etc.), возникающие в результате преувеличенного представления о собственной значимости.

в категории множеств. Однако существует и много других важных примеров. Например, вместо множеств и отображений здесь можно рассматривать одну из следующих категорий:

• топологические пространства и непрерывные отображения — в этом случае получатся **топологические группы**, см. § 18,

• аналитические многообразия и аналитические отображения — в этом случае получатся **аналитические группы** более известные широким народным кругам как **группы Ли**, см. § 19,

• алгебраические многообразия и регулярные отображения — в этом случае получатся **алгебраические группы**, см. § 20.

С другой стороны, можно рассматривать и такие категории, в которых морфизмы не являются отображениями:

• топологические пространства и гомотопические классы непрерывных отображений — в этом случае получатся **H-группы**. Разумеется, для H-групп и коммутативность диаграмм тоже нужно понимать с точностью до гомотопии,

• схемы и морфизмы схем — в этом случае получатся **групповые схемы**.

§ 3◇. Первые примеры абелевых групп

Много примеров групп встречалось уже в школьном курсе математики.

• **Аддитивные группы чисел.** Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ образуют группы по сложению. Иногда чтобы подчеркнуть, что речь идет именно об аддитивных структурах на этих множествах, пишут $\mathbb{Z}^+$, $\mathbb{Q}^+$ и т. д. Эти группы называются **аддитивными группами** целых, рациональных, вещественных и комплексных чисел, соответственно.

• **Мультипликативные группы чисел.** Множества ненулевых рациональных, вещественных или комплексных чисел $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ образуют группы по умножению, называемые **мультипликативными группами** рациональных, вещественных и комплексных чисел, соответственно. Напомним, что *для поля* K^* совпадает с $K^\bullet = K \setminus \{0\}$, в общем случае через R^* обозначается множество обратимых элементов кольца R.

• **Мультипликативные группы чисел, cont.** Множества $\mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x > 0\}$ и $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ положительных рациональных и вещественных чисел представляют собой группы по умножению.

Комментарий. Во многих книгах для групп $\mathbb{R}_+$ и $\mathbb{Q}_+$ используется обозначения $\mathbb{R}_{>0}$ и $\mathbb{Q}_{>0}$. Эти обозначения не вызывают у меня аллергии и я часто спрашиваю студентов, что они предпочитают. Однако здесь, как и всегда, сам я предпочитаю использовать более короткие обозначения.

• **Группа углов** (`circle group`). Множество $\mathbb{T}$ комплексных чисел модуля 1 также представляет собой группу по умножению. Заметим, впрочем, что операция в этой группе (группе поворотов эвклидовой плоскости или группе углов) обычно записывается **аддитивно**, что согласуется со следующей ее интерпретацией. Группа $\mathbb{T}$ истолковывается как аддитивная группа вещественных чисел $\mathbb{R}^+$ по модулю $2\pi\mathbb{Z}$ (читается `целые кратные` 2π). Иными словами, $\mathbb{T}$ представляется как полуинтервал $[0, 2\pi)$, операция сложения $\oplus$ на котором определяется следующим образом: если $x+y < 2\pi$, то $x \oplus y = x+y$, а если $x+y \geq 2\pi$, то $x \oplus y = x+y-2\pi$. В действительности, конечно, операция в $\mathbb{T}$ записывается обычным знаком $+$ (`сложение углов`), см. главу 3 по поводу деталей.

• **Группа корней из 1.** Мультипликативная группа $\{1\}$ состоит из одного элемента, а $\{\pm 1\}$ — из двух. Вообще, корни n-й степени из 1 в поле $\mathbb{C}$ комплексных чисел образуют группу по умножению, обозначаемую обычно μ_n. Эти группы конечны, т. е. содержат конечное число элементов. Мы уже упоминали, что для конечной группы G мощность $|G|$ обычно называется ее **порядком**. С точки зрения своей структуры группа μ_n является **циклической группой** порядка n (см. главу 2). Например, *с точностью до изоморфизма* $\mu_1 = \{1\}$ единственная группа порядка 1, $\mu_2 = \{\pm 1\}$ — единственная группа порядка 2, а $\mu_3 = \{1, \omega, \omega^2\}$ — единственная группа порядка 3.

• **Квазициклические группы.** Множество μ_{p^∞} всех корней из 1 степеней p^n, $n \in \mathbb{N}$, в поле $\mathbb{C}$ комплексных чисел образует группу, называемую **квазициклической группой** типа p^∞ (или просто **группой типа** p^∞).

• **Булева группа.** Множество 2^X подмножеств в X является группой относительно **симметрической разности** (aka **булевой суммы**) Δ. При этом нейтральный элемент этой операции равен $\varnothing$, а $Y \Delta Y = \varnothing$, так что каждый элемент является симметричным сам себе.

• **Векторные группы.** Пусть снова K обозначает одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — в школьной программе обычно рассматривался случай $K = \mathbb{R}$. Если рассмотреть n-мерное векторное пространство $V = K^n$ и забыть о том, что векторы можно умножать на скаляры, а оставить на V только аддитивную структуру (сложение векторов), то V называется **векторной группой** (`vector group`). Как мы узнаем в § 4, она изоморфна прямой сумме n экземпляров аддитивной группы K^+.

• **Группы трансляций.** Группу V можно заставить действовать

на себе, а именно, каждому вектору $u \in V$ сопоставляется **аффинное преобразование** $T_u : V \longrightarrow V$, $v \mapsto v + u$, называемое **трансляцией***, или параллельным переносом. Группа $T(V) = \{T_u \mid u \in V\}$ называется **группой трансляций**. В случае, когда $K = \mathbb{R}$, группа $T(V)$ состоит из эвклидовых движений пространства V.

Комментарий. В элементарных учебниках трансляции часто называются **сдвигами**, но профессиональные алгебраисты называют **сдвигом** (`shift`) преобразование, которое трансляция аргументов индуцирует на функциях. Сдвиги *контравариантны* по отношению к трансляциям: когда аргумент транслируется *вправо*, график функции сдвигается *влево*, подробнее об этом см. главу 6.

• **Решетки.** Зафиксируем базис $e_1, \dots, e_n$ в векторном пространстве $V = \mathbb{R}^n$ и рассмотрим множество $L = \mathbb{Z}e_1 + \dots + \mathbb{Z}e_n$ всевозможных *целочисленных* линейных комбинаций векторов $e_1, \dots, e_n$. Это множество называется **решеткой** в V с базисом $e_1, \dots, e_n$. Как абстрактная группа L изоморфна свободной абелевой группе $\mathbb{Z}^n$ ранга n, однако в понятие решетки входит еще и свойства вложения: чтобы подгруппа $L \cong \mathbb{Z}^n$ в векторной группе $V = \mathbb{R}^n$ могла называться решеткой, она должна быть дискретной, а фактор V/L компактен!

Комментарий. Обозначение L стандартно и происходит от первой буквы английского `lattice`. Заметим, что по-английски, как и по-русски имеется крайне неудачная омонимия, так как, кроме того, слово `lattice` употребляется для обозначения частично упорядоченных множеств, в которых существует супремум и инфимум. Поэтому в случае необходимости профессионалы переводят слово **решетка** обратно на немецкий, где терминология, *как всегда*, однозначна: свободная абелева группа называется `Gitter`, в то время как частично упорядоченное множество — `Verband`.

§ 4◇. Первые примеры неабелевых групп

> Лев Толстой очень любил детей. Приведет полную комнату, шагу ступить негде, а он все кричит: “Еще! Еще!”
>
> Даниил Хармс. *Веселые ребята*

Предшествующие примеры дают совершенно превратное представление о том, что такое группа — группы, фигурирующие во всех этих примерах, абелевы. В действительности, группа гораздо больше похожа не на множество чисел, а на множество взаимно однозначных

*`Трансляция` — перенос, перемещение, передвижение, сдвиг. В дальнейшем в нашем курсе встречаются трансвекции, **трансвекция** это смещение, перенос одной части предмета относительно другой его части, в то время как трансляция есть движение предмета как целого.

преобразований чего-то, сохраняющих, быть может, какую-то дополнительную структуру. Следующий пример архетипичен, как мы вскоре увидим, каждая группа **есть** множество преобразований.

• **Симметрическая группа.** Пусть G — множество всех взаимно однозначных отображений множества X на себя. Тогда G является группой относительно композиции, называемой **симметрической группой** множества X и обозначаемой S_X или $S(X)$ (`symmetric group`). В самом деле, как мы знаем, композиция отображений ассоциативна; композиция двух биекций снова является биекцией; тождественное отображение является биекцией и служит нейтральным элементом композиции и, наконец, любая биекция обратима, причем обратное отображение также является биекцией. В главе 5 мы подробно рассмотрим этот пример в случае, когда X конечно. Заметим, что в случае $|X| \geq 3$ эта группа некоммутативна. В частности, при $n = 3$ получаем **группу треугольника** S_3 порядка 6 — самую маленькую неабелеву группу.

• **Группы преобразований.** Специализируя этот пример, т. е. рассматривая не все биекции X на себя, а только те, которые сохраняют имеющуюся на X структуру (например, алгебраическую, геометрическую, топологическую, или какую-то их комбинацию), можно получить множество новых примеров групп. Эти примеры рассмотрены в § 12.

• **Группа кватернионов.** Рассмотрим группу Q, состоящую из 8 элементов $\{\pm 1, \pm i, \pm j, \pm k\}$; причем $+1 = 1$ действительно действует как единица группы, квадраты всех отличных от ± 1 элементов равны -1, знаки подчиняются обычному правилу (т. е., например, $(-i)(-k) = ik$), а попарно различные i, j, k умножаются как орты $\mathbb{R}^3$ относительно векторного умножения: $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Так определенное умножение ассоциативно (можно проверить это и непосредственно, но вскоре мы узнаем гораздо более красивое доказательство, использующее матричные представления), а все элементы обратимы, например, $i^{-1} = -i$ и, соответственно, $(-i)^{-1} = i$. Группа Q обычно называется **группой кватернионов** (`quaternion group`, `Quaternionengruppe`), хотя правильнее называть ее **группой кватернионных единиц**. Эта группа была использована Гамильтоном в 1842 году при построении тела кватернионов $\mathbb{H}$.

• **Полная линейная группа.** Пусть K — поле, например, $K =$

Сэр **Уильям Роуан Гамильтон** (Sir William Rowan Hamilton, 4 августа 1805, Дублин — 2 сентября 1865, Дублин) — гениальный ирландский математик, один из величайших классиков XIX века. Гамильтон был необычайно одарен с детства, к пяти годам он выучил латынь, греческий и иврит, а к 13 годам — еще десяток европейских и восточных языков. Уже в 1927 году — в возрасте 21 года! — Гамильтон был назначен профессором астрономии Trinity College, однако вскоре после этого он потерял интерес к астрономии и полностью переключился на математику.

Два самых знаменитых открытия, связанных с именем Гамильтона — это гамильтонова формулировка классической механики, данная им и Якоби (гамильтониан) и гамильтоновы кватернионы. По общему признанию, гамильтониан является не просто самым важным понятием, а самой сутью физики. В 1833 году Гамильтон истолковал комплексные числа как пары вещественных чисел, однако потребовалось еще 10 лет, прежде, чем он научился умножать *четверки* вещественных чисел.

Кватернионы были открыты в понедельник 16 октября 1843 года, когда Гамильтон вместе с женой шел вдоль Королевского Канала в Дублине на заседание Академии. Он тут же нацарапал формулу $i^2 = j^2 = k^2 = ijk = -1$ на каменных перилах Brougham Bridge. Я полностью солидаризуюсь со взглядом самого Гамильтона, что ИЗОБРЕТЕНИЕ КВАТЕРНИОНОВ — СОБЫТИЕ *по крайней мере* СТОЛЬ ЖЕ ЗНАЧИТЕЛЬНОЕ, КАК ИЗОБРЕТЕНИЕ ДИФФЕРЕНЦИАЛЬНОГО И ИНТЕГРАЛЬНОГО ИСЧИСЛЕНИЯ. Дело, конечно, не столько в самих кватернионах, сколько в том, что они начали новую эпоху, послужив толчком к изучению некоммутативных операций. Именно под влиянием кватернионов Кэли начал систематически изучать умножение матриц.

Гамильтое описал алгебру кватернионов и ее применения в геометрии, анализе и физике в двух классических книгах: *Lectures on quaternions* и *Elements of quaternions*. В действительности, если бы это открытие было воспринято физиками столь же серьезно, многие физические теории, в том числе теория относительности, могли бы быть открыты лет на 50 раньше. К сожалению, вместо того, чтобы пытаться понять его идеи или вообще заниматься чем-нибудь полезным, большинство физиков XIX века — собственно, все, кроме Максвелла, — посвящали свое время исключительно травле Гамильтона.

Эта травля, а также его запутанные отношения с женщинами в конечном счете привели к тому, что Гамильтон начал серьезно злоупотреблять алкоголем. Как констатируют О'Коннор и Робертсон, он умер от приступа подагры после того, как ему сообщили, что он избран первым иностранным членом Национальной Академии Наук США.

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Тогда множество

$$\mathrm{GL}(n, K) = \{g \in M(n, K) \mid \det(g) \neq 0\}$$

всех невырожденных матриц порядка n является группой относительно умножения, называемой **полной линейной группой** степени n над K. Обозначение $\mathrm{GL}(n, K)$ является сокращением английского General Linear group. В § 9 мы рассмотрим эту группу и некоторые

связанные с ней группы в частном случае $n = 2$. Много дальнейших примеров матричных групп встретится нам в книгах III и IV.

• **Группа Мебиуса.** Рассмотрим множество **дробно-линейных преобразований** сферы Римана$\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ (**расширенной комплексной плоскости**). Оно состоит из всех преобразований вида: $z \mapsto \dfrac{az+b}{cz+d}$, где $a, b, c, d \in \mathbb{C}$ и $ad - bc \neq 0$. Очевидно, что композиция двух дробно-линейных преобразований снова будет дробно-линейным преобразованием, а обратное преобразование имеет вид $z \mapsto \dfrac{dz-b}{-cz+a}$ (проверьте!). Получающаяся так группа называется **группой Мебиуса** (или **группой конформных преобразований** $\overline{\mathbb{C}}$). Различные связанные с ней группы, ее варианты и обобщения играют громадную роль во многих разделах анализа, теории чисел и геометрии.

Август Фердинанд Мёбиус (August Ferdinand Möbius, 17 ноября 1790, Шульпфорта — 26 сентября 1868, Лейпциг) — выдающийся немецкий геометр, директор обсерватории и профессор университета в Лейпциге, работы которого проложили путь к теоретико-групповой трактовке геометрии. Мебиус учился в Лейпциге, в Геттингене у Гаусса и в Халле у Пфаффа. Большую часть жизни Мебиус работал как астроном, но в действительности его наиболее известные результаты относятся к проективной геометрии, геометрическим преобразованиям и топологии. Кроме группы Мебиуса в нашем курсе Вам встретятся функция Мебиуса, формула обращения Мебиуса, формула Мебиуса—Дедекинда, а в курсе топологии — лист Мебиуса.

Задача. Преобразование $z \mapsto \dfrac{a\overline{z}+b}{c\overline{z}+d}$, где a, b, c, d такие же, как выше, называется **антиконформным**. Докажите, что конформные и антиконформные преобразования образуют группу. Некоторые авторы называют группой Мебиуса именно эту группу.

• **Группа $\mathbf{ax+b}$.** Пусть K — некоторое поле, например, $K = \mathbb{Q}$ или $K = \mathbb{R}$. Определим на множестве $K^* \times K$ умножение, полагая $(a, b)(c, d) = (ac, ad + b)$. Это умножение превращает $K^* \times K$ в группу (проверьте!), которую (алгебраические) геометры называют **группой $\mathbf{ax+b}$**. В этой группе $(a, b)^{-1} = (a^{-1}, -a^{-1}b)$. В случае $K = \mathbb{R}$ это в точности группа аффинных преобразований прямой.

• **Аффинная группа.** Предыдущий пример легко обобщить на случай произвольной размерности. А именно, пусть, как и выше, K — некоторое поле. Рассмотрим пары (g, u), где $g \in \mathrm{GL}(n, K)$ — обратимая матрица, а $u \in K^n$ — столбец высоты n. Определим на множестве $\mathrm{GL}(n, K) \times K^n$ умножение, полагая $(g, u)(h, v) = (gh, gv + u)$.

Легко видеть, что $(e,0)$ является нейтральным элементом этой операции, а $(g,u)^{-1}=(g^{-1},-g^{-1}u)$. Получающаяся так группа называется **аффинной группой** степени n над K и обозначается $\mathrm{Aff}(n,K)$. Аффинное преобразование (g,u) действует на пространстве $V=K^n$ по следующей формуле: $(g,u)v=gv+u$ — проверьте, что это на самом деле действие, иными словами, что выполняется тождество внешней ассоциативности $((g,u)(h,v))w=(g,u)((h,v)w)$. Физики, химики и кристаллографы вместо (g,u) обычно пишут $\{g|u\}$ и называют $\{g|u\}$ **символом Зейтца**. При этом матрица g называется **линейной частью** (`Linearanteil`) преобразования $\{g|u\}$, а вектор u — его **трансляционной частью** (`Translationsanteil`).

• **Группа Гейзенберга.** Пусть снова K — некоторое поле, ${}^nK$ множество строк длины n, а K^n множество столбцов высоты n. Определим на множестве ${}^nK\times K^n\times K$ умножение формулой

$$(u,v,a)(x,y,b)=(u+x,v+y,a+b+uy).$$

Это умножение превращает ${}^nK\times K^n\times K$ в группу (проверьте!), называемую **группой Гейзенберга**, которая естественно возникает при рассмотрении коммутационных соотношений в квантовой теории.

• **Группа Рубика.** Пусть теперь Γ — группа внутренних вращений кубика Рубика. В главе 8 мы сможем полностью описать строение этой группы, для этого необходимо знание еще одной важнейшей теоретико-групповой конструкции — сплетения. Из этого описания, в частности, будет вытекать, что порядок группы Рубика равен

$$\frac{1}{2}2^{11}12!\,3^7 8!=43252003274489856000,$$

что является совсем небольшим числом по стандартам современной теории конечных групп. Аналогично легко вычислить порядок группы внутренних вращений игрушки, известной в народе как **месть Рубика** (= `Rubik's revenge`), которая представляет собой куб $4\times4\times4$, это сделано в работах Ларсена [41], [42]. Порядок этой группы равен

$$\frac{3^7 8!\,24!^2}{24^7}=7401196841564901869874093974498574336000000000.$$

Автор оставляет читателю в качестве несложного упражнения по теории групп провести аналогичное вычисление для куба $5\times5\times5$, известного как **профессорский куб** (= `Professor's cube`).

Вернер Гейзенберг (`Werner Karl Heisenberg`, 05 декабря 1901, Вюрцбург — 1 февраля 1976, Мюнхен) — гениальный немецкий физик, один из создателей квантовой механики. В 1909 году его отец получил кафедру средневекового греческого языка в Мюнхене, где и прошло детство Гейзенберга. В гимназии его любимым предметом была математика, и он мечтал заниматься теорией чисел, однако Фердинанд фон Линдеманн отказался быть его руководителем (!!) — нет никакого сомнения, что иначе сегодня мы знали бы Гейзенберга как гениального теоретико-числовика. В результате Гейзенберг вслед за своим другом Паули стал учеником Зоммерфельда, что и определило его дальнейшую судьбу. В 1922–1923 годах Зоммерфельд поехал в США, а Гейзенберг — в Геттинген, где он учился у Борна, Гильберта и Франка. Позже он так вспоминал свои студенческие годы: Я научился оптимизму у Зоммерфельда, математике в Геттингене, а физике — у Борна. Большую часть ключевых 1924–1926 годов он провел в Копенгагене у Нильса Бора, вначале по гранту, а потом как ассистент. Вернувшись в 1925 году в Геттинген, Гейзенберг — с некоторой помощью Борна и Йордана в том, что касалось собственно математических аспектов — предложил аппарат матричной механики, который позволил произвести первые квантовомеханические вычисления. В 1927 году он сформулировал прославивший его имя принцип неопределенности и стал профессором в Лейпциге, где оставался до 1941 года, когда его назначили директором Физического института в Берлине. В 1932 году, в возрасте 31 года(!!) он был удостоен Нобелевской премии по физике за создание квантовой механики. В 1935 году нацисты ввели закон, согласно которому профессор должен уходить на пенсию в возрасте 65 лет (кстати, этот абсурдный закон продолжает действовать в Германии и сегодня!). Зоммерфельду как раз исполнилось 66, и он предлагал Гейзенберга в качестве своего преемника в Мюнхене, но квантовая механика, как и теория относительности, рассматривалась патриотически настроенными **немецкими учеными** как **еврейская наука**, а сам Гейзенберг как **еврейский прихвостень**. Тем не менее, во время Второй мировой войны Гейзенберг вместе с Отто Ханом возглавил немецкий ядерный проект. То ли из-за отсутствия ресурсов, то ли из-за преступной халатности, им удалось блестяще провалить работу над **оружием возмездия**. В 1945 году Гейзенберг был арестован американской спецслужбой ALSOS, но отпущен после года ежедневных допросов. В 1946 году он возглавил институт Макса Планка в Гетингене, а после переезда института в Мюнхен в 1958 году, наконец вернулся туда вместе с институтом, директором которого он оставался до ухода на пенсию в 1970 году. Гейзенберг написал несколько замечательных книг по физике и философии.

§ 5♢. Простейшие конструкции над группами

В этом параграфе мы начнем конкретизацию рассмотренных в книге I понятий общей алгебры. В дальнейшем мы детально изучим эти понятия в главах 2, 3 и 8.

1. Подгруппа. Пусть H непустое подмножество группы G. Предположим, что вместе с любыми двумя своими элементами $g, h \in H$ мно-

жество H содержит также их произведение gh и элемент g^{-1}. Тогда H само является группой относительно того же умножения. Ассоциативность и наличие нейтрального элемента проверять не надо, так как они автоматически вытекают соответствующих свойств группы G и непустоты H. Такое подмножество H называется **подгруппой** в G и в главе 2 мы подробно рассмотрим это понятие.

2. Фактор-группа. В главе 3 мы узнаем, как выглядят *конгруэнции* на группе G. Оказывается, каждая конгруэнция $\equiv$ определяется сравнением по модулю некоторой подгруппы $H \leq G$. При этом конгруэнции отвечают отнюдь не всякой подгруппе, а только **нормальным** подгруппам. Как обычно на множестве классов $G/\equiv$, которое в этом случае обозначается G/H, естественно вводится структура группы, превращающая G/H в **фактор-группу** группы G.

3. Прямое произведение/прямая сумма. Пусть H и G две группы. Рассмотрим покомпонентное умножение на $H \times G$:

$$(h_1, g_1)(h_2, g_2) = (h_1h_2, g_1g_2).$$

Ясно, что это умножение превращает $H \times G$ в группу. В самом деле, в книге I мы уже видели, что это умножение ассоциативно, а его нейтральным элементом является $e = (e, e)$ (педант написал бы $e_{H\times G} = (e_H, e_G)$). Осталось заметить, что $(h, g)^{-1} = (h^{-1}, g^{-1})$. Таким образом, $H \times G$ образует группу относительно умножения, называемую **прямым произведением** групп H и G.

В случае, когда H и G абелевы и операция в них записывается аддитивно, эта группа обычно обозначается $H \oplus G$ и называется **прямой суммой** групп H и G. По определению сложение в $H \oplus G$ задается так:

$$(h_1, g_1) + (h_2, g_2) = (h_1 + h_2, g_1 + g_2).$$

При этом $0 = (0, 0)$, а $-(h, g) = (-h, -g)$.

Эти определения моментально обобщаются на случай произвольного конечного семейства групп. А именно, **прямое произведение** $G_1 \times \ldots \times G_n$ групп $G_1, \ldots, G_n$ это декартово произведение множеств $G_1, \ldots, G_n$ с покомпонентными операциями. Прямое произведение *конечного числа* абелевых групп обычно обозначается $G_1 \oplus \ldots \oplus G_n$ и называется их **прямой суммой**.

Как обычно, мы полагаем $G^n = G \times \ldots \times G$, где количество сомножителей равно n. Два примера таких групп будут встречаться нам особенно часто:

- $\mathbb{Z}^n$ **свободная абелева группа** ранга n,

• $E_{p^n} = C_p^n$ **элементарная абелева группа** типа $(p, \ldots, p)$.

В главе 8 мы детальнейшим образом изучаем конструкцию прямого произведения групп, ее варианты, аналоги и обобщения (почти прямое произведение, подпрямое произведение, полупрямое произведение, скрюченное произведение, ...)

4. Прямое произведение $\neq$ прямая сумма. Для случая *конечных абелевых* групп во многих книгах термины **прямое произведение** и **прямая сумма** используются как синонимы. Дело в том, что прямое произведение и прямая сумма являются, соответственно, произведением и копроизведением в категории абелевых групп и для конечного числа факторов (сомножителей или слагаемых) они действительно совпадают. Это создает у начинающих опасные иллюзии. Однако, во-первых, в категории всех групп копроизведение устроено гораздо сложнее — это свободное произведение, которое мы построим в главе 11. Во-вторых, в случае бесконечного числа факторов даже для абелевых групп следует различать прямое произведение и прямую сумму. Как правило, они не только не изоморфны, но даже имеют разную мощность!

А именно, прямое произведение $\prod G_\alpha$, $\alpha \in \Omega$, семейства групп G_α, $\alpha \in \Omega$, как множество совпадает с их декартовым произведением, т. е. состоит из всех семейств (g_α), $\alpha \in \Omega$, $g_\alpha \in G_\alpha$. В то же время прямой суммой (копроизведением) абелевых групп G_α называется подгруппа в $\bigoplus G_a$, $\alpha \in \Omega$, состоящая не из всех семейств (g_α), а только из таких семейств, что $g_\alpha = 0$ для почти всех α. Например, если множество Ω и все группы G_α счетны, то $\bigoplus G_\alpha$ тоже счетна, в то время как $\prod G_\alpha$ имеет мощность континуума. Прямая сумма абелевых групп является частным случаем конструкции ограниченного прямого произведения групп, которую мы тоже изучим в главе 8. При этом начинающему следует иметь в виду, что в теории групп G^Ω как правило обозначает прямую сумму $|\Omega|$ экземпляров группы G, а вовсе не их прямое произведение! Например, $\mathbb{Z}^\mathbb{N}$ или $\mathbb{Z}^\omega$ используется для обозначения **свободной абелевой группы счетного ранга**.

Комментарий. В случае неабелевых групп аналог прямой суммы, т. е. подгруппа в прямом произведении $\prod G_a$, $\alpha \in \Omega$, состоящая из всех семейств $g = g(\alpha)$ таких, что $g_\alpha = 1$, называется **слабым произведением**. В книгах [**207**] и [**97**] то, что мы называем прямым произведением, называется **декартовым произведением**, а прямым произведением называется слабое произведение. Однако все мои инстинкты математика протестуют против того, чтобы различать термины прямое и декартово произведение в категории групп — ведь декартово произведение это не что иное, как прямое произведение в категории множеств (групп, колец, модулей, etc.). Кроме того, опыт показывает, что подобная терминология неизбежно ведет к путанице.

5. Функции со значениями в группе. Пусть G — группа, а X — произвольное множество. Тогда множество G^X всех отображений из X в G является группой относительно умножения функций $(fg)(x) = f(x)g(x)$. В самом деле, единицей в этой группе служит постоянная функция $f(x) = e$. Обратная к функции f (в смысле умножения, а не композиции!) это функция f^{-1}, для которой $f^{-1}(x) = f(x)^{-1}$.

§ 6◇. Образующие и соотношения: первый приступ

> Человеческие чувства часто сильнее возбуждаются или смягчаются конкретными примерами, чем общими словами.
>
> Пьер Абеляр. *История моих бедствий*

В главах 11 и 12 мы изложим основы систематической современной теории *задания групп образующими и соотношениями*. Эта теория — известная как **комбинаторная теория групп** — основана на понятии свободной группы и реализации каждой группы как факторгруппы свободной. Изучение подгрупп свободной группы представляет собой достаточно хитрое занятие и эта наука *начала* формироваться только в 1882–1911 годах и была поставлена на твердую алгебраическую основу только в 1921–1927 годах. Однако в действительности Гамильтон и Кэли использовали задания групп образующими и соотношениями задолго до этого и сейчас мы изложим наивный подход XIX века, без всяких там свободных групп и пр., примерно в том духе, как это делается в книге Бернсайда.

Артур Кэли (`Arthur Cayley`, 16 августа 1821, Ричмонд — 26 января 1895, Кембридж) — гениальный английский алгебраист и геометр, один из самых продуктивных математиков XIX века, наряду с Галуа и Гамильтоном один из основателей современной алгебры, в особенности линейной алгебры, теории колец, теории групп и алгебраической геометрии. Детство Кэли прошло в Санкт-Петербурге, но в 1830 году семья вернулась в Англию. После окончания Кембриджского университета в 1842 году он четыре года преподавал в университете и за это время опубликовал около 30 статей. Однако его позиция была временной, и Кэли пришлось избрать профессию юриста. Интересно отметить, что за 14 лет Кэли *в свободное от составления нотариальных актов о передаче имущества время* сумел написать около 250 статей — всего за свою карьеру он опубликовал более 900 работ! Наконец в 1863 году он получил кафедру чистой математики в Кембридже и смог полностью переключиться на математику. Его самые знаменитые работы относятся к теории матриц, теории групп, теории инвариантов, проективной геометрии, теории функций и комбинаторике. Колоссальное влияние на направление исследований Кэли оказали лекции Гамильтона о кватернионах. Вдохновленный Гамильтоном в 1842 году Кэли определил умножение матриц, а в 1843 году обобщая конструкцию кватернионов он построил неассоциативную 8-мерную алгебру с делением над полем вещественных чисел, известную как **`алгебра Кэли--Грейвса`** ака **`октонионы`**, **`октавы Кэли`** или **`числа Кэли`**. Кроме октав в нашем курсе встречаются алгебры Кэли—Диксона, таблица Кэли, теорема Кэли, теорема Кэли—Гамильтона, модель Кэли—Клейна геометрии Лобачевского и т. д. Много лет Кэли работал в тесном контакте со своим другом Сильвестром, кстати, тоже юристом по профессии.

Уильям Бернсайд (William Burnside, 02 июля 1852, Лондон — 21 августа 1927, Вест Викэм, Лондон) — блестящий английский математик, один из классиков алгебры, вместе с Фробениусом и Шуром создатель теории представлений. Из более, чем 150 статей Бернсайда лишь около 50 посвящены теории групп, однако эти работы и поставленные им проблемы в значительной степени предопределили развитие теории групп, как конечных, так и бесконечных.

Бернсайд учился в Кэмбридже у Стокса, Адамса и Максвелла и первые его публикации относятся к математической физике и теории эллиптических функций. Начиная с 1885 года, когда он был назначен профессором математики Королевского морского колледжа в Гринвиче, его основные научные интересы смещаются в область гидродинамики, где он с блестящим успехом применил методы теории функций комплексной переменной. Эти его работы считались настолько важными, что в 1893 году его избирают членом Royal Society именно за достижения в гидродинамике!!

Однако, еще в Кембридже он слушал лекции Кэли по теории групп, и после того как ему пришлось использовать группу дробно-линейных преобразований в теории конформных отображений, он заинтересовался абстрактными свойствами групп и с 1894 года полностью переключился на изучение конечных групп. Уже через три года он выпустил первое издание своей **очаровательной** книги *Theory of groups of finite order* (наиболее доступен Dover'овский репринт издания 1911 года, выпущенный в 1955 году в N. Y.). С моей точки зрения эта книга — если там слегка освежить терминологию — и сегодня хорошо смотрелась бы как курс теории групп для нематематиков — заведомо гораздо более **адекватный***, чем книги Куроша или Каргаполова—Мерзлякова, именно поэтому ее никогда не переводили на русский! Сомнительно, чтобы Бернсайду довелось когда-нибудь читать курс по теории групп в Морском Колледже, не было у него и прямых учеников. Влияние Бернсайда обязано, главным образом его изумительной книге и сформулированным им задачам, которые оказались узловыми проблемами всей теории групп. В частности, он предложил доказать разрешимость конечных групп нечетного порядка и доказать или опровергнуть конечность периодической конечно порожденной группы!

В 1918 году Бернсайд производит новый резкий вираж в своей карьере, полностью переключаясь на теорию вероятностей. К 1927 году он заканчивает книгу The theory of probability, которая выходит в свет через год после его смерти.

Конечно, это подход с точки зрения физика (если быть совсем точным, специалиста в области *гидродинамики*), а не математика, но он вполне достаточен, чтобы понимать, о чем идет речь, и трактовать *простейшие* примеры. Говоря по секрету, этого достаточно, чтобы понимать **все** обращения к заданиям групп вплоть до глав 11 и 12, **исключительно** — JUSQUE AU FEU, EXCLUSIVEMENT. Читатель, который уже знает, что значит запись

$$G = \langle x, y \mid x^2 = y^3 = (xy)^7 = e \rangle,$$

может без ущерба для понимания дальнейшего пропустить этот параграф. Более того, действительно сознательный и/или мотивированный студент-математик просто ОБЯЗАН пропустить этот параграф, даже если он не знает, что значит эта запись!! Вместо этого, чтобы избежать **контаминации** чуждой идеологией, ему следует прочесть §§ 1–3 главы 11 и § 1 главы 12, после чего сразу переходить к § 7 настоящей главы.

1. Образующие, соотношения, определяющие соотношения. Пусть G — группа, а $X \subseteq G$ — какое-то ее непустое подмножество. Вообще говоря, совершенно неверно, что если $x, y \in X$, то $xy \in X$ и $x^{-1} \in X$ (если это так, то множество X называется **подгруппой** в G). Будем образовывать *всевозможные* произведения элементов из X и их обратных и смотреть, что получится. Такие произведения называются **групповыми словами** в образующих X.

Тонкость здесь состоит в том, что мы должны спросить себя, **что именно** мы понимаем под произведением? *Запись* этого произведения в буковках $x, y, \ldots$ или все же тот *элемент* группы G, который представляется этой записью? Это тот же вопрос, с которым мы сталкиваемся в линейной алгебре, когда пытаемся определить линейную комбинацию векторов $u_1, \ldots, u_n$ с коэффициентами $a_1, \ldots, a_n$. Что такое $a_1u_1 + \ldots + a_nu_n$? Если это *вектор*, то он, конечно не помнит коэффициентов $a_1, \ldots, a_n$. А если он помнит коэффициенты, то он не вектор (или, точнее, вектор в каком-то другом пространстве). Конечно, в случае групп все усугубляется некоммутативностью. Например, записи $x^{-1}x$ и xx^{-1} несомненно отличаются *графически*, тем не менее, они будут представлять один и тот же элемент в ЛЮБОЙ группе G, а именно e. В терминах главы 11 говоря, что эти записи представляют собой один и тот же элемент в ЛЮБОЙ группе, мы имеем в виду, что эти записи совпадают *как групповые слова* или *как элементы свободной группы*.

С другой стороны, мы можем интересоваться не формой записи, а тем, чему это произведение *фактически* равно в группе G. Обозначим множество всех таких произведений, рассматриваемых как элементы

---

*В нормативном великорусском языке **что-то** может быть **адекватным чему-то** — однако в невском диалекте **адекватный** рутинно употребляется в *десятках* других значений, не требующих дополнения, особенно часто как сокращение выражения **compos mentis** (= **находящийся в здравом уме и твердой памяти**), но также в смысле **вменяемый**, **подходящий**, **пригодный**, **платежеспособный**, **работоспособный**, **дееспособный**, **компетентный**, **понятный**, **внушающий доверие**, **ответственный**, **съедобный**, **удовлетворительный**, **достаточный** и т. д.

группы G, через $\langle X\rangle$. Поначалу мы будем больше всего интересоваться случаем, когда $\langle X\rangle = G$, в этом случае говорят, что X **порождает** группу G или что X является ее **системой образующих**.

Интересный нюанс: два таких произведения в группе G могут оказаться равными, даже если формально они выглядят по разному и их равенство *не вытекает* исключительно из свойств групповых операций. В этом случае мы говорим, что мы получили **соотношение** между элементами множества X. Например, если группа G конечна, то количество возможностей *записи* произведений бесконечно, а количество возможных *значений* такого произведения конечно. Поэтому между элементами любого непустого подмножества X в *конечной* группе G заведомо есть нетривиальные соотношения. С другой стороны, **свободная группа** F это как раз и есть такая группа, в которой формальная точка зрения совпадает с фактической, т. е. все произведения $x_i \dots x_n$, где $x_i \in X$ или $x_i^{-1} \in X$, не содержащие фрагментов вида xx^{-1}, $x^{-1}x$ представляют собой различные элементы группы F. Иными словами, в свободной группе F между элементами множества X нет никаких нетривиальных соотношений.

Принципиальный момент, на котором, собственно, и основана возможность задания групп образующими и соотношениями, состоит в том, что рассматриваемые графически (т. е. как элементы свободной группы в алфавите X), соотношения сами образуют группу. Иными словами, если $x_1 \dots x_m = e$ и $y_1 \dots y_n = e$, представляют собой два соотношения, то $x_1 \dots x_m y_1 \dots y_n = e$ и $x_m^{-1} \dots x_1^{-1} = e$ тоже соотношения. Например, если мы уже знаем, что $x^2 = e$ и $y^3 = e$, то нас не должно удивлять, что $x^2y^{-3} = e$ или, иными словами, $x^2 = y^3$. Пусть Y — некоторое множество соотношений, тогда мы можем рассмотреть всевозможные **следствия** этих соотношений, которые получаются как произведения соотношений из Y и обратных к ним. Может оказаться, что вообще любое соотношение, выполняющееся между элементами X в группе G, окажется следствием соотношений из Y. В этом случае говорят, что Y образует множество **определяющих соотношений** группы G в образующих X и пишут $G = \langle X \mid Y\rangle$. Перед вертикальной чертой здесь указывается множество образующих, а после вертикальной черты — множество *определяющих* соотношений. Если $X = \{x_1, \dots, x_m\}$, а $Y = \{y_1 = e, \dots, y_n = e\}$, то пишут

$$G = \langle x_1, \dots, x_m \mid y_1 = \dots = y_n = e\rangle.$$

Часто, впрочем, нагляднее записывать соотношения в виде $u = v$, чем в виде $uv^{-1} = e$. В этом случае задание будет выглядеть примерно

так:

$$G = \langle x_1, \dots, x_m \mid u_1 = v_1, \dots, v_m = v_m \rangle.$$

Однако давно пора переходить от общих слов к конкретным примерам.

2. Циклические группы. Пусть $X = \{x\}$ состоит из одного элемента $x \in G$. Тогда из x и x^{-1} можно образовать:

• одно произведение длины 0, по определению такое произведение равно e;

• два произведения длины 1, а именно x и x^{-1};

• четыре произведения длины 2, а именно $x^2 = xx$, xx^{-1}, $x^{-1}x$ и $x^{-2} = x^{-1}x^{-1}$.

`Ups!` Здесь нужно начинать быть внимательным. Дело в том, что, во-первых, по определению x^{-1} мы имеем $xx^{-1} = x^{-1}x = e$. Эти равенства справедливы в любой группе G и не представляют собой соотношений. Однако может произойти нечто более интересное. А именно, элемент x^2 может оказаться равным какому-то из предшествующих элементов, скажем, $x^2 = e$, $x^2 = x$ или $x^2 = x^{-1}$. Эти равенства не вытекают из определения группы (легко привести примеры группы G и элемента x в ней, для которых эти равенства не выполняются!) и представляют собой *соотношения* в группе G. Разберем эти возможности.

∘ Умножив равенство $x^2 = e$ на x^{-1} мы получим равенство $x = x^{-1}$. `Ups!` Это значит, что мы не заметили возможность появления соотношений уже на предыдущем шаге! В этом случае все четные степени x равны e, а все нечетные — x, так что $G = \{e, x\}$ представляет собой циклическую группу C_2 из двух элементов.

∘ Разделив равенство $x^2 = x$ на x, мы получим $x = e$. `Ups!` Это значит, что мы снова не заметили появление соотношения на предыдущем шаге! Ясно, что в этом случае все степени x тоже равны e, так что $G = \{e\}$ представляет собой циклическую группу $\mathrm{C}_1 = 1$ из одного элемента.

∘ А вот равенство $x^2 = x^{-1}$ является новым, мы не могли его увидеть на предыдущем шаге, так как из него не вытекает, что два каких-либо из элементов e, x и x^{-1} совпадают, и значит, мы можем считать, что все они различны. Но вот все остальные степени x будут равны одному из этих элементов. В самом деле, умножая равенство $x^2 = x^{-1}$ на x, мы видим, что $x^3 = e$. Тем самым, $G = \{e, x, x^{-1}\} = \{e, x, x^2\}$ представляет собой циклическую группу C_3 из трех элементов.

Этим возможности приравнять x^2 к чему-то более короткому исчерпаны. Кроме того, обращая равенства $x^{-2} = e, x, x^{-1}$ мы получим уже рассмотренные нами равенства $x^2 = e, x^{-1}, x$, так что никаких новых групп эти соотношения нам не дадут. С другой стороны, теперь мы уже знаем, что новые соотношения могут появиться между только что написанными словами. Это значит, что нам может встретиться еще соотношение $x^2 = x^{-2}$.

∘ Если $x^2 = x^{-2}$, то $x^3 = x^2x = x^{-2}x = x^{-1}$ и $x^4 = x^3x = x^{-1}x = e$. Впрочем, в этом можно убедиться и непосредственно, умножив исходное равенство на x^2. Итак, любая степень x будет совпадать с одной из четырех степеней e, x, x^{-1} или $x^2 = x^{-2}$. Это значит, что в этом случае $G = \{e, x, x^{-1}, x^2\} = \{e, x, x^2, x^3\}$ представляет собой циклическую группу C_4 из четырех элементов.

Продолжим строить все более длинные произведения x и x^{-1}. Теперь мы уже понимаем, что *как групповое слово* любое такое произведение равно x^m для некоторого $m \in \mathbb{Z}$. Таким образом, любое соотношение имеет вид $x^m = x^n$ для некоторых $m, n \in \mathbb{Z}$, $m \neq n$. Сокращая на $x^{\min(m,n)}$ мы можем даже ограничиться соотношениями $x^l = e$. С другой стороны, если у нас есть *два* таких соотношения $x^k = x^l = e$, то у нас есть и соотношение $x^d = e$, где $d = \gcd(k, l)$. Почему? Да потому, что R есть кольцо главных идеалов и, значит наибольший общий делитель допускает там линейное представление, $d = ak + bl$ для некоторых $a, b \in \mathbb{Z}$. Тем самым, $x^d = x^{ak+bl} = x^{ak}x^{bl} = (x^k)^a(x^l)^b = e^a e^b = e$. Это значит, что все соотношения, в которые входит один элемент x, вытекают из *одного* из них, скажем $x^m = e$. Такое m называется **порядком** x и обозначается $o(x)$ или $|\langle x\rangle|$. Равенство $x^n = e$ означает в точности, что n делится на $o(x)$. Если группа G порождается элементом x порядка m, то $G = \{e, x, x^2, \dots, x^{m-1}\}$. Все другие степени x выражаются через эти, например, $x^m = e$, $x^{m+1} = x$, $x^{m+2} = x^2$ и так далее. Точно так же $x^{-1} = x^m x^{-1} = x^{m-1}$, $x^{-2} = x^m x^{-2} = x^{m-2}$ и так далее. Это значит, что любая группа, порожденная одним элементом x, в которой выполнено хотя бы одно нетривиальное соотношение, изоморфна $C_m = \langle x \mid x^m = e\rangle$ для какого-то $m \in \mathbb{N}$. Нам остается рассмотреть еще случай, когда в группе G нет нетривиальных соотношений, в этом случае все степени x попарно различны, так что $G = \{\dots, x^{-2}, x^{-1}, e, x, x^2, \dots\} \cong \mathbb{Z}$ есть бесконечная циклическая группа. Мы еще вернемся к этой теме с другой точки зрения в главе 2. Пока же отметим, что конечная группа G не может содержать бесконечной циклической подгруппы. Поэтому если из каких-то потусторонних соображений известно, что множество X порождает

конечную группу G (например, элементы X изначально выбраны из некоторой другой конечной группы), то для каждой образующей $x \in X$ при каком-то $n \in \mathbb{N}$ из определяющих соотношений должно следовать равенство $x^m = e$. Более того, часто удобно явно указывать порядки всех образующих, например с тем, чтобы записывать все соотношения как *полугрупповые* слова, в которые входят элементы множества X, но не обратные к ним. Сейчас мы увидим именно такой пример.

3. Диэдральные группы. Рассмотрим чуть менее тривиальный пример. Пусть теперь G порождается *двумя* неединичными элементами $x \neq y$, однако для упрощения анализа предположим, что $x^2 = y^2 = e$. Элемент $x \neq e$ такой, что $x^2 = e$ в теории групп принято называть **инволюцией**; группа, порожденная двумя инволюциями, называется **диэдральной**. В этом случае каждое слово в образующих x и y можно записать в виде $xyx\ldots$ или $yxy\ldots$. Почему? Да, конечно, просто потому, что $x^{-1} = x$ и $y^{-1} = y$, так что в записи можно обойтись без отрицательных степеней. С другой стороны, каждое вхождение двух одинаковых букв подряд можно вычеркнуть, с тем, чтобы получить более короткую запись того же элемента. Рассмотрим несколько простейших соотношений, в которые входят обе переменные x и y.

∘ Имеется два слова длины 2, а именно, xy и yx, причем в силу наших предположений относительно x и y эти произведения не могут совпадать ни с e, ни с x, ни с y. Однако они могут, конечно, совпадать между собой, $xy = yx$. Это значит, что элементы x и y коммутируют и в этом случае ни одно более длинное произведение не будет давать новых элементов. Например, $xyx = yxx = y$, $yxy = xyy = x$ и т. д. Это значит, что в этом случае $G = \{e, x, y, xy\}$. Заметим, что с учетом соотношений $x^2 = y^2 = e$ соотношение $xy = yx$ можно переписать в виде $(xy)^2 = xyxy = e$, так что все элементы группы G имеют порядок 2, и, значит, это **четверная группа** V:

$$D_2 = V = \langle x, y \mid x^2 = y^2 = e, xy = yx\rangle = \langle x, y \mid x^2 = y^2 = (xy)^2 = e\rangle.$$

Начинающему, конечно, проще пользоваться соотношением $xy = yx$ а не (эквивалентным!) соотношением $(xy)^2 = e$.

Перейдем теперь к анализу соотношений, которые возникают при рассмотрении слов длины 3. Для этого полезно вспомнить **принцип Дирихле**, который я подробно обсуждаю в книге I. В простейшей форме этот принцип утверждает, что ИЗ ЛЮБЫХ ТРЕХ ОБЫКНОВЕННЫХ ЛЮДЕЙ ПО КРАЙНЕЙ МЕРЕ ДВОЕ ОДНОГО ПОЛА[♯]. Именно эта форма

[♯]Справедливость принципа Дирихле в такой формулировке зависит от неко-

принципа Дирихле нам и понадобится. А именно, любое произведение $xyx\ldots$ или $yxy\ldots$ *нечетной* длины не может равняться никакому произведению такого вида *четной* длины. Почему? Ну, скажем, произведение нечетной длины начинается и заканчивается на *одну и ту же* букву. А вот произведение *четной* длины начинается и заканчивается на *две разные* буквы. Далее по тексту: у нас в наличии три обыкновенные буквы и всего два возможных значения, которые эти буквы могут принимать. Значит по крайней мере две из них совпадают и на эту совпадающую букву можно сократить, так что мы получим более короткое соотношение, в котором снова одна сторона нечетная, а вторая — четная. Продолжая действовать таким образом мы придем к одному из двух (невозможных!) соотношений $x = e$ или $y = e$.

◦ Это значит, что слова длины 3, а именно, xyx и yxy, не могут совпадать ни с e, ни с xy, ни с yx. Конечно, они не могут совпадать и с x или y, так как это означало бы, что $x = y$. Таким образом, единственная возможность это соотношение $xyx = yxy$. Это замечательное соотношение, называемое **braid relation**, является одним из самых важных в математике. В сочетании с соотношениями $x^2 = y^2 = e$ его можно переписать в виде $(xy)^3 = xyxyxy = e$. В группе G, в которой выполняются эти соотношения, 6 элементов, $G = \{e, x, y, xy, yx, xyx = yxy\}$. Как эти элементы умножаются между собой? Чему, например, равно $xyx \cdot y$ или $xyx \cdot yx$? Ну, это ясно, $xyx \cdot y = yxy \cdot y = yx$, а $xyx \cdot yx = yxy \cdot yx = y$.

◦ Посмотрим теперь на слова длины 4. Снова по той же причине они могут давать единственное *новое* соотношение, $xyxy = yxyx$, которое можно переписать в виде $(xy)^4 = e$. Таким образом, в этом случае группа G содержит восемь элементов,

$$G = \{e, x, y, xy, yx, xyx, yxy, xyxy = yxyx\}$$

и начинающий должен попрактиковаться в умножении в этой группе.

◦ Разберем еще пример, когда первое нетривиальное соотношение появляется для слов длины 6, $xyxyxy = yxyxyx$ или, что то же самое, $(xy)^6 = e$. В этом случае в группа G содержит 12 элементов:

$$G = \{e, x, y, xy, yx, xyx, yxy, xyxy, yxyx,$$
$$xyxyx, yxyxy, xyxyxy = yxyxyx\}.$$

торых экстраматематических предположений. Как известно, многие герои Воннегута формулируют принцип Дирихле следующим образом: из любых шести обыкновенных людей по крайней мере двое одного пола.

Теперь уже ясно, что в группу $D_n = \langle x, y \mid x^2 = y^2 = (xy)^n = e\rangle$ входит $2n$ элементов, а именно, произведения $xyx\ldots$ и $yxy\ldots$, в которые входит не более n множителей. Все эти произведения попарно различны, кроме двух самых длинных произведений, в которые входит ровно n множителей и которые равны между собой. Это и будет в точности диэдральная группа. Много дальнейших примеров задания групп небольших порядков приведено в следующем параграфе.

4. Несколько общих замечаний. К заданию группы образующими и соотношениями следует относиться с некоторой осторожностью. Такое задание *в принципе* содержит всю информацию необходимую, чтобы восстановить группу G с точностью до изоморфизма. Однако извлечение этой информации часто оказывается совсем непростым делом. Более того, как мы узнаем в главе 12, не существует никакого алгоритма, который позволил бы даже установить, изоморфны две группы, заданные образующими и соотношениями, или нет. Например, в общем случае, без привлечения какой-то потусторонней информации невозможно даже узнать, тривиальна группа $G = \langle X \mid Y\rangle$, или нет!

Кроме того, даже если отвлечься от принципиальных и алгоритимических аспектов, изучение групп, заданных образующими и соотношениями, представляет значительные трудности в чисто материальном плане. Например, в пункте 2 мы без труда описали группы с *одной* образующей. Нет никакой надежды получить сколь-нибудь обозримый ответ для групп с *двумя* образующими — такие группы обычно называются **2-порожденными**. Почему? Ну хотя бы потому, что любая конечная простая группа порождается двумя элементами, притом многими различными образами. Совсем легко убедиться в том, что любая конечная группа вкладывается в 2-порожденную группу. Если же добавить сюда и бесконечные 2-порожденные группы, ситуация становится и вовсе необозримой. Например, библиографический обзор по теории групп, порожденных **двумя** элементами, опубликованных в 1900–1970 годах (при том, что большинство главных статей в этой области написано за последние 10–15 лет!!), содержит многие сотни работ [43].

Однако с учетом всех этих оговорок задание групп оказывается *чрезвычайно* полезным инструментом самой теории групп и одним из основных сюжетов в применении групп в комбинаторике, топологии, геометрии, теории чисел и т. д. Более того, для групп совсем небольших порядков — скажем, несколько десятков или сотен — или в сочетании с дополнительной информацией о группе, связанной со знанием

ее действия в каком-то представлении, задание групп образующими и соотношениями может оказаться и вполне эффективным средством для вычислений в ней. Каждый серьезный студент должен на самом раннем этапе изучения теории групп овладеть базовой техникой таких вычислений.

§ 7♡. Группы порядков < 32

> Solche inductive Untersuchungen sind namentlich darum nützlich, weil sie eine Fülle bemerkenswerther allgemeiner Eigenschaften der Gruppen liefern.
>
> Georg Frobenius. *Über auflosbare Gruppen* I

В настоящем параграфе мы перечислим все группы порядка < 32 с точностью до изоморфизма. Группы порядков ≤ 8 были классифицированы Кэли в 1859 году [44], а порядков ≤ 12 — им же в 1889 году [45]. Группы порядка < 32 классифицированы Джорджем Миллером, который в 1896 году [46] сделал последний трудный шаг, описав группы порядка 24. В том же году группы порядка 24 были описаны Ле Вавассером [47]. Однако его краткий анонс содержит опечатки и не дает никакого намека на доказательства. В том же году [48] Миллер смог классифицировать группы порядка 32 — и, тем самым, все группы порядка < 48, а еще через два года [49] он добил случай групп порядка 48 и, тем самым, классифицировал все группы порядка < 64. После этого Миллер еще лет 40–50 занимался подобной деятельностью и к 1930 году [50], [51] дошел до групп порядка 96, дезавуировав при этом свою работу о группах 32 и сделав десятки ошибок в списках групп порядков 64 и 96 — в главе 9 мы еще вернемся к драматической истории классификации групп порядка 32 и 64! К середине 1930-х годов Синиор и Ланн [52], [53] в основном описали группы порядков ≤ 200. В главе 9 мы обсуждаем современное состояние этого вопроса и, в частности, полученный в 2001 году список всех групп порядка ≤ 2000.

Включение в тексты по теории групп списка всех групп порядка < 32 имеет давнюю традицию, восходящую, видимо, к книге Бернсайда. Замечу, что § 118 его книги специально посвящен группам порядка 16, а § 126 — группам порядка 24. Как мы сейчас увидим, это как раз два трудных случая и их-то он полностью разбирает. Для остальных случаев он либо ссылается на общие теоремы, такие как воспроизведенное в § 59 его книги описание групп порядка p^2q, либо ограничивается формулировкой ответа, указывая, что все порядки < 32 разбираются так же, как порядок 24, но *гораздо проще*. Список

Джордж Абрам Миллер (George Abram Miller, 31 июля 1863, Lynnville, Пеннсильвания — 10 февраля 1951, Урбана, Иллинойс) — замечательный американский математик, один из классиков теории конечных групп. В 1895–1897 годах он учился в Европе, где посещал лекции Ли и Жордана. Все 359 статей, включенных в его собрание сочинений (а всего он написал около 800 работ, примерно половина из которых научно-популярные!), посвящены почти исключительно теории конечных групп: "К моменту окончания своего обзора по общей теории групп в 1939 году Магнус оценивал общий объем литературы по теории групп в 8000 статей. Около 4% из них принадлежало одному автору — Дж.Миллеру" ?? , с. 212. В своих исторических штудиях О'Коннор и Робертсон следующим образом отзываются о деятельности Миллера: "Although interesting because it was done at an early stage, his work fails to show much depth". Причины такого отношения мне понятны, и я вынужден согласиться, что Миллер не был математиком такого калибра, как Кэли, Фробениус или Бернсайд. Тем не менее, с моей точки зрения, и сегодня многие его работы представляют не исторический, а вполне реальный научный интерес. Просто темы, которыми он занимался, такие, как явные задания, группы малых порядков, экономное порождение и пр. надолго вышли из моды. Однако последние лет 15–20, после завершения классификации конечных простых групп все эти вопросы снова оказались в центре интересов многих ведущих специалистов по теории групп. При этом выяснилось, что все, что можно было сделать в этой области до компьютеров — и до появления новых мощных методов, связанных с алгебраическими группами, геометрией и классификацией конечных простых групп — можно найти уже у Миллера: *es steht schon bei Miller*. Хотя и не всегда безошибочно! Написанная им совместно с Блихфельдом и Диксоном книга стала классикой теории групп. Он завещал университету Иллинойса в Урбане, где преподавал 25 лет, миллион долларов, все деньги, которые он получил от университета за время работы там!!

групп порядка < 32 приводится также в книге Миллера, Блихфельда и Диксона и в учебнике Кармайкла. Чуть другие задания этих групп приведены в книге Коксетера и Мозера ?? (таблица 1. неабелевы группы порядка < 32). В своем учебнике де Сегье [**344**] идет еще дальше и приводит список групп порядка 32 (§§ 154–159). Порядок 32 представляет собой *естественную* границу, после которой описание *всех* групп становится довольно затруднительным для того, кто не вооружен *мощной теорией и компьютером* (как говорил по этому поводу Аль Капоне, я неоднократно имел возможность проверить, что доброе слово и пистолет убеждают гораздо лучше, чем просто доброе слово).

После изучения главы 9 читатель сможет *без труда* доказать **все** содержащиеся в настоящем параграфе утверждения. Сложнее всего описываются группы, порядки которых делятся на большую степень 2 или 3. Изучив, кроме того, главу 7, читатель смог бы *в принци-*

не классифицировать группы *почти* всех порядков < 1000. Это не относится к порядкам, делящимся на непомерно большую степень 2: даже с использованием всех возможных **дивайсов** описание групп порядков 512, 768 и 1024 представляет собой серьезную исследовательскую проблему и было завершено только в 2000–2002 годах. Это спорт несколько другого рода, чем описание всех групп порядка 48, которым занимались профессионалы век назад[♮]. Но для того, чтобы проверить хотя бы только список *простых* групп порядка $< 100\,000\,000$, который мы приводим в главе 10, он должен был бы пользоваться уже гораздо более глубокими и трудными результатами. Что касается описания *всех* групп такого порядка, то при сегодняшнем уровне вычислительных возможностей об этом не может быть и речи.

• **Группы порядка p.** Если $n = p$ — простое число, то существует **единственная** группа порядка n, а именно, циклическая группа C_n. Простые порядки меньшие 32, это $\mathbf{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31}$.

• **Группы порядка $\mathbf{p^2}$.** Как заметил в 1882 году Эужен Нетто, существуют всего **две** неизоморфные группы порядка p^2, обе абелевы:

⋆ циклическая, C_{p^2},

⋆ элементарная абелева $E_{p^2} = C_p \times C_p$.

Имеющие такой вид порядки, меньшие 32 — это $\mathbf{4, 9}$ и $\mathbf{25}$. Порядок 4 — это первый порядок, в котором существуют **две** неизоморфные группы, циклическая группа C_4 и **четверная группа** $V = C_2 \times C_2$.

• **Группы порядка 2p.** В порядках $2p$, где $p \geq 3$ — простое число, существуют **2** неизоморфные группы, абелева и неабелева:

⋆ циклическая группа $C_{2p} \cong C_3 \times C_2$,

⋆ диэдральная группа $D_p = \langle x, y \mid x^2 = y^2 = (xy)^p = 1 \rangle$, она же группа треугольника $T(2, 2, p)$.

Имеющие такой вид порядки, меньшие 32 — это $\mathbf{6, 10, 14, 22}$ и $\mathbf{26}$. Порядок 6 — это первый порядок, в котором существует неабелева группа $S_3 \cong D_3$.

• **Группы порядка $\mathbf{p^3}$.** В порядке p^3 существуют уже **5** неизоморфных групп, **3** абелевых и **2** неабелевых. Абелевы группы:

[♮]См. цитированную выше работу Миллера 1898 года, а также [54]: “имеется 30 групп порядка 48, не говоря о 34 разложимых группах”. Искать новые группы порядка 48 вручную — занятие не для слабонервных, так как для этого нужно как минимум детально понимать строение групп порядка 16, например, знать их группы автоморфизмов. Однако после чтения настоящего параграфа Вы можете в качестве полезного упражнения проверить вторую часть этого высказывания.

⋆ циклическая группа C_{p^3},

⋆ группа $C_{p^2} \times C_p$,

⋆ элементарная абелева группа $E_{p^3} = C_p \times C_p \times C_p$.

Существуют два порядка вида p^3 меньшие 32, это **8** и **27**.

Неабелевы группы порядка **8**:

⋆ диэдральная группа $D_4 = \langle x, y \mid x^2 = y^2 = (xy)^4 = 1 \rangle$,

⋆ группа кватернионов $Q = \langle 2, 2, 2 \rangle$ с заданием

$$\langle x, y \mid x^2 = y^2 = (xy)^2 \rangle .$$

Неабелевы группы порядка **27** детально обсуждаются в главе 7.

• **Группы порядка 12.** Имеется **5** неизоморфных групп порядка $12 = 2^2 \cdot 3$, из которых **2** абелевых и **3** неабелевых. Абелевы группы:

⋆ циклическая $C_{12} = C_4 \times C_3$,

⋆ нециклическая $C_6 \times C_2$.

Неабелевы группы

⋆ диэдральная $D_6 = S_3 \times C_2$,

⋆ знакопеременная A_4, она же собственная группа тетраэдра T^+, она же группа треугольника†

$$T(3, 3, 2) = \langle x, y \mid x^3 = y^3 = (xy)^2 = 1 \rangle .$$

⋆ метациклическая группа

$$\overline{T}(2, 2, 3) = \langle 2, 2, 3 \rangle = \langle x, y \mid x^2 = y^2 = (xy)^3 \rangle .$$

Эту группу можно истолковать еще как полупрямое произведение $C_3 \leftthreetimes C_4$, отвечающее нетривиальному действию C_4 на C_3. Иными словами, она задается еще следующим образом:

$$\langle x, y \mid x^4 = y^3 = 1, xyx^{-1} = y^{-1} \rangle .$$

Эту группу можно мыслить еще в представлении

$$\left\langle x = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, y = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \right\rangle .$$

†В книге Коксетера—Мозера ошибочно напечатано $T^2 = 1$, должно быть $T^3 = 1$.

• **Группы порядка pq.** Группы порядков pq, где $p, q \geq 3$ — различные простые числа, детально изучены в главе 7. Имеется два порядка такого вида, меньших 30, а именно, $15 = 5 \cdot 3$ и $21 = 7 \cdot 3$. В качестве одной из первых иллюстраций теорем Силова, мы докажем, что существует **единственная** группа порядка **15**, а именно, C_{15} и **2** группы порядка **21**, а именно,

⋆ циклическая группа C_{21},

⋆ **группа Фробениуса** $C_7 \leftthreetimes C_3$ с заданием‡

$$\langle x, y \mid x^3 = y^7 = 1, xyx^{-1} = y^2 \rangle .$$

• **Группы порядка 16.** Существует **14** неизоморфных групп порядка 16, из которых **5** абелевых и **9** неабелевых. Абелевы группы:

⋆ циклическая C_{16},

⋆ $C_8 \times C_2$,

⋆ гомоциклическая группа $C_4 \times C_4$,

⋆ $C_4 \times C_2 \times C_2$,

⋆ элементарная абелева $E_{2^4} = C_2 \times C_2 \times C_2 \times C_2$,

Описание неабелевых групп порядка 16 представляет собой уже вполне достойное упражнение, переходящее в `уебунг`* и обычно автор рекомендует его только наиболее настырным студентам♯:

⋆ диэдральная группа D_8,

⋆ прямое произведение $D_4 \times C_2$,

⋆ прямое произведение $Q \times C_2$,

⋆ **квазидиэдральная группа** порядка 16, с заданием

$$\langle x, y \mid x^2 = y^8 = 1,\ xyx^{-1} = y^3 \rangle ,$$

---

‡В книге Коксетера—Мозера соотношение $S^7 = 1$ пропущено.

*`Уебунг`, от немецкого `Übung` (в традиционной орфографии `Uebung`), — термин Василеостровского диалекта, обозначающий утомительное упражнение, требующее для своего выполнения значительного времени и усилий.

♯**Анекдот:** в середине 1960-х годов будущий профессор Анатолий Владимирович [Яковлев] дал будущему доценту Сергею Сергеевичу [Валландеру] на экзамене следующую задачу на отличную оценку: классифицировать группы порядка p^5. Из этого факта не следует делать вывод о резком падении уровня преподавания на мат-мехе за прошедшие 40 лет, так как после пяти часов напряженной работы, написав список групп порядка p^5, но еще не доказав, что других нет, Сергей Сергеевич неожиданно выяснил, что Анатолий Владимирович имел в виду классификацию *абелевых* групп порядка p^5.

Фердинанд Георг Фробениус (Ferdinand Georg Frobenius, 26 сентября 1849 — 03 августа 1917, Берлин) — гениальный немецкий алгебраист, основные работы которого относятся к теории чисел, теории алгебр (или, как тогда было принято говорить, гиперкомплексных систем), теории матриц, теории конечных групп и их представлений, алгебраической и дифференциальной геометрии. После учебы в Берлине, где он слушал лекции Кронекера, Куммера и Вейерштрасса, и Геттингене, уже в 1870 году Фробениус защищает диссертацию под руководством Вейерштрасса, который всегда считал Фробениуса своим лучшим учеником.

После кратковременной работы в школе, в 1875 году Фробениус стал профессором в Цюрихе, а в 1902 году — в Берлине. Фробениус начинал свою научную деятельность как аналитик, и около трети его опубликованных работ посвящено анализу. Однако потом он почти полностью переключился на теорию групп, алгебр и теорию представлений.

С моей точки зрения именно Фробениус был создателем теории групп как отдельной математической дисциплины. Если какая-то теорема в начальном курсе теории групп (например, теорема о строении конечнопорожденных абелевых групп) рутинно упоминается без имени автора, то примерно в половине случаев ее впервые явно сформулировал и/или доказал именно Фробениус.

В нашем курсе встречаются теорема Фробениуса о гиперкомплексных системах, несколько десятков — sic!! — теорем Фробениуса о группах, формула индекса Фробениуса, группы, подгруппы и ядра Фробениуса, эндоморфизм Фробениуса, клетки Фробениуса и фробениусова форма матриц, несколько формул Фробениуса в теории матриц, неравенство Фробениуса, теорема Фробениуса—Перрона и т. д. В книге IIbis по крайней мере половина всех результатов о представлениях конечных групп принадлежит Фробениусу.

Будучи великим математиком, Фробениус не был столь же великим организатором. При Кронекере, Куммере и Вейерштрассе математический факультет Берлинского университета был лучшим математическим факультетом в Германии, однако в конце XIX века и начале XX века при Клейне и Гильберте Геттинген резко вырывается вперед. В результате *антипатия Фробениуса к Клейну не знала границ* [55], [56].

⋆ **обобщенная кватернионная группа** порядка 16 с заданием

$$\left\langle x, y \mid x^2 = y^4,\ xyx^{-1} = y^{-1} \right\rangle,$$

⋆ группа $G_{4,4}$ с заданием

$$\left\langle x, y \mid x^4 = y^4 = (xy)^2 = 1,\ xy^3 = yx^3 \right\rangle,$$

⋆ группа с заданием

$$\left\langle x, y \mid x^2 = y^8 = 1,\ xyx^{-1} = y^5 \right\rangle,$$

⋆ группа с заданием

$$\left\langle x, y \mid x^4 = y^4 = 1,\ xy = yx^3 \right\rangle,$$

⋆ группа с заданием

$$\left\langle x, y, z \mid x^2 = y^2 = z^4 = 1, xz = zx, yz = zy, z^2 = (xy)^2 \right\rangle.$$

• **Группы порядка 18.** Имеется **5** неизоморфных групп порядка $18 = 2 \cdot 3^3$, **2** абелевых и **3** неабелевых. Абелевы группы:

⋆ циклическая $C_{18} = C_9 \times C_3$,

⋆ нециклическая $C_6 \times C_3$.

Неабелевы группы

⋆ диэдральная D_9,

⋆ прямое произведение $S_3 \times C_3$,

⋆ полупрямое произведение $(C_3 \times C_3) \leftthreetimes C_4$, отвечающее действию C_2 на $C_3 \times \mathrm{C}_3$ обращением. Иными словами, эта группа допускает задание

$$\left\langle x, y, z \mid x^2 = y^3 = z^3 = 1,\ yz = zy,\ xyx^{-1} = y^{-1},\ xzx^{-1} = z^{-1} \right\rangle.$$

• **Группы порядка 20.** Имеется **5** неизоморфных групп порядка $20 = 2^2 \cdot 5$, **2** абелевых и **3** неабелевых. Абелевы группы:

⋆ циклическая $C_{20} = C_5 \times C_4$,

⋆ нециклическая $C_{10} \times C_2$.

Неабелевы группы:

⋆ диэдральная D_{10},

⋆ метациклическая группа $\mathrm{C}_5 \leftthreetimes C_4$ с заданием

$$\left\langle x, y \mid x^4 = y^5 = 1,\ xyx^{-1} = y^{-1} \right\rangle.$$

⋆ **Группа Фробениуса** $\mathrm{C}_5 \leftthreetimes C_4$ порядка 20 с заданием

$$\left\langle x, y \mid x^4 = y^5 = 1,\ xyx^{-1} = y^2 \right\rangle.$$

Как подгруппа в S_5 она порождена циклами $x = (2345)$ и $y = (12345)$.

• **Группы порядка 24.** Это первый случай, после групп порядка 16, который требует некоторого размышления. Всего имеется **15**

неизоморфных групп порядка $24 = 2^3 \cdot 3$, из которых **3** абелевых и **12** неабелевых, однако **6** из этих неабелевых групп получаются как произведения неабелевых групп порядка 6 или 12 на абелевы группы, так что в реальности, нам нужно найти только **6** новых групп порядка 24. Абелевы группы:

⋆ циклическая $C_{24} = C_8 \times C_3$,

⋆ $C_{12} \times C_2 \cong C_6 \times C_4$,

⋆ $C_6 \times C_2 \times \mathrm{C}_2$.

Неабелевы группы, являющиеся прямыми произведениями:

⋆ $S_3 \times C_4$,

⋆ $S_3 \times C_2 \times C_2 \cong D_6 \times C_2$,

⋆ $D_4 \times C_3$,

⋆ $Q \times C_3$,

⋆ $A_4 \times C_2$,

⋆ $G \times C_2$, где G — группа порядка 12, не изоморфная D_6 и A_4.

Для незрелого читателя описание новых неабелевых групп порядка 24 тоже превращается в уебунг, однако, поскольку этот уебунг многократно проделывался в учебниках теории групп, начиная с книги Бернсайда, я вопроизведу его результат.

⋆ диэдральная группа D_{12},

⋆ симметрическая группа S_4, она же группа тетраэдра T, она же собственная группа куба O^+, она же группа треугольника

$$T(2,3,4) = \left\langle x, y \mid x^2 = y^3 = (xy)^4 = 1 \right\rangle,$$

⋆ бинарная группа тетраэдра $T^\star$, которую мы строим в главе 3 как подгруппу в мультипликативной группе целых гурвицевых кватернионов, она же расширенная группа треугольника

$$\overline{T}(2,3,3) = \langle 2,3,3 \rangle = \left\langle x, y, z \mid x^2 = y^3 = z^3 = xyz \right\rangle,$$

⋆ группа

$$(4,6,2,2) = \left\langle x, y \mid x^4 = y^6 = (xy)^2 = (x^{-1}y)^2 = 1 \right\rangle,$$

⋆ метациклическая группа

$$\langle -2,2,3 \rangle = \left\langle x, y, z \mid x^2 = y^2 = (xy)^3 \right\rangle,$$

⋆ дициклическая группа

$$\langle 2,2,6\rangle = \left\langle x,y \mid x^2 = y^2 = (xy)^6 \right\rangle .$$

• **Группы порядка 28.** Имеется **4** неизоморфные группы порядка $28 = 2^2 \cdot 7$, **2** абелевых и **2** неабелевых. Абелевы группы:

⋆ циклическая $C_{28} = C_7 \times C_4$,

⋆ нециклическая $C_{14} \times C_2$.

Неабелевы группы:

⋆ диэдральная D_{14},

⋆ прямое произведение $D_7 \times C_2$.

• **Группы порядка 30.** Имеется **4** неизоморфные группы порядка $30 = 2 \cdot 3 \cdot 5$, **1** абелева и **3** неабелевых. Единственная абелева группа — циклическая

$$C_{30} \cong \mathrm{C}_{15} \times C_2 \cong \mathrm{C}_{10} \times C_3 \cong \mathrm{C}_6 \times C_5 \cong \mathrm{C}_5 \times C_3 \times C_2.$$

Неабелевы группы:

⋆ диэдральная D_{15},

⋆ прямое произведение $D_5 \times C_3$,

⋆ прямое произведение $S_3 \times C_5$.

Это завершает описание всех групп порядка до 31 включительно. Тот, кто не понимает, почему мы остановились здесь, может проделать *такое* упражнение.

Уебунг. Опишите все неизоморфные группы порядка 32.

Brutta ora il mattino. Ну, Миллер занимался этим 40 лет, *с переменным успехом.* С утра их 51 штука, а к вечеру 47 — см. главу 9.

§ 8♡. Граф Кэли

Сейчас мы изложим еще один геометрический подход к образующим и соотношениям.

Пусть G — группа, а $X \subseteq G$ какое-то ее подмножество. **Граф Кэли** $\Gamma(G,X)$ (называемый также просто **графом группы**, `Gruppenbild`) группы G по отношению к множеству X выглядит следующим образом. Это цветной граф, вершинами которого являются элементы группы G, а цвета дуг соответствуют элементам X. Две вершины $h, g \in G$ соединяются дугой цвета x, направленной от h к g, если $hx = g$. Получающийся при этом граф обладает чрезвычайно высокой степенью

однородности, из каждой вершины в нем выходит *единственная* дуга каждого цвета — в самом деле, любой элемент h группы G можно умножить на любой элемент $x \in X$, причем результат определен однозначно. Заметим, что прохождение дуги в отрицательном направлении интерпретируется как умножение на x^{-1}. Иными словами, наличие дуги цвета x, направленной из h в g можно истолковать еще как $gx^{-1} = h$. В силу только что сказанного, в каждую вершину графа Кэли входит *единственная* дуга каждого цвета.

Для многих приложений особенно интересна ситуация, когда $x = x^{-1}$, иными словами, когда x является **инволюцией**, т. е. $x^2 = e$. При этом $hx = g$ в том и только том случае, когда $gx = h$, так что мы должны были бы соединить h и g *парой* противоположно направленных дуг цвета x. Вместо этого обычно изображается одно ребро цвета x.

Чаще всего ограничиваются рассмотрением случая, когда получающийся граф связен. В этом случае говорят, что группа G **порождается множеством** X или, что X является **системой образующих** группы G. Это значит, что любой элемент $h \in G$ — или, что то же самое, нейтральный элемент $e \in G$ — соединен с любым другим элементом некоторым путем, все дуги которого помечены элементами X. При этом дуги можно проходить как в положительном, так и в отрицательном направлении. Иными словами, множество X в том и только том случае является системой образующих группы G, когда любой элемент группы G можно представить в виде $x_1 \dots x_n$, где $n \in \mathbb{N}_0$, причем $x_i \in X$ или $x_i^{-1} \in X$ для каждого $i = 1, \dots, n$.

• Пусть $G = \mu_n$ — циклическая группа порядка n, а $X = \{\xi\}$ — образующая этой группы (первообразный корень из 1). Тогда граф Кэли $\Gamma(G, X)$ это цикл длины n.

• Если $G = \mathbb{Z}$ — бесконечная циклическая группа, $X = \{1\}$. Тогда граф Кэли $\Gamma(G, X)$ это бесконечная цепочка.

Граф Кэли группы G самым существенным образом зависит от выбора множества X, так как при разном выборе X одна и та же группа может давать абсолютно разные графы. Наоборот, группа G не определяется топологией своего графа Кэли как таковой, чрезвычайно существенна также раскраска дуг графа **и их направление**! Чтобы убедиться в этом, рассмотрим две группы порядка 6.

Задача. Изобразите графы Кэли групп $G = C_6$, S_3 относительно двухэлементной системы образующих X, состоящей из элемента порядка 2 и элемента порядка 3. Найдите отличие!

Следующее упражнение весьма полезно для начинающего, чтобы почувствовать, что такое образующие и соотношения. Для групп порядка 12 и 16 это упражнение проделывается легко, для групп порядка 24 требует уже некоторого труда. Для групп порядка 60 (ну, скажем, кроме циклической и диэдральной) красиво и правильно нарисовать граф Кэли с первой попытки уже не удастся.

Задача. Нарисуйте графы Кэли нескольких групп перечисленных в предыдущем параграфе относительно приведенных там систем образующих.

Задача. Что можно сказать про граф $\Gamma(H \times G, X \sqcup Y)$, где X и Y — системы образующих в H и G соответственно. Как выглядят соотношения между элементами X и Y?

Задача. Представьте себе граф Кэли $G(\mathbb{Z}^n, \{e_1, \dots, e_n\})$, где, как обычно,

$$e_1 = (1, 0 \dots, 0), \dots, e_n = (0, \dots, 0, 1).$$

Начните со случая $n = 2$!

Граф Кэли совершенно замечателен тем, что он позволяет визуализировать элементы группы, ее образующие и соотношения. Составим небольшой словарик, позволяющий переводить понятия, связанные с группой G, на язык ее графа Кэли $\Gamma(G, X)$:

элемент группы G	вершина Γ
элемент множества X	цвет ребер графа Γ
X порождает G	граф Γ связен
слово в образующих X	путь с ребрами нужных цветов
умножение в G	последовательное прохождение путей
соотношение между элементами X	цикл в Γ
определяющие соотношения	независимые циклы, начинающиеся в фиксированной вершине

Например, так как между элементами свободной системы образующих X свободной группы F нет вообще никаких соотношений, ее граф Кэли $\Gamma(F, X)$ вообще не содержит циклов, т. е. является *деревом*. Это соображение играет ключевую роль в главе 11.

§ 9♢. Группы симметрий

Симметрии любого объекта образуют группу, и сейчас мы рассмотрим простейшие примеры групп симметрий.

1. Группы симметрий в трехмерном пространстве. Сейчас мы приведем несколько простейших примеров конечных подгрупп в группе $O(3, \mathbb{R})$ вращений трехмерного эвклидова пространства. В следующем параграфе мы покажем, что построенными здесь группами C_n, D_n, T^+, O^+, I^+ исчерпываются все конечные подгруппы в группе собственных вращений $\mathrm{SO}(3, \mathbb{R})$.

• **Группа вращений правильного n-угольника.** Пусть Γ — правильный n-угольник на эвклидовой плоскости. Тогда поворот Γ на любой угол кратный $2\pi/n$ вокруг центра Γ совмещает Γ с собой. Все такие повороты образуют конечную группу C_n порядка n, изоморфную группе μ_n корней степени n из 1, называемую **циклической группой порядка** n. Каждый ее элемент является степенью поворота на угол $2\pi/n$. Буква `C` в обозначении C_n как раз и происходит от английского названия `cyclic group`, в старых книгах эта группа обычно обозначается Z_n, от немецкого `zyklische Gruppe`. Эту группу можно рассматривать и как полную группу симметрий некоторых трехмерных тел, например, правильной n-угольной пирамиды. /

• **Группа симметрий правильного n-угольника.** Рассмотрим теперь все движения эвклидовой плоскости, переводящие Γ в себя. Кроме вращений сюда относятся также отражения относительно прямых, проходящих через две противоположные вершины Γ или середины противоположных сторон (если n четно), либо через какую-то вершину и середину противоположной стороны (если n нечетно). Композиция двух отражения является вращением. Получающаяся так группа порядка $2n$ обозначается D_n и называется **группой диэдра** alias **диэдральной группой**. Буква `D` в обозначении происходит от названия `Diedergruppe` — `dihedral group`. Эту группу можно рассматривать и как полную группу симметрий некоторых трехмерных тел, например, правильной n-угольной призмы или правильной n-угольной бипирамиды.

Задача. Опишите группу симметрий i) свастики или **совастики***, ii) прямоугольника, не являющегося квадратом. Изоморфны ли эти группы?

Пусть теперь Γ — правильный многогранник в трехмерном пространстве. Так как любое эвклидово движение, сохраняющее Γ, сохраняет и двойственный многогранник, можно ограничиться случаем, когда Γ тетраэдр, куб или додекаэдр. Легко убедиться, что порядок группы симметрий Γ в этих случаях будет принимать значения 24, 48, 120, соответственно. Собственных вращений, не меняющих ориентацию пространства, в каждом случае ровно в 2 раза меньше.

• **Группы тетраэдра.** Перечислим все 24 эвклидовых движения, сохраняющих правильный тетраэдр. Прежде всего, это следующие 12 вращений, образующих **собственную группу тетраэдра** T^+ (от немецкого `eigentliche Tetraedergruppe`), изоморфную знакопеременной группе A_4:

◦ тождественное преобразование,

---

*`Совастика` — индийский религиозный символ, симметричный по отношению к свастике. Иными словами, совастика представляет собой равносторонний крест, концы которого загнуты под прямым углом *влево*, в то время как у свастики они загнуты под прямым углом *вправо*. По-видимому, альтернативные чтения `сувастика`, `саувастика` и `сууастика` ближе к санскритскому оригиналу. Однако по привычке я придерживаюсь традиционного петербургского произношения: “я заметил затем на стене у одного из окон комнаты Их Величеств любимый знак Государыни `совастику`, который она приказывала всюду изображать на счастье”. — П.Жильяр, *Император Николай* II *и его семья*. В любом случае, это чрезвычайно удивительное свидетельство, так как совастика была символом богини Кали и рассматривалась в оккультных науках как **`нефастный`** символ.

∘ 8 вращений, на углы $2\pi/3$ и $4\pi/3$, вокруг четырех осей, соединяющих вершины с центрами противоположных граней,

∘ 3 вращения, на угол π, вокруг трех осей, соединяющих середины скрещивающихся ребер.

Вращения осуществляют *четные* перестановки вершин. Кроме того, имеется 12 несобственных движений тетраэдра, осуществляющих *нечетные* перестановки, а именно

∘ 6 симметрий относительно шести плоскостей, проходящих через ребра,

∘ 6 композиций вращений с отражениями, перемещающих все четыре вершины;

таким образом, вся **группа тетраэдра** T (от немецкого `Tetraedergruppe`) изоморфна S_4.

• **Группы куба.** Имеется 48 эвклидовых движений, переводящих куб (как и октаэдр) в себя. Перечислим все 24 эвклидовых вращения, сохраняющих куб. Эти вращения образуют **собственную группу куба** O^+ (от немецкого `eigentliche Oktaedergruppe`, известную также под народным названием `eigentliche Würfelgruppe`, что объясняет используемое некоторыми авторами для этой группы обозначение W^+), изоморфную S_4. Вот они:

∘ тождественное преобразование, /

∘ 6 вращений, на углы $\pi/2$, $3\pi/2$ вокруг трех осей, соединяющих центры противоположных граней,

∘ 3 вращения, на углы π вокруг трех осей, соединяющих центры противоположных граней,

∘ 8 вращений, на углы $2\pi/3$ и $4\pi/3$, вокруг четырех осей, соединяющих пары противоположных вершин, называемых в дальнейшем диагоналями куба,

∘ 6 вращений, на угол π, относительно шести осей, соединяющих середины противоположных ребер.

Замечание. Мы различаем два типа вращений вокруг осей, соединяющих центры противоположных граней, так как вращения на углы $\pi/2$, $3\pi/2$ имеют порядок 4, а вращение на угол π — порядок 2. Поэтому они представляют собой два разных класса сопряженности в группе симметрий куба.

Убедимся в том, что O^+ изоморфна S_4. Ясно, что любая симметрия куба переводит в себя множество его диагоналей. Легко видеть, что

уже вращения куба осуществляют все 24 перестановки этого множества. Отражения же могут, кроме того, переставлять концы диагоналей. То же самое мы можем увидеть и несколько иначе — в терминах октаэдра. Для этого отсечем у тетраэдра углы так, чтобы секущие плоскости делили его ребра пополам. Ясно, что все 24 симметрии исходного тетраэдра сохраняют получившийся октаэдр, причем в терминах октаэдра все симметрии исходного тетраэдра реализуются как вращения.

Все 48 симметрий куба образуют **группу куба** O (`Oktaedergruppe`, некоторые авторы называют ее `Würfelgruppe` и обозначают W). Ясно, что O порождается O^+ и симметрией i относительно центра куба. Симметрия i является *центральной* инволюцией, иными словами, $i^2 = 1$ и $gi = ig$ для всех $g \in O^+$. В этом проще всего убедиться используя матричную реализацию O. Для этого расположим куб так, чтобы его центр совпал с началом координат, а ребра были параллельны координатным осям. Тогда элемент O изобразится матрицей из вещественной ортогональной группы $O(3,\mathbb{R})$, причем i соответствует матрица $-e$, которая, очевидно, центральна в $O(3,\mathbb{R})$ (читатель, уже знакомый с матрицей линейного преобразования, может попытаться найти и матрицы остальных элементов группы O). Тем самым, $O = O^+ \times \langle i \rangle \cong S_4 \times C_2$.

Комментарий. Имеет место замечательный исключительный изоморфизм $O \cong S_3 \wr C_2 = S_3 \leftthreetimes C_2^3$, который отвечает за существование внешнего автоморфизма у группы S_6. Группа $O = S_3 \wr C_2$ часто называется **октаэдральной группой**, но мы хотим зарезервировать этот термин для многомерного обобщения $\mathrm{Oct}_n = S_n \wr C_2 = S_n \leftthreetimes C_2^n$ — того, что часто называется **группа гиперкуба** или **гипероктаэдральная группа**.

• **Группы икосаэдра.** Перечислим все 60 эвклидовых вращений, сохраняющих икосаэдр (как и додекаэдр). Эти вращения образуют **собственную группу икосаэдра** I^+ (`eigentliche Ikosaedergruppe`), изоморфную A_5. Это

◦ тождественное преобразование,

◦ $24 = 12+12$ вращений на углы $2\pi/5$, $4\pi/5$, $6\pi/5$, $8\pi/5$ вокруг осей, соединяющих центры противоположных граней,

◦ 20 вращений на углы $2\pi/3$, $4\pi/3$ вокруг осей, соединяющих пары противоположных вершин,

◦ 15 вращений на угол π относительно осей, соединяющих середины противоположных ребер.

Замечание. В действительности, 24 вращения вокруг осей, соединяющих центры противоположных граней разбиваются на 2 класса

сопряженности, кажлый из которых содержит по 12 элементов. При изоморфизме с A_5 эти классы отвечают двум классам 5-циклов с представителями (12345) и (12354), соответственно.

Интересено увидеть, где те 5 символов, которые переставляются группой икосаэдра? В терминах икосаэдра их можно описать, например, следующим образом: 15 осей симметрии, проходящих через середины противоположных ребер, разбиваются на 5 троек попарно ортогональных осей. Ясно, что любая симметрия икосаэдра переводит тройку ортогональных осей в тройку ортогональных осей. При этом вращения икосаэдра осуществляют лишь четные перестановки такие троек. Заметим, что в терминах самой группы тройка ортогональных осей это в точности подгруппа порядка 4.

Дадим теперь чуть иное описание тех же 5 элементов в терминах додекаэдра. У додекаэдра 20 вершин, которые можно разбить на 5 групп по 4 вершины так, чтобы каждая четверка задавала правильный вписанный тетраэдр и эти 5 правильных тетраэдров переводились друг в друга вращениями. В действительности, существует еще одна конфигурация 5 правильных вписанных тетраэдров, которая переводится в исходную конфигурацию отражением.

Все 120 симметрий икосаэдра, как собственные, так и несобственные, образуют **группу икосаэдра** I (`Ikosaedergruppe`). Порядок группы I равен порядку группы S_5, но I изоморфна не S_5, а $A_5 \times C_2$. Чтобы убедиться в этом, достаточно заметить, что I порождается I^+ и симметрией i относительно центра икосаэдра. Таким образом, центр группы I равен i, в то время как S_5 — группа без центра. Некоторые авторы обозначают группы I^+ и I через Y^+ и Y соответственно.

2. Многомерные обобщения. Обобщение этих примеров на многомерный случай представляет собой содержание нескольких больших разделов математики (см., в частности, ??), и на том уровне понимания теории групп, на котором мы пока находимся, мы не можем, конечно, углубиться в эту тему. Ограничимся поэтому двумя простейшими примерами, первый из которых нам уже известен, а второй может оказаться новым; два дальнейших четырехмерных примера обсуждаются в § 7.

В каждой размерности $n \geq 2$ существует два следующих правильных многогранника: правильный симплекс (равносторонний треугольник, правильный тетраэдр, ...) и гиперкуб (квадрат, куб, ...). Кроме того, в размерностях $n \geq 3$ гиперкуб отличается от своего двойственного многогранника, называемого гипероктаэдром. Пусть $V = \mathbb{R}^n$ — n-мерное эвклидово пространство с ортонормированным базисом $e_1, \dots, e_n$. Ортонормированность базиса означает, что $(e_i, e_j) = \delta_{ij}$, иными словами, любые два вектора e_i, e_j, $i \neq j$, ортогональны, и каждый вектор e_i имеет длину 1.

• **Симплекс.** Проще всего построить правильный n-мерный симплекс не в n-мерном, а в $(n+1)$-мерном пространстве, а именно, $e_1, \dots, e_{n+1} \in \mathbb{R}^{n+1}$ как раз

и образуют вершины такого симплекса (расстояние между любыми двумя из них равно $\sqrt{2}$). В действительности, конечно, эти $n+1$ вершин лежат в n-мерном линейном подмногообразии

$$\{a_1e_1 + \ldots + a_{n+1}e_{n+1} \mid a_1 + \ldots + a_{n+1} = 1\}$$

и *при желании* их можно запихнуть обратно в n-мерное пространство

$$\{a_1e_1 + \ldots + a_{n+1}e_{n+1} \mid a_1 + \ldots + a_{n+1} = 0\}$$

при помощи подходящего параллельного переноса, скажем, на вектор

$$-\frac{1}{n+1}(e_1 + \ldots + e_{n+1}).$$

Правда, координаты получающихся при этом вершин окажутся *слегка* дробными:

$$\frac{n}{n+1}e_1 - \frac{1}{n+1}e_2 - \ldots - \frac{1}{n+1}e_{n+1}, \ldots, -\frac{1}{n+1}e_1 - \ldots - \frac{1}{n+1}e_n + \frac{n}{n+1}e_{n+1},$$

поэтому большинство математиков предпочитает работать с векторами в пространстве на 1 большей размерности, но зато с целыми координатами.

В описанной выше реализации становится очевидно, что группа симметрий правильного n-мерного симплекса это в точности симметрическая группа S_{n+1} перестановок его вершин (=группа перестановок базиса $e_1, \ldots, e_{n+1}$). Порядок этой группы равен $(n+1)!$, так, что, например, порядок группы симметрий 4-х мерного симплекса равен 120, но, как мы уже отмечали, эта группа не изоморфна I.

• **Гиперкуб.** Вершинами гиперкуба в n-мерном пространстве являются 2^n точек $\pm e_1 \pm \cdots \pm e_n$. Однако с точки зрения автоморфизмов несколько удобнее рассматривать не гиперкуб, а гипероктаэдр.

• **Гипероктаэдр.** Вершинами гипероктаэдра в n-мерном пространстве являются $2n$ точек $\pm e_1, \ldots, \pm e_n$. Таким образом, группу симметрий гипероктаэдра Oct_n можно представлять себе как группу **означенных перестановок** (signed permutations) базиса $e_1, \ldots, e_n$, иными словами, отображений, которые посылают каждый базисный вектор e_i либо в какой-то вектор базиса, либо в вектор противоположный к базисному. Детальное обсуждение всех симметрий гиперкуба/гипероктаэдра в связи с расположением гиперплоскостей приведено в статье [57]. Группа Oct_n называется **октаэдральной группой**, сказанное выше означает, что ее можно мыслить как подгруппу в S_{2n}. С другой стороны, в главе 10 мы обсуждаем октаэдральную группу как сплетение $\mathrm{Oct}_n = S_n \wr C_2$. В частности, порядок группы Oct_n равен $n!2^n$.

В § 7 мы обсудим два исключительных примера больших групп симметрий в четырехмерном пространстве.

§ 10♡. Конечные группы симметрий сферы

Вопрос о приоритете Е. С. Федорова или П. Кюри в деле вывода совокупностей элементов симметрии для конечных фигур вскоре отпал, так как в 1892 году Л. Зонке заново открыл забытую работу Гесселя, уже содержавшую аналогичный вывод.

Иларион Шафрановский. [58]

Ясно, что единственными конечными подгруппами $\mathrm{SO}(2,\mathbb{R})$ являются циклические группы C_n, а в $O(2,\mathbb{R})$, кроме того, появляются диэдральные группы D_n. Соответствующие результаты для групп $\mathrm{SO}(3,\mathbb{R})$ и $O(3,\mathbb{R})$ уже не столь очевидны и были впервые получены в 1830 году Иоганном Гесселем. Сейчас мы покажем, что построенными в предыдущем параграфе группами исчерпываются все конечные группы вращений трехмерного пространства и, кроме того, классифицируем вообще все конечные группы движений. Кристаллографы и физики обычно называют эти группы **точечными группами** (`point groups`). Доказательства основных результатов настоящего параграфа предполагают знакомство с понятиями нормальной подгруппы, сопряженности, изоморфизма и действий групп, а также основами линейной алгебры.

Леонард Эйлер (`Leonhard Euler`, 15 апреля 1707, Базель — 18 сентября 1783, Санкт-Петербург) — величайший и самый плодовитый математик XVIII века, основатель Петербургской математической школы. Ученик Иоганна Бернулли, с 1730 года был профессором физики, а с 1733 года — профессором математики Петербургской Академии наук. В 1741 году переехал в Берлин, но продолжал получать зарплату в Петербургской Академии и публиковаться в ее трудах, а в 1766 году окончательно вернулся в Петербург. Жена Эйлера, дочь художника Гзелля, родила ему тринадцать детей, из которых только три сына пережили самого Эйлера. В 1735 году в результате перенапряжения при вычислениях он потерял правый глаз, а концу жизни полностью ослеп, но именно на это время парадоксальным образом приходится невероятный взлет его творческой активности.

Его работы относятся ко всем областям математики и ее приложений: теории чисел, алгебре, геометрии, комбинаторной топологии, вещественному и комплексному анализу, дифференциальным уравнениям, теории вероятностей, комбинаторике, астрономии, механике твердого тела и небесной механике, гидродинамике, кораблестроению, навигации, артиллерии, картографии, оптике и теории музыки. Он написал более 900 работ, в том числе изрядно книг. Его книги, в особенности, *Введение в анализ бесконечно малых* (1748), *Интегральное исчисление*, *Элементы алгебры* оказали такое же влияние на построение **всех** последующих учебников анализа, что и *Элементы* Эвклида на построение учебников геометрии.

В нашем курсе встречаются круги Эйлера, функция Эйлера, тождество Эйлера, углы Эйлера, формула Эйлера, формулы Эйлера—Фурье, теорема Эйлера—Лагранжа, несколько теорем Эйлера, а в курсе топологии — эйлерова характеристика. Несколько мест на Васильевском острове представляют особенный интерес для математического туриста: Эйлер работал в здании Академии наук напротив Главного здания Университета, а жил в доме академиков на площади Трезини. Он был похоронен на Смоленском кладбище и позже перезахоронен в Александро-Невской лавре.

Классификация сопряженных элементов в $\mathrm{SO}(3,\mathbb{R})$ известна как теорема Эйлера. Следующее рассуждение использует понятие собственного числа и простейшие

свойства собственных чисел, которые мы доказываем в 3-м семестре (все эти свойства можно найти в любом учебнике линейной алгебры, например, в **[111]**). Конечно, это рассуждение при желании было бы легко перевести на геометрический язык.

Теорема Эйлера. *Каждый элемент $g \in \mathrm{SO}(3,\mathbb{R})$ является поворотом вокруг некоторой оси, проходящей через начало координат.*

Доказательство. Достаточно доказать, что среди собственных чисел g всегда по крайней мере одно равно 1. Тогда g является поворотом вокруг оси в направлении собственного вектора u, отвечающего этому собственному числу. В самом деле, пусть $\lambda_1, \lambda_2, \lambda_3$ — собственные числа матрицы g. Так как матрица g ортогональна, все ее собственные числа по модулю равны 1. Так как матрица g вещественная, то по крайней мере одно из них вещественное, скажем, $\lambda_3 = \pm 1$. Либо два других корня тоже вещественные, и тогда, так как $\lambda_1\lambda_2\lambda_3 = \det(g) = 1$, то среди $\lambda_1, \lambda_2, \lambda_3$ четное число -1, так что по крайней мере один из них равен 1. Либо два других корня сопряженные мнимые числа, $\overline{\lambda_1} = \lambda_2$. Тем самым, $\lambda_1\lambda_2 = 1$ и, снова $\lambda_3 = 1$.

Напомним, что **зеркальным поворотом** (`rotary reflection`) называется композиция поворота вокруг некоторой оси с отражением относительно плоскости перпендикулярной этой оси.

Следствие. *Каждый элемент $g \in O(3,\mathbb{R})$ является либо поворотом, либо зеркальным поворотом вокруг некоторой оси проходящей через начало координат,*

Нашей ближайшей целью является доказательство следующего результата.

Теорема. *Конечные подгруппы в $\mathrm{SO}(3,\mathbb{R})$ исчерпываются следующими группами:*

многогранник:	G	$\lvert G\rvert$	m_1	m_2	m_3
n-угольная пирамида	C_n	n	1	1	$-$
n-угольная призма	D_n	$2n$	2	n	n
правильный тетраэдр	T^+	12	4	4	6
куб	O^+	24	6	8	12
правильный икосаэдр	I^+	60	12	20	20

Смысл чисел m_1, m_2, m_3 будет объяснен в процессе доказательства. Приводимое нами доказательство этой теоремы восходит к Клейну [59] и использует идею действия группы на множестве и понятие орбиты, которое мы обсуждаем в главе 6. Это доказательство многократно излагалось в книгах на русском языке, см., например, [60], **[51]**, Приложение А, и **[103]**, с. 391–400. Опишем, прежде всего, в чем состоит основная идея. Пусть G — конечная подгруппа в $\mathrm{SO}(3,\mathbb{R})$, порядка n. По теореме Эйлера каждый элемент $g \in G^\sharp = G \setminus \{e\}$ является нетривиальным поворотом, так что ему соответствует ось, пересекающая единичную сферу в двух точках P и Q, называемых **полюсами** элемента g. Клейн подсчитывает число пар (g, P) двумя способами.

Христиан Феликс Клейн (Felix Klein, 25 апреля 1849, Дюссельдорф — 22 июня 1925, Геттинген) — замечательный немецкий математик и педагог, основные работы которого относятся к теории автоморфных функций, теории групп, геометрии и прикладной математике. В 1865–1870 годах Клейн учился в Бонне у Плюккера. В 1870 году во время стажировки в Париже, которую Клейн провел вместе с Софусом Ли, он увлекся теорией групп. С 1872 года Клейн был профессором в Эрлангене, с 1875 года — в Мюнхене, с 1880 года — в Лейпциге и, наконец, с 1886 года — в Геттингене.

Его инаугурационная лекция при вступлении в профессорскую должность в Эрлангене известна как **Эрлангенская программа**. В ней Клейн определяет геометрию как теорию инвариантов групп. В течение 50 лет Клейн был главным редактором журнала Mathematische Annalen, в то время лучшего математического журнала в мире. Кроме уже цитированных *Лекций об икосаэдре* на русский переведены замечательные классические книги Клейна [61], [62], [63]*. В нашем курсе упоминаются клейновы группы и модель Клейна геометрии Лобачевского.

Доказательство Клейна. . Пусть $n \geq 2$. С одной стороны, так как для каждого из $n-1$ нетривиальных поворотов имеется 2 полюса, поэтому общее количество полюсов равно $2(n-1)$. С другой стороны, пусть полюсы распадаются на s орбит под действием G, причем порядок i-й орбиты равен m_i, а порядок стабилизатора точки из i-й орбиты равен l_i. Число l_i называется **кратностью** полюса P из i-й орбиты. В главе 6 установлено, что $l_i m_i = n$ для всех $i = 1, \ldots, s$. Для i-й орбиты имеется $m_i(l_i - 1)$ пар вида (g, P). Сравнивая два результата, мы получаем основное равенство

$$2(n-1) = m_1(l_1 - 1) + \ldots m_s(l_s - 1).$$

Разделив это равенство на n, мы получаем

$$2 - \frac{2}{n} = \left(1 - \frac{1}{l_1}\right) + \ldots + \left(1 - \frac{1}{l_s}\right),$$

или, что то же самое, $\dfrac{1}{l_1} + \ldots + \dfrac{1}{l_s} = s - 2 + \dfrac{2}{n}$. Так как $l_i \geq 2$ для всех i, то левая часть не превосходит $s/2$, в то время как правая не меньше $s - 2$. Это значит, что $s < 4$. С другой стороны, если $s = 1$, то левая часть положительна, а правая — неположительна. Это значит, что s может принимать только два значения: $s = 2, 3$.

Если $s = 2$, то уравнение принимает вид $\dfrac{1}{l_1} + \dfrac{1}{l_2} = \dfrac{2}{n}$ или, что то же самое, $m_1 + m_2 = \dfrac{n}{l_1} + \ldots + \dfrac{1n}{l_s} = 2$. Два натуральных числа в сумме редко дают 2. Поэтому $l_1 = l_2 = n$ и, тем самым, $m_1 = m_2 = 1$. Это объясняет первую строку таблицы.

---

*Заметим, кстати, что название этой книги представляет собой типичный пример полной утраты смысла при переводе с немецкого. Собственно, по-немецки книга называется Elementarmathematik vom höheren Standpunkte aus, что значит, примерно, Элементарная математика с высшей точки зрения.

Если $s = 3$, то уравнение принимает вид $\frac{1}{l_1} + \frac{1}{l_2} + \frac{1}{l_3} = 1 + \frac{2}{n}$. Расположим порядки централизаторов в порядке возрастания: $l_1 \leq l_2 \leq l_3$. Все три числа l_1, l_2, l_3 не могут быть ≥ 3, так как в этом случае левая часть ≤ 1, в то время как правая часть > 1. Это значит, что $l_1 = 2$.

Тем самым, уравнение принимает вид $\frac{1}{l_2} + \frac{1}{l_3} = \frac{1}{2} + \frac{2}{n}$. Оба числа l_2, l_3 не могут быть ≥ 4, так как в этом случае левая часть $\leq \frac{1}{2}$, в то время как правая часть $> \frac{1}{2}$. Это значит, что $l_2 = 2$ или 3

Рассмотрим вначале случай, когда $l_1 = l_2 = 2$. Тогда уравнение принимает вид $\frac{1}{l_3} = \frac{2}{n}$. Тем самым, $n = 2l_3$ и мы получаем два класса полюсов кратности 2, каждый из которых состоит из n и один класс, состоящий из двух полюсов кратности n. Таким образом, в этом случае мы получаем диэдральную группу D_n.

В случае $l_1 = 2$, $l_2 = 3$, легко убедиться в том, что имеется лишь три возможности: $l_3 = 3$, $n = 12$, либо $l_3 = 4$, $n = 24$, либо $l_3 = 5$, $n = 60$, которые отвечают, соответственно, собственной группе тэтраэдра, собственной группе куба и собственной группе икосаэдра.

Зная конечные подгруппы в $\mathrm{SO}(3, \mathbb{R})$, теперь совсем просто описать конечные подгруппы в $O(3, \mathbb{R})$.

Теорема Гесселя. *Следующими группами исчерпываются все конечные подгруппы в* $O(3, \mathbb{R})$*:*

- 5 *типов конечных подгрупп, содержащихся в* $\mathrm{SO}(3, \mathbb{R})$*, а именно,* C_n*,* D_n*,* T^+*,* O^+*,* I^+*;*
- 5 *типов прямых произведений конечных подгрупп в* $\mathrm{SO}(3, \mathbb{R})$ *и* C_2*:*

$$C_n \times C_2, \quad D_n \times C_2, \quad T^+ \times C_2, \quad O = O^+ \times C_2, \quad I = I^+ \times C_2;$$

- 4 *типа групп, не содержащихся в* $\mathrm{SO}(3, \mathbb{R})$*, но изоморфных конечным подгруппам в* $\mathrm{SO}(3, \mathbb{R})$*, имеющим подгруппу индекса 2*:

$$C_{2n} \geq C_n, \quad D_n \geq C_n, \quad D_{2n} \geq D_n, \quad T \cong S_4 \geq A_4.$$

Чтобы отличать группы, возникающие в третьей строке ответа от изоморфных им групп в первой строке ответа, иногда пользуются обозначениями Коксетера $C_{2n}C_n$, D_nC_n, $D_{2n}D_n$ и S_4A_4.

Наиболее часто воспроизводится следующее доказательство этой теоремы (см., например, **[51]**, Приложение B, или **[103]**, с.400–401, а также десятки учебников на английском языке **[246]**, **[284]**, etc.). Это доказательство основано на двух простейших теоретико-групповых идеях. Пусть $G \leq O(3, \mathbb{R})$ — подгруппа, не содержащаяся в $\mathrm{SO}(3, \mathbb{R})$. Тогда $H = G \cap \mathrm{SO}(3, \mathbb{R})$ имеет индекс 2 в G и, значит, $G = H \sqcup gH$, где g — любой элемент G, не являющийся вращением.

Доказательство Пойа—Майер. Обозначим через f центральную симметрию. Тогда либо $f \in G$, либо $f \notin G$. В первом случае в качестве g можно взять f, так

что $G = H \times \langle f \rangle$, что и объясняет первую строчку ответа. Если же $f \notin G$, то сопоставление $h \mapsto h$ и $gh \mapsto fgh$, определяет изоморфизм группы $G = H \sqcup gH$ на группу $G = H \sqcup fgH$ (убедитесь в этом!). Таким образом, нам остается лишь найти полный список подгрупп в $\mathrm{SO}(3,\mathbb{R})$, в которых есть подгруппа индекса 2. Все такие случаи как раз и перечислены во второй строке ответа.

Сделаем в связи с этой теоремой три важных наблюдения.

Замечание 1. Группа $T^+ \times C_2$ не совпадает с группой симметрий тетраэдра! Это группа симметрий кристалла пирита FeS_2 (сульфид железа, известный также как серный колчедан). Геометры называют идеальную форму этих кристаллов **пентагон-додекаэдрической**, минералоги иногда говорят о **пиритоэдре** (`piritohedron`), см. рис. 134 в книге Смита [68]. Интересно, что на рис. 29 этой книги в связи с описанием кристаллографических классов тот же самый многогранник фигурирует под названием **пентагон-додекаэдра**!

Замечание 2. Группы классифицированы здесь не с точностью до изоморфизма, а с точностью до сопряженности в $O(3,\mathbb{R})$. Скажем, группы T и O^+ изоморфны как абстрактные группы, но не сопряжены в $O(3,\mathbb{R})$, потому что первая из них содержит зеркальные вращения, в то время как вторая состоит целиком из собственных вращений. В действительности, в большинстве приложений интерес представляет вовсе не изоморфизм двух групп, как абстрактных групп, а их сопряженность в какой-то большей группе (т. е. например, их изоморфизм как групп перестановок, изоморфизм как линейных групп и т. д.).

Замечание 3. В действительности, эта теорема классифицирует даже все конечные подгруппы в $\mathrm{GL}(3,\mathbb{R})$. В самом деле, одна из первых идей, с которой знакомится студент при изучении теории представлений конечных групп, состоит в том, что любая *конечная* подгруппа $G \leq \mathrm{GL}(3,\mathbb{R})$ сопряжена с подгруппой в $O(3,\mathbb{R})$. В этом проще всего убедиться посредством **усреднения** по группе G. В самом деле, если $B(u,v)$ — положительно определенное скалярное произведение на пространстве $V = \mathbb{R}^n$, то мы можем определить на этом пространстве новое скалярное произведение $A(u,v) = \dfrac{1}{|G|}\sum\limits_{g\in G} B(gu,gv)$, которое уже инвариантно относительно G в том смысле, что $A(gu,gv) = A(u,v)$. Но это как раз и значит, что $G \leq O(n,\mathbb{R},A)$. Осталось заметить, что так как A положительно определена, группа $O(n,\mathbb{R},A)$ сопряжена с $O(n,\mathbb{R})$.

Однако, конечные подгруппы в $O(3,\mathbb{R})$ совсем несложно описать и в духе Клейна [69]. При этом мы тоже получим полный список конечных подгрупп в $O(3,\mathbb{R})$, но нужно некоторое дополнительное усилие, чтобы привести этот список к той форме, в которой он содержится в теореме (см., например, с. 334 в цитированной статье Сенешаль, где обсуждается различие `rotary reflection` $\widetilde{n}$ и `rotary inversion` $\overline{n}$ и связанные с этим нюансы, зависящие от вычета n по модулю 4, и явное отождествление двух списков на с. 335).

Доказательство Сенешаль. Так как $H \trianglelefteq G$, то движение g должно переставлять полюса H. Для каждой орбиты полюсов имеет место следующая альтернатива: либо эта орбита остается на месте, либо под действием g происходит **слияние** (`fusion`) этой орбиты с какой-то орбитой того же порядка. Разумеется, для того, чтобы могла реализовываться вторая возможность, у группы H действительно должно быть две орбиты одинакового порядка! Так как $|G| = 2|H|$, то стабилизатор любой неподвижной орбиты удваивается.

Дьердь Пойа (Gyorgy Polya, 13 декабря 1887, Будапешт — 07 сентября 1985, Пало Альто, Калифорния) — замечательный венгерский математик, основные работы которого относятся к теории групп, комбинаторике, теории чисел, теории вероятностей, математической физике и теории функций. Самое прославленное достижение Пойа в теории групп — это его **теория перечисления**, которая излагается в главе 6 настоящей книги. Пойа происходил из еврейской семьи, но его отец, Яков Поллак, вынужден был сменить фамилию на венгерскую и принять католицизм, чтобы получить позицию в Университете Будапешта!! Это считалось обычной практикой в то время, [почти] все венгерские математики происходили из еврейских семей и большинство из них вынуждены были сменить фамилии и/или религию, чтобы *продемонстрировать солидарность с венгерской культурой*. Скажем, Липот Фейер был рожден как Леопольд Вайс, настоящая фамилия Эрдеша Энгландер, etc., etc., etc., etc., etc. В межвоенный период это интересное явление не ограничивалось Венгрией, но захватило также и братскую Польшу (Polak, Węgier dwa bratanki, jak do szabli, tak do szklanki). Как мы знаем из книги I, Альфред Тарский, урожденный Тейтельбаум, вынужден был сменить фамилию — и религию — чтобы *продемонстрировать солидарность с польской культурой* и получить преподавательскую позицию.

В 1905 году Пойа поступил на юридический факультет университета Будапешта, но не выдержал там больше одного семестра. После этого он поучился на филологическом факультете и даже получил там промежуточный диплом, но потом решил заняться математикой. Как он вспоминал в одном из интервью: I thought I was not good enough for physics and far too good for phylosophy. Mathematics was somewhere in between. Под влиянием Фейера он довольно быстро добился первых успехов и провел 1910–1914 годы в Вене, Геттингене и Париже, где познакомился с такими блестящими математиками как Гильберт, Клейн, Герман Вейль, Курант, Ландау, Теплиц, Каратеодори, Пикар и Адамар. Однако наибольшее влияние на его дальнейшую карьеру оказал Гурвиц, который пригласил его на работу в Цюрихскую Eidgenossische Technische Hochschule. Это был наиболее продуктивный период его жизни: именно в это время он пишет свою замечательную книгу с Сеге [64] сотрудничает с Харди и Литтлвудом [65] и публикует по дюжине статей в год. Именно тогда он написал свои основные работы по теории групп, посвященные математической кристаллографии и теории перечисления. В 1940 в связи с непрерывно ухудшающейся ситуацией в Европе Пойа решает эмигрировать в США, где преподает вначале в Brown University, а потом, до ухода на пенсию, в Стэнфорде. На русский язык переведены несколько совершенно изумительных педагогических книг Пойа, в частности [66], [67]. Пойа объяснял свой интерес к педагогике тем, что, поскольку сам он пришел в математику сравнительно поздно, он хорошо помнил свои собственные трудности при усвоении новых математических концепций. Из того же интервью: the proof seems to be conclusive, but how can people find such results? My difficulty in understanding mathematics: how was it discovered.

Пусть вначале $s = 2$. Тогда g либо фиксирует, либо переставляет полюса. Если

g фиксирует полюса, то группа G диэдральна. Если g переставляет полюса, то g является либо отражением и тогда $G = H \times \langle g \rangle$, либо зеркальным поворотом и тогда G является циклической группой в 2 раза большего порядка, чем H.

С другой стороны, если $s = 3$, то всегда есть орбита неподвижная под действием g, т.к. это единственная орбита такого порядка. Для $H = O^+$ и $H = I^+$ это условие уже однозначно определяет группу G, так как все три орбиты полюсов имеют разные размеры. Тем самым, g фиксирует каждую из них. Для групп же $H = D_n$ и $H = T^+$ имеются два выбора g, в зависимости от того, сохраняет ли g две оставшиеся орбиты или переставляет их между собой. В первом случае мы получаем группы симметрий призмы и правильного тетраэдра, а во втором случае — группы симметрий антипризмы и пиритоэдра.

§ 11♡. De divina proportione: икосианы, $\{3,3,5\}$ и $\{5,3,3\}$, $W(H_4)$

> Вы, особенно в подростковом возрасте, должны пользоваться всеми достижениями геометрии, когда проводите линии, призванные служить ориентирами при разработке композиции картины. Я знаю, что художники более романтического склада полагают, будто эти строительные леса математики губительно сказываются на вдохновении, заставляя художника предаваться излишним размышлениям. Можете смело и без колебаний возразить им, что вам не придется утруждать свою голову, так как золотое сечение, которое Лука Пачоли называет **божественной пропорцией**, позволит вам воспользоваться теми естественными возможностями, которые этот метод открывает перед вами. В знаменитой книге Пачоли, являющейся наиглавнейшим из всех известных трактатов по эстетике, философское учение Платона очищается от примитивного идеализма. Вам необходимо познакомиться с этим произведением, которое всегда должно быть при вас, став вашей настольной книгой.
>
> Сальвадор Дали. [70]

Большинство профессиональных алгебраистов охарактеризуют группы T и O не как группы симметрий правильных многогранников, а как **группы Вейля** $W(A_3)$, $W(B_3)$ кристаллографических систем корней типов A_3 и B_3. Точно так же группа I представляет собой группу Вейля $W(H_3)$ некристаллографической системы корней H_3. В этом параграфе мы построим еще две совершенно замечательные группы, которые реализуются как группы симметрий в четырехмерном пространстве, а именно, группу Вейля $W(F_4)$ кристаллографической системы F_4, порядка $1152 = 2^7 \cdot 3^2$ и группу Вейля $W(H_4)$ некристаллографической системы корней типа H_4, порядка $14400 = 2^6 \cdot 3^2 \cdot 5^2$. Однако мы построим эти группы не алгебраически, а геометрически, как группы симметрий исключительных многогранников.

По-английски обычно проводится различие между **полиэдрами** (`polyhedra`) — многогранниками в размерности 3 и **политопами** (`polytopes`) — многогранниками в произвольной размерности. Мы передаем оба эти слова термином **многогранник**. С другой стороны, поскольку нас все же больше всего интересуют

Герман Вейль (`Hermann Weyl`, 9 ноября 1885, Эльмсхорн — 9 декабря 1955, Цюрих) — гениальный немецкий математик, один из классиков над классиками, определивших развитие математики в XX веке. В 1904 году поступил в Геттингенский Университет, где стал непосредственным учеником Гильберта. С 1913 года он преподавал в Цюрихе, где какое-то время сотрудничал с Эйнштейном. В 1930 году переехал в Геттинген, но после прихода к власти нацистов эмигрировал в США, где работал в Institute for Advanced Studies в Принстоне. В 1951 году вернулся в Цюрих. Вейль написал почти 200 статей и 16 книг, в том числе *Die idee der Riemannschen Fläche*; *Raum, Zeit, Materie*; *Das Kontinuum*; *Meromorphic functions and analytic curves*, и др. Будучи одним из последних математиков универсалов, он внес *основополагающий* вклад в столь разные разделы математики, как теория групп Ли и их представлений, геометрия, теория римановых поверхностей, теория аналитических функций, равномерное распределение, теория дифференциальных уравнений и т. д. Кроме того, ему принадлежат фундаментальные работы, посвященные приложениям математики в квантовой теории и теории относительности, общим и философским вопросам математики и систематические изложения нескольких крупных разделов математики, в том числе таких, которыми он сам непосредственно не занимался, скажем, алгебраической теории чисел. Именно Г. Вейлю и Дж. фон Нейману принадлежит первая математически корректная формализация квантовой механики в терминах операторов в гильбертовых пространствах. Кроме групп Вейля в нашем курсе встречаются алгебры Вейля, теорема Картана—Вейля, а в теории чисел рассматриваются суммы Вейля. Последнее его появление в широкой математической аудитории произошло на международном математическом конгрессе в Амстердаме в 1954 году, где он представил работы филдсовских лауреатов Кодаиры и Серра. На русский язык переведены его книги *Классические группы, их инварианты и представления*, *Алгебраическая теория чисел*, *Симметрия*, *Теория групп и квантовая механика*, и большое количество статей, в том числе в томе [71]. Биографию Вейля можно найти в статье [72].

многогранники в размерности 4, мы сохраняем специальные имена для их граней разных размерностей: а именно, 0-мерные грани называются **вершинами** (`vertices`), 1-мерные грани — **ребрами** (`edges`), 2-мерные грани — **гранями** (`faces`) и 3-мерные грани — **ячейками** (`cells`).

А именно, $W(F_4)$ будет группой симметрий исключительного правильного многогранника $\{3,4,3\}$ с 24 вершинами, 96 ребрами, 96 гранями и 24 трехмерными ячейками, каждая из которых является правильным октаэдром, С другой стороны, $W(H_4)$ будет построена как группа симметрий исключительного правильного многогранника $\{3,3,5\}$ со 120 вершинами, 720 ребрами, 1200 гранями и 600 ячейками, каждая из которых является правильным тетраэдром, — или двойственного к нему многогранника $\{5,3,3\}$ с 600 вершинами, 1200 ребрами, 720 гранями и 120 ячейками, каждая из которых является правильным додекаэдром.

Так как эти многогранники строятся в терминах **золотого сечения**, и мы не собираемся воспроизводить все вычисления, необходимые для того, чтобы убедиться в том, что мы действительно построили правильные многогранники и дать представление о том, какого рода рассуждения при этом используются, мы сейчас

для разминки построим правильные додекаэдр и икосаэдр. Все детали приводятся в замечательной книге Дональда Коксетера [73].

Гарольд Коксетер (`Harold Scott McDonald Coxeter`, 9 февраля 1907, Лондон — 31 марта 2003, Торонто) — замечательный английский математик, основные работы которого относятся к геометрии, теории групп и комбинаторике. Коксетер получил Ph. D. в Кэмбридже под руководством Бейкера, после чего провел два года в Принстоне у Веблена а в 1936 году принял постоянную позицию в Университете Торонто, Канада, где оставался следующие 67 лет, вначале как действующий профессор, а потом как Professor Emeritus. Самые знаменитые достижения Кокстера связаны с теорией групп, порожденных отражениями, и их обобщениями, теорией многогранников и неэвклидовой геометрией. Его идеи оказали глубочайшее влияние на геометрическую трактовку конечных, дискретных и алгебраических групп в XX веке. Много терминов в теории групп связано с его именем: группа Коксетера, система Коксетера, элемент Коксетера, коксетеровские образующие, число Коксетера, и т. д. Кроме 167 статей Коксетер опубликовал 12 абсолютно блистательных книг, как исследовательских и научно-популярных, так и таких, которые *одновременно* являются исследовательскими и научно-популярными, в частности, *Вещественная проективная плоскость* (1955), *Образующие и соотношения дискретных групп* (1957, совместно с Мозером), *Введение в геометрию* (1961), *Правильные многогранники* (1963), *Неэвклидова геометрия* (1965), *Правильные комплексные многогранники* (1974), и т. д. Некоторые из них — но, к сожалению, далеко не все!! — переведены на русский язык. Робертсон вспоминает, что в 89 лет Коксетер мог 50 раз отжаться и говорил о себе: I am never bored. Я думаю, для компетентного читателя не будет секретом, что и эта книга, в меру сил, является *подражанием Коксетеру* (*imitation of Christ*).

Обозначим через σ и τ корни уравнения $x - \dfrac{1}{x} = 1$. Если на Вашем компьютере установлена программа `Mathematica`, то при помощи команды `Roots` Вы можете даже вычислить эти корни: $\sigma = \dfrac{1-\sqrt{5}}{2}$ и $\tau = \dfrac{1+\sqrt{5}}{2}$. Легко видеть, что τ — это в точности диагональ правильного пятиугольника со стороной 1:

$$\tau = \frac{1+\sqrt{5}}{2} = 2\cos\ \frac{\pi}{5}\ = 1.6180339887498948482045868343656381177 20...,$$

численное значение найдено при помощи `N[GoldenRatio,40]`.

В научно популярной литературе число τ часто обозначается через ϕ и называется **отношением крайнего и среднего** (`extreme and mean ratio`), **божественной пропорцией** (`divina proportione`), **золотым сечением**[♮,♭] (`golden ratio`,

[♮]В советской математической энциклопедии введение термина золотое сечение приписывается Леонардо да Винчи. Впрочем, Дэн Пидо [74] высказывает точку зрения, что термин `der goldene Schnitt` весьма позднего происхождения и появился в Германии в начале XIX века.

[♭]Уместна некоторая осторожность, так как в полиграфии, живописи и архи-

golden section) или **числом Фидия** [76], последнее название и объясняет выбор греческой буквы ϕ. В этом случае σ обозначается через $\widehat{\phi}$. Мы, однако, пользуемся обозначениями σ и τ принятыми в геометрии и теории групп. Литература, посвященная золотому сечению с различных точек зрения, необозрима. Золотое сечение часто использовалось греческими скульпторами и архитекторами и явно описывается в *Элементах* Эвклида, который рассматривает пропорцию $\dfrac{y}{z} = \dfrac{y+z}{y}$. Ясно, что в терминах $x = \dfrac{y}{z}$ эта пропорция переписывается в виде $x = 1 + \dfrac{1}{x}$, а как мы знаем $x = \tau$ как раз и является положительным корнем этого уравнения. Посмотрев для мнемоники на фаланги указательного пальца, это уравнение можно переписать в виде $x^2 = 1 + x$. Самое знаменитое классическое произведение — это опубликованная в 1507 году книга Луки Пачоли *De divina proportione*, в иллюстрациях к которой использованы модели и 59 таблиц, изготовленные его близким другом Леонардо да Винчи. Третья часть книги Пачоли представляет собой итальянский перевод книги Пьеро делла Франческа *De quinque corporibus regularibus*, которую тот сочинил когда ослеп и не мог больше заниматься живописью. Связь золотого сечения с числами Фибоначчи, непрерывными дробями и филлотаксисом обсуждается, *например*, в главе 11 книги Коксетера **[103]** и его статье [77] и книге Пидо [74]. Из текстов, написанных нематематиками, большое впечатление производит манифест Ле Корбюзье [78].

Лука Пачоли (Luca Pacioli, 1445, Борго Сан Сеполькро — 1515) — крупнейший итальянский математик XV века. В молодости он работал домашним учителем в Риме и Венеции, а в 1475 году вступил в орден францисканцев. Монахи обращаются друг к другу fra, от итальянского fratello — брат[элло], поэтому Луку Пачоли часто называют **Фра** Лука Пачоли. Это не мешало ему преподавать в университетах Болоньи, Милана, Флоренции, Рима и Неаполя. Кроме *De divina proportione* в 1494 году он опубликовал другую очень влиятельную книгу *Summa de arithmetica, geometria, proportioni et proportionalita*, фактически свод математических знаний европейского Средневековья и Возрождения. Лука Пачоли называет алгебру **arte maggiore** — Великое искусство, что объясняет название книги Кардано *Ars Magna*. В то время математика в Италии и Германии была теснейшим образом связана с живописью, поэтому Лука Пачоли работал в близком контакте с ведущими живописцами и скульпторами того времени. Сохранилось несколько замечательных портретов Луки Пачоли, самый знаменитый из которых выполнен лучшим итальянским художником XV века Пьеро делла Франческа.

тектуре выражение золотое сечение, la section d'or, в зависимости от контекста может обозначать *почти любое* положительное вещественное число! Например, французские кубисты искренне верили, что $\tau = \sqrt{2}$, той же точки зрения (но не из эстетических, а из чисто прагматических соображений) придерживается немецкий индустриальный стандарт DIN, в чем можно убедиться, разглядывая лист бумаги формата A4, ширина которого равна 210 миллиметрам, а высота $210\sqrt{2}$ миллиметров. С другой стороны, в типографском деле принято считать что $\tau = 8/5$, см., например, [75].

Начнем со следующего общеизвестного наблюдения (по этому поводу см., например, [**103**], с. 238–240, или [**28**], т. 1, с. 487–489). Если разделить ребра октаэдра с вершинами

$$(\pm\tau^2, 0, 0), \quad (0, \pm\tau^2, 0), \quad (0, 0, \pm\tau^2)$$

в отношении $\tau : 1$, то получившиеся 12 вершин являются вершинами правильного икосаэдра.

Теорема. *Следующие* 12 *точек*

$$(\pm 1, 0, \pm\tau), \quad (\pm\tau, \pm 1, 0), \quad (0, \pm\tau, \pm 1)$$

образуют вершины правильного икосаэдра.

Доказательство. Легко видеть, что пять вершин $(1, 0, \tau)$, $(\tau, -1, 0)$, $(1, 0, -\tau)$, $(0, \tau, -1)$, $(0, \tau, 1)$ лежат в одной плоскости — а именно, в плоскости задаваемой уравнением $\tau x + y - \tau = 0$. Расстояние между любыми двумя соседними из этих пяти вершин, а также между $(\tau, 1, 0)$ и любой из них равно 2. Так как расстояние между двумя точками при центральной инверсии не меняется, то поворот на $2\pi/5$ вокруг оси, проходящей через $(\tau, 1, 0)$ и $(-\tau, -1, 0)$ переводит конфигурацию из 12 точек в себя. Поскольку группа симметрий этих 12 вершин, кроме того, содержит вращение вокруг оси, соединяющей центры треугольников $(1, \tau, 0)$, $(0, 1, \tau)$, $(\tau, 0, 1)$ и $(-1, -\tau, 0)$, $(0, -1, -\tau)$, $(-\tau, 0, -1)$ и 3 отражения относительно координатных плоскостей, то группа симметрий этого многогранника транзитивна на **флагах**: т. е. наборах, состоящих из вершины, содержащего эту вершину ребра и содержащей это ребро грани. Но это и значит, что многогранник правильный.

Столь же легко убедиться в справедливости следующего результата. Это можно сделать точно так же, как в доказательстве предыдущей теоремы.

Теорема. *Следующие* 20 *точек*

$$(\pm 1, \pm 1, \pm 1), \quad (\pm\sigma, \pm\tau, 0), \quad (0, \pm\sigma, \pm\tau), \quad (\pm\tau, 0, \pm\sigma)$$

образуют вершины правильного додекаэдра.

Забавно и поучительно, что 8 из вершин додекаэдра, а именно, $(\pm 1, \pm 1, \pm 1)$, являются вершинами куба — будет ли это столь же очевидным геометрически без явного задания координат вершин?

Теперь мы проведем аналогичные (но, конечно, более сложные!) конструкции в четырехмерном пространстве. Полная классификация правильных многогранников в n-мерном пространстве была получена Шлефли в 1850 году.

Как мы уже знаем, во всех размерностях $n \geq 3$ существует по крайней мере 3 правильных многогранника: симплекс с вершинами $e_1, \ldots, e_{n+1}$, гиперкуб с вершинами $\pm e_1 \pm \ldots \pm e_n$ и гипероктаэдр с вершинами $\pm e_i$. Кроме того, в размерности 3 существует еще ровно два **исключительных** правильных многогранника: додекаэдр и икосаэдр. Оказывается, в размерности 4 исключительных многогранников ровно 3. Описывать правильный многогранник проще всего его **символом Шлефли** $\{p, q, r, \ldots\}$. Символ Шлефли определяется по индукции следующим образом. Определим p как число сторон 2-мерной грани. Зафиксируем теперь какую-то вершину P многогранника Γ и рассмотрим все вершины Γ, соединенные с ней ребром.

Людвиг Шлефли (Ludwig Schläfli, 15 января 1814, Берн — 20 марта 1895, Берн) — замечательный швейцарский геометр. Основные достижения Шлефли относятся к геометрии и алгебраической геометрии, но он работал также в области арифметики, специальных функций и небесной механики. Шлефли вначале собирался стать теологом и 10 лет работал школьным учителем в Туне, изучая математику в свободное время. Еще одним увлечением Шлефли было изучение языков, причем не только европейских, а и, скажем, санскрита. В 1843 году Штейнер, Якоби и Дирихле взяли Шлефли в качестве переводчика во время своей поездки в Рим и общение с великими математиками окончательно склонило его к занятиям математикой. Самое знаменитое открытие Шлефли — это обнаружение им 27 прямых на кубической гиперповерхности, один из наиболее ярких и глубоких геометрических результатов XIX века. В 1853 году Шлефли стал профессором в Берне.

Все эти вершины лежат в одной гиперплоскости H (ортогональной к оси, соединяющей центр многогранника с вершиной P) и сечение $\Gamma\cap H$ многогранника Γ гиперплоскостью H представляет собой правильный многогранник на единицу меньшей размерности. Так как все вершины Γ *социологически одинаковы* (sociologically equal), то тип этого многогранника не зависит от выбора вершины P. Определим теперь q как число сторон 2-мерной грани многогранника $\Gamma\cap H$. Продолжая действовать таким образом до тех пор, пока получающееся сечение имеет двумерную грань, мы получим символ Шлефли Γ. Таким образом, символ Шлефли n-мерного многогранника состоит из $n-1$ целого числа ≥ 3.

Теорема Шлефли. *С точностью до подобия все возможные правильные многогранники исчерпываются следующим списком:*

- *При $n=2$ правильный m-угольник $\{m\}$ для любого целого $m\geq 3$.*
- *При $n=3$ один из пяти многогранников: тетраэдр $\{3,3\}$, октаэдр $\{3,4\}$, куб $\{4,3\}$, икосаэдр $\{3,5\}$, додекаэдр $\{5,3\}$.*
- *При $n=4$ один из шести многогранников:*

$$\{3,3,3\},\quad \{3,3,4\},\quad \{4,3,3\},\quad \{3,4,3\},\quad \{3,3,5\},\quad \{5,3,3\}.$$

- *При $n\geq 5$ один из трех следующих многогранников:*
  - *симплекс $\{3,\dots,3\}$,*
  - *гипероктаэдр $\{3,\dots,3,4\}$,*
  - *гиперкуб $\{4,3,\dots,3\}$.*

Обратно, для каждого из этих символов существует правильный многогранник с таким символом.

В дальнейшем многогранники $\{3,4,3\}$, $\{3,3,5\}$ и $\{5,3,3\}$ будут называться, соответственно, (правильными) 24-клеточником, 600-клеточником и 120-клеточником. Начнем с построения самого простого из исключительных четырехмерных многогранников, $\{3,4,3\}$. В качестве его вершин можно взять 24 вершины вида $\pm e_i\pm e_j$, $1\leq i\neq j\leq 4$. Группа симметрий этого многогранника обозначается $W(F_4)$ и называется **группой Вейля типа $\mathbf{F_4}$**. Как уже было упомянуто, порядок этой группы равен 1152 и она содержит октаэдральную подгруппу $W(B_4)=\mathrm{Oct}_4$ порядка 384. Однако нам будет удобнее изменить масштаб и

взять следующие 24 точки $(\pm\tau, \pm\tau, 0, 0)$, $(\pm\tau, 0, \pm\tau, 0)$, $(\pm\tau, 0, 0, \pm\tau)$, $(0, \pm\tau, \pm\tau, 0)$, $(0, \pm\tau, 0, \pm\tau)$, $(0, 0, \pm\tau, \pm\tau)$. Разделим теперь 96 ребер этого многогранника в отношении $\tau : 1$ и добавим к ним 16 вершин гиперкуба и 8 вершин гипероктаэдра. Получившиеся 120 точек будут вершинами правильного многогранника типа $\{3, 3, 5\}$.

Теорема. *Следующие* 120 *точек:*

- 16 *точек* $(\pm 1, \pm 1, \pm 1, \pm 1)$,
- 8 *точек, получающихся из* $(\pm 2, 0, 0, 0)$ *перестановками координат,*
- 96 *точек, получающихся из* $(\pm 1, \pm\sigma, \pm\tau, 0)$ **четными** *перестановками координат,*

образуют вершины правильного многогранника $\{3, 3, 5\}$.

Группа $W(H_4)$ симметрий этого многогранника называется **группой Вейля типа $\mathbf{H_4}$**. Порядок этой группы равен 14400. Ее можно истолковать и как группу симметрий правильного 120-клеточника.

Теорема. *Следующие* 600 *точек:*

- 24 *точки получающихся из* $(\pm 2, \pm 2, 0, 0)$, *перестановками координат,*
- 64 *точки, получающихся из* $(\pm 1, \pm 1, \pm 1, \pm\sqrt{5})$ *перестановками координат,*
- 64 *точки, получающихся из* $(\pm\sigma, \pm\sigma, \pm\sigma, \pm\tau^2)$ *перестановками координат,*
- 64 *точки, получающихся из* $(\pm\tau, \pm\tau, \pm\tau, \pm\sigma^2)$ *перестановками координат,*
- 96 *точек, получающихся из* $(\pm 1, \pm\tau^2, \pm\sigma^2, 0)$ **четными** *перестановками координат,*
- 96 *точки, получающихся из* $(\pm\sqrt{5}, \pm\sigma, \pm\tau, 0)$ **четными** *перестановками координат,*
- 192 *точки, получающихся из* $(\pm 1, \pm\tau, \pm\sigma, \pm 2)$ **четными** *перестановками координат,*

образуют вершины правильного многогранника $\{5, 3, 3\}$.

С правильным 600-клеточником связана еще одна совершенно замечательная группа, называемая **группой икосианов** или **бинарной группой икосаэдра**. А именно, 120 его вершин после нормировки сами образуют группу относительно обычного умножения кватернионов. А именно, разделив все координаты вершин на 2, мы получим 120 кватернионов нормы 1. Легко проверить (мы делаем это в главе 3), что эти кватернионы образуют мультипликативную группу, которая обычно обозначается через $2.A_5$. Хотя порядок этой группы равен 120, она не изоморфна ни S_5, ни $I = A_5 \times C_2$. В самом деле, как в группе S_5, так и в группе I есть подгруппа A_5, в то время как у группы икосианов $2.A_5$ есть *фактор-группа* типа A_5, но нет подгруппы такого типа! С точки зрения теории групп $2.A_5$ является **нерасщепляющимся расширением** A_5 при помощи C_2. Ее называют также бинарной группой икосаэдра.

§ 12♡. Группы автоморфизмов

> Many of the examples given are not stated precisely. The flavor and potential of applications seem more important in the present context than do comprehensive lists.
>
> William M. Kantor. [79]

Роль теории групп в математике определяется тем, что все биективные преобразования любого множества, сохраняющие заданную на этом множестве структуру, образуют группу. Сейчас мы перечислим некоторые из наиболее часто встречающихся типов структур вместе с традиционными названиями сохраняющих их преобразований. Некоторые из таких групп автоморфизмов подробно обсуждаются в настоящем курсе, изучением остальных занимаются алгебраическая геометрия, геометрия, топология, анализ, теория меры, комбинаторика и т. д.

• **Группа автоморфизмов группы.** Биекция φ группы G на себя называется **автоморфизмом**, если $\varphi(gh) = \varphi(g)\varphi(h)$ для любых $g, h \in G$. Легко проверить, что множество $\mathrm{Aut}(G)$ всех автоморфизмов группы G на себя является группой относительно композиции. В главе 4 мы приведем некоторые результаты, проясняющие структуру этой группы.

• **Группа автоморфизмов кольца.** Биекция φ кольца R на себя называется **автоморфизмом**, если $\varphi(x+y) = \varphi(x) + \varphi(y)$ и $\varphi(xy) = \varphi(x)\varphi(y)$ для любых $x, y \in R$. Снова множество $\mathrm{Aut}(R)$ всех автоморфизмов кольца R на себя является группой относительно композиции.

• **Группа Галуа**. Пусть L/K — расширение полей (эта традиционная запись не имеет ничего общего с факторизацией, а просто указывает, что K рассматривается как подполе в L). Подгруппа $\mathrm{Aut}_K(L)$ в группе $\mathrm{Aut}(L)$, состоящая из всех автоморфизмов, ограничение которых на K тождественно, называется **группой Галуа** расширения L/K и обозначается $\mathrm{Gal}(L/K)$. При этом действие элементов группы Галуа обычно записывается экспоненциально, т. е. вместо $g(x)$ пишут x^g. Таким образом,

$$\mathrm{Gal}(L/K) = \{g \in \mathrm{Aut}(L) \mid \forall x \in K, x^g = x\}.$$

В действительности, термин `группа Галуа` обычно резервируется для случая, когда расширение L/K *алгебраическое* или даже только для случая, когда L/K является **расширением Галуа**, иными словами, когда K совпадает с полем инвариантов группы $\mathrm{Gal}(L/K)$:

$$K = \{x \in L \mid \forall g \in G,\ x^g = x\}.$$

В противоположном же случае *чисто трансцендентного* расширения группа автоморфизмов называется группой Кремона.

• **Группа Кремона**. Пусть $K(x_1, \dots, x_n)$ — поле рациональных дробей от n переменных над полем K. Группа автоморфизмов

$$\mathrm{Cr}(n, K) = \mathrm{Aut}_K K(x_1, \dots, x_n)$$

называется **группой Кремона**. Эта группа возникает в алгебраической геометрии как группа бирациональных автоморфизмов n-мерного аффинного (или проективного) пространства.

Луиджи Кремона (Luigi Cremona, 7 декабря 1830, Павия — 10 июня 1903, Рим) — основоположник итальянской геометрической школы. После окончания университета в Павии он несколько лет преподает в школах в Павии, Кремоне и Милане, а в 1860 году становится профессором Болонского университета. В 1867 году он возвращается в Милан, где становится профессором Миланского Политехнического Института. Основные исследования Кремона относятся к проективной геометрии и теории бирациональных преобразований.

• **Группа линейных автоморфизмов.** Пусть V – векторное пространство над полем K. Отображение $\varphi : V \longrightarrow V$ называется **линейным**, если $\varphi(u + v) = \varphi(u) + \varphi(v)$ и $\varphi(\lambda u) = \lambda\varphi(u)$ для любых $u, x \in V$ и $\lambda \in K$. Линейные отображения V в себя называются еще **линейными операторами**, а биективные линейные отображения — **обратимыми** линейными операторами. Множество $\mathrm{GL}(V) = \mathrm{Aut}(V)$ всех обратимых линейных операторов на V называется **полной линейной группой** пространства V.

• **Группа аффинных автоморфизмов.** Пусть снова V – векторное пространство над полем K. Отображение $\varphi : V \longrightarrow V$ называется **аффинным**, если преобразование $v \mapsto \varphi(v) - \varphi(0)$ линейно. Таким образом, аффинное отображение является композицией линейного отображения и трансляции на вектор $u = \varphi(0)$. Ясно, что для обратимости аффинного преобразования необходимо и достаточно, чтобы его линейная часть была обратима. Множество $\mathrm{Aff}(V)$ всех обратимых аффинных преобразований на V называется **аффинной группой** пространства V.

• **Группа коллинеаций.** Пусть, как и выше, V — векторное пространство над полем K. Отображение φ называется **полулинейным**, если оно аддитивно, т. е. $\varphi(u + v) = \varphi(u) + \varphi(v)$ и, кроме того, существует такой автоморфизм $\theta \in \mathrm{Aut}(K)$, что $\varphi(\lambda u) = \theta(\lambda)\varphi(u)$ для

любых $u \in V$ и $\lambda \in K$. Биективное полулинейное отображение V на себя называется **коллинеацией**. Множество $\mathrm{\Gamma L}(V)$ всех коллинеаций пространства V образует группу, называемую **группой коллинеаций пространства** V.

• **Группа изометрий.** Пусть X метрическое пространство с расстоянием $d : X \times X \longrightarrow \mathbb{R}$. Биекция φ множества X на себя называется **изометрией**, если $d(\varphi(x), \varphi(y)) = d(x, y)$ для любых двух точек $x, y \in X$. Как всегда, легко проверить, что множество $\mathrm{Isom}(X)$ всех изометрий X на себя образует группу относительно композиции. Эта группа называется **группой изометрий** (или, иногда, **группой автометрий**) множества X.

• **Группа автоморфизмов графа.** Пусть $\Gamma = (V, E)$ — граф с множеством **вершин** V и множеством **ребер** $E \subseteq \bigwedge^2(X)$. Напомним (см. аппендикс 1), что $\bigwedge^2(X)$ обозначает множество всех двухэлементных подмножеств X, таким образом, рассматриваются неориентированные графы без петель и кратных ребер. Биекция φ множества X на себя называется **автоморфизмом** графа Γ, если $(\varphi(x), \varphi(y)) \in E$ в том и только том случае, когда $(x, y) \in E$. Все автоморфизмы графа Γ образуют группу $\mathrm{Aut}(\Gamma)$, называемую **группой графа** или **группой автоморфизмов графа**. Мы оставляем читателю обобщить это понятие на графы с петлями и кратными ребрами, ориентированные графы, и т. д.

• **Билипшицева группа.** Пусть, как и выше, X метрическое пространство с расстоянием $d : X \times X \longrightarrow \mathbb{R}$. Биекция φ множества X на себя называется **билипшицевой**, если для нее существуют две положительные константы $\lambda, \mu \in \mathbb{R}_+$, такие, что $\lambda d(x, y) \leq d(\varphi(x), \varphi(y)) \leq \mu d(x, y)$ для любых двух точек $x, y \in X$. Как обычно, множество всех билипшицевых биекций X на себя образует группу относительно композиции.

Рудольф Липшиц (`Rudolph Otto Sigismund Lipschitz`, 14 мая 1832, Кенигсберг — 07 октября 1903, Бонн) — знаменитый немецкий математик, основные работы которого относятся к теории чисел, теории дифференциальных уравнений, теории потенциала, математической физике и теории рядов Фурье. После учебы в Кенигсберге под руководством Франца Ноймана и Берлине под руководством Дирихле и **временных позиций** в Кенигсберге, Берлине и Бреслау (Вроцлав), в 1864 году Липшиц стал профессором в Бонне. Работы Липшица в теории чисел связаны главным образом с теорией квадратичных форм. В нашем курсе несколько раз встречается **условие Липшица** и определяемые этим условием липшицевы и билипшицевы отображения метрических пространств, а также целые липшицевы кватернионы. Именно Липшиц ввел спинорную группу Spin.

• **Группа изотонных преобразований.** Пусть теперь X — частично упорядоченное множество с отношением порядка $\leq$. Биекция φ множества X на себя называется **изотонной**, если она сохраняет порядок, т. е. для любых $x, y \in X$ из того, что $x \leq y$ вытекает, что $\varphi(x) \leq \varphi(y)$. Все изотонные биекции множества X на себя образуют группу, называемую **группой автоморфизмов** частично упорядоченнного множества X и обозначаемой $\mathrm{Aut}(X, \leq)$.

Задача. Биекция φ называется **антитонной**, если она обращает порядок, т. е. из $x \leq y$ вытекает, что $\varphi(x) \geq \varphi(y)$. Антитонные преобразования называются **антиавтоморфизмами** частично упорядоченного множества X. Биекция называется **монотонной**, если она изотонна или антитонна. Убедитесь, что все монотонные биекции X на себя образуют группу.

• **Группа гомеоморфизмов.** Пусть X — топологическое пространство. Биекция φ на себя называется **гомеоморфизмом**, если φ одновременно является непрерывной и открытой (т. е. как прообраз, так и образ открытого множества открыты). Группа $\mathrm{Aut}(X)$ всех гомеоморфизмов X на себя называется группой автоморфизмов топологического пространства X.

• **Группа метрических автоморфизмов.** Пусть (X, μ) – пространство с мерой μ, определенной на некоторой σ-алгебре измеримых множеств $\Omega \subseteq 2^X$. Биекция φ множества X на себя называется **метрическим автоморфизмом** этого пространства, если она **биизмерима** (иными словами, как прообразы, так и образы измеримых множеств измеримы), и **сохраняет меру**, т. е. $\mu(\varphi(U)) = \mu(U)$ для любого измеримого множества $U \in \Omega$. Множество $\mathrm{Aut}(X, \mu)$ называется группой метрических автоморфизмов пространства X.

Предостережение. В теории меры, эргодической теории и теории динамических систем принято пренебрегать множествами меры 0. В этом случае и метрические автоморфизмы часто понимаются не в определенном выше точном смысле, а по модулю множеств меры 0, причем никаких специальных оговорок об этом обычно не делается!

• **Группа диффеоморфизмов.** Пусть X — дифференцируемое многообразие. Биекция X на себя называется **диффеоморфизмом**, если как она сама, так и обратное к ней преобразование φ^{-1} бесконечно дифференцируемы. Множество $\mathrm{Diff}(X)$ всех диффеоморфизмов X на себя образует группу, называемую группой диффеоморфизмов X.

В геометрии встречаются *десятки* подобных примеров, например, в теории комплексных аналитических пространств расматривается

группа биголоморфных автоморфизмов, в алгебраической геометрии рассматриваются **группа бирегулярных автоморфизмов** и **группа бирациональных автоморфизмов** и т. д.

§ 13◇. Группы матриц

В этом параграфе мы рассмотрим некоторые группы матриц степени $n = 2$. В дальнейшем в книгах III, IV и IIbis мы вернемся ко многим из этих примеров в более общем контексте.

1. Группа $\mathrm{GL}(2, K)$. Пусть K — некоторое поле, например, $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Введем определитель матрицы $x \in M(2, K)$

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc.$$

Как мы узнаем в книге IV, определитель является гомоморфизмом, т. е. для любых двух матриц $\det(xy) = \det(x)\det(y)$.

Упражнение. Убедитесь в этом непосредственно для $n = 2$. Проверьте, что

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

• Тем самым, **полная линейная группа** степени 2 над K может быть определена как

$$\mathrm{GL}(2, K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc \neq 0 \right\}.$$

Это определение обобщается на матрицы над коммутативными кольцами, однако в этом случае условия $\det(x) \neq 0$ недостаточно, нужно требовать, чтобы $\det(x)$ был обратимым элементом кольца R. Для произвольных колец с 1 группа $\mathrm{GL}(n, R)$ вообще не может быть охарактеризована в терминах определителя и определяется непосредственно как группа обратимых элементов матричного кольца $M(n, R)$.

• **Специальная линейная группа** состоит из всех матриц с определителем 1. Таким образом,

$$\mathrm{SL}(2, K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; ad - bc = 1 \right\}.$$

В случае $K = \mathbb{R}$ группа $\mathrm{SL}(n, \mathbb{R})$ состоит из линейных преобразований пространства $\mathbb{R}^n$, сохраняющих *ориентированный* объем.

• Часто приходится рассматривать группу преобразований $\mathbb{R}^n$, сохраняющих объем, но *меняющих ориентацию*:

$$\mathrm{SL}^{\pm}(2,K)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\;\middle|\;ad-bc=\pm1\right\}.$$

2. Некоторые важнейшие подгруппы. Вот еще несколько примеров матричных групп (проверьте, что в каждом из этих примеров произведение двух матриц указанного вида, и обратная к такой матрице снова имеют такой же вид!).

• **Группа диагональных матриц**

$$D(2,K)=\left\{\begin{pmatrix}a&0\\0&d\end{pmatrix}\;\middle|\;a,d\in K^*\right\}.$$

• **Аффинная группа**

$$\mathrm{Aff}(1,K)=\left\{\begin{pmatrix}a&b\\0&1\end{pmatrix}\;\middle|\;a\in K^*,b\in K\right\}.$$

Убедитесь, что эта группа изоморфна группе $ax+b$, построенной в § 1.

• **Группа верхних треугольных матриц**

$$B(2,K)=\left\{\begin{pmatrix}a&b\\0&d\end{pmatrix}\;\middle|\;a,d\in K^*,b\in K\right\}.$$

• **Группа нижних треугольных матриц**

$$B^-(2,K)=\left\{\begin{pmatrix}a&0\\c&d\end{pmatrix}\;\middle|\;a,d\in K^*,c\in K\right\}.$$

Замечание. Буква `B` в названии этих групп является сокращением от **борелевская**[♮] **подгруппа** (`Borel subgroup`). Группа $B(2,K)$ называется стандартной борелевской подгруппой. Группа нижних треугольных матриц $B^-(2,K)$ совпадает с группой верхних треугольных матриц $B(2,K)$ для такого порядка индексов $1,2$, что $2<1$. Поэтому во многих книгах именно группа $B^-(n,K)$ называется

[♮]Как известно, биографии современников не приводятся, однако начинающий должен иметь в виду, что борелевские подгруппы, борелевские подалгебры, борелевские клетки и т. д. называются так в честь *швейцарского* математика **Армана Бореля**, который не имеет никакого отношения к *французскому* `аналисту` начала XX века **Эмилю Борелю** (1871–1956), в честь которого называются борелевские множества, борелевские функции и т. д.

стандартной борелевской подгруппой. В частности, группы $B(2,K)$ и $B^-(2,K)$ сопряжены в $\mathrm{GL}(2,K)$. Тем не менее, *на самом деле* т. е. в теоретико-множественном смысле, как подгруппы в $\mathrm{GL}(2,K)$, эти группы различны.

• **Группа верхних унитреугольных матриц**

$$U(2,K)=\left\{\begin{pmatrix}1&b\\0&1\end{pmatrix}\;\middle|\;b\in K\right\}.$$

• **Группа нижних унитреугольных матриц**

$$U^-(2,K)=\left\{\begin{pmatrix}1&0\\c&1\end{pmatrix}\;\middle|\;c\in K\right\}.$$

• **Группа мономиальных матриц**

$$N(2,K)=\left\{\begin{pmatrix}a&0\\0&d\end{pmatrix}\;\middle|\;a,d\in K^*\right\}\cup\left\{\begin{pmatrix}0&a\\d&0\end{pmatrix}\;\middle|\;a,d\in K^*\right\}.$$

• **Группа циркулянтов**

$$A(2,K)=\left\{\begin{pmatrix}a&b\\b&a\end{pmatrix}\;\middle|\;a,b\in K,a^2-b^2\neq 0\right\}.$$

• **Группа антициркулянтов**

$$A^-(2,K)=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix}\;\middle|\;a,b\in K,a^2+b^2\neq 0\right\}.$$

3. Классические группы. Пусть A — кольцо с инволюцией $a\mapsto\overline{a}$, т. е. антиавтоморфизмом порядка 2: $\overline{a+b}=\overline{a}+\overline{b}$, $\overline{ab}=\overline{b}\,\overline{a}$, $\overline{\overline{a}}=a$. Определим **симплектическую группу** как

$$\mathrm{Sp}(2,K)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}(2,A)\;\middle|\;\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\begin{pmatrix}\overline{d}&-\overline{b}\\-\overline{c}&\overline{a}\end{pmatrix}\right\}$$

и **ортогональную группу** как

$$\mathrm{O}(2,K)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}(2,A)\;\middle|\;\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\begin{pmatrix}\overline{d}&\overline{b}\\\overline{c}&\overline{a}\end{pmatrix}\right\}.$$

Упражнение. Проверьте, что эти определения действительно задают подгруппы в $\mathrm{GL}(2,A)$.

В дальнейшем мы применяем эту конструкцию главным образом к случаю, когда $R = M(n, A)$ является кольцом матриц над коммутативным кольцом, а в качестве инволюции на R рассматривается транспонирование $x \mapsto x^t$. Заметим, что коммутативность нужна именно для того, чтобы гарантировать, что транспонирование является инволюцией. В этом случае уравнения, определяющие $\mathrm{Sp}(2, R)$ и $\mathrm{O}(2, R)$, превращаются в

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & e \\ -e & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} 0 & e \\ -e & 0 \end{pmatrix}$$

или, соответственно, в

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^t = \begin{pmatrix} 0 & e \\ e & 0 \end{pmatrix},$$

так что эти группы действительно совпадают (с точностью до сопряженности) с **расщепимыми классическими группами**, которые мы рассматриваем в книге IV, посвященной линейной алгебре и во второй части настоящей книги.

4. Конечные линейные группы. Многие важные группы (например, свободные группы и **все** конечные группы) допускают естественные реализации как группы матриц над коммутативными кольцами, в частности, над полями. Вот несколько примеров.

• Пусть $R = \mathbb{Z}/m\mathbb{Z}$. Группа

$$\left\{ \begin{pmatrix} \pm 1 & x \\ 0 & 1 \end{pmatrix},\ x \in \mathbb{Z}/m\mathbb{Z} \right\}$$

изоморфна группе диэдра.

• Группа кватернионов может быть реализована как следующая группа матриц в $\mathrm{SL}(2, \mathbb{C})$:

$$\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \quad \pm \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

Эти матрицы ввел Кэли, но физики обычно называют их — или какие-то их скалярные кратные — **матрицами Паули**.

• Физики обычно реализуют группу треугольника $S_3 \cong D_3$ как следующую группу матриц в $\mathrm{GL}(2, \mathbb{R})$

$$\begin{matrix} \pm 1 & 0 \\ 0 & 1 \end{matrix}, \quad \begin{matrix} \frac{1}{2} & 1 & \pm\sqrt{3} \\ \frac{1}{2} & \pm\sqrt{3} & -1 \end{matrix}, \quad \begin{matrix} \frac{1}{2} & -1 & \pm\sqrt{3} \\ \frac{1}{2} & \mp\sqrt{3} & -1 \end{matrix},$$

(знаки пробегаются согласованно, так что в этой группе действительно 6 элементов). Сопряжение позволяет сделать все коэффициенты матриц рациональными, т. е. вложить S_3 в $\mathrm{GL}(2,\mathbb{Q})$:

$$\begin{pmatrix}\pm1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}\frac{1}{2} & 1\\ \pm3 & -1\end{pmatrix},\ \begin{pmatrix}\frac{1}{2} & -1\\ \mp3 & -1\end{pmatrix}\ \pm1.$$

Небольшое дополнительное усилие позволяет реализовать S_3 уже как подгруппу $\mathrm{GL}(2,\mathbb{Z})$:

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\ \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ \begin{pmatrix}1 & 0\\ -1 & -1\end{pmatrix},\ \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix},\ \begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix},\ \begin{pmatrix}-1 & -1\\ 0 & 1\end{pmatrix}.$$

Проверьте, что эти группы действительно сопряжены над $\mathbb{Q}$. Что бы это могло означать с точки зрения полей характеристики 2?

§ 14♡. Группы движений

> Релятивистские **преобразования Лоренца** никогда великим физиком Лоренцем не рассматривались: он *поставил* вопрос о группе преобразований симметрии уравнений электродинамики Максвелла, но решил его *неверно*, указав совсем не те преобразования, которые сейчас называют его именем. Пуанкаре, излагая эту ошибочную работу Лоренца в своих лекциях, нашел правильные преобразования, а при публикации этих результатов назвал их **преобразованиями Лоренца**, и это название сохранилось до сих пор.
>
> Владимир Игоревич Арнольд. *Что такое математика?*

По знаменитому тезису Феликса Клейна геометрия есть теория групп[♮]. Впрочем, сегодня принято говорить чуть иначе: теория групп есть геометрия. Движения, переносы, вращения, собственные вращения (т. е. вращения, не меняющие ориентацию) обычной эвклидовой геометрии образуют группы (композиция двух переносов является переносом, тождественное преобразование является переносом, etc.).

1. Ортогональная группа. Пусть вначале K — произвольное поле, в дальнейшем мы будем, как правило, предполагать, что $K=\mathbb{R}$. Зафиксируем **симметрическую** матрицу $f\in M(n,R)$, иными словами, мы предполагаем, что матрица f совпадает со своей транспонированной, $f^t=f$. С матрицей f связаны несколько групп:

• **ортогональная группа**

$$O(n,K,f)=\{g\in \mathrm{GL}(n,K)\mid gfg^t=f\},$$

[♮]Вот как в точности звучало его *определение* геометрии: “Дано многообразие и в нем группа преобразований. Требуется развить теорию инвариантов этой группы.” — *Erlanger Programm*, [80].

проверьте, что это действительно группа! **Решение:** $(hg)^t = g^t h^t$ и $(g^{-1})^t = (g^t)^{-1}$.

• **специальная ортогональная группа**

$$\mathrm{SO}(n, K, f) = \{g \in \mathrm{SL}(n, K) \mid gfg^t = f\} = O(n, K, f) \cap \mathrm{SL}(n, K).$$

• **спинорная группа** $\mathrm{Spin}(n, K, f)$, **ядро спинорной нормы** $\Omega(n, K, f)$ и другие группы, которые будут определены в дальнейшем.

При этом как правило предполагается, что матрица $f = (f_{ij})$ сама невырождена, иными словами $\det(f) \neq 0$. Ортогональную группу можно истолковать как группу изометрий пространства $V = K^n$ со скалярным произведением, которое задается на базисе $e_1, \ldots, e_n$ пространства K^n посредством $B(e_i, e_j) = f_{ij}$. Как мы узнаем в книге IV, в случае $K = \mathbb{R}$ всякое n-мерное пространство с невырожденным скалярным произведением изометрично *ровно одному* из пространств $\mathbb{R}^{p,q}$, $p + q = n$, для которого

$$f = \begin{matrix} e_p & 0 \\ 0 & -e_q \end{matrix}$$

(это утверждение вытекает из теоремы Лагранжа и закона инерции Сильвестра). Иными словами, в $\mathbb{R}^{p,q}$ скалярное произведение двух векторов $x = (x_1, \ldots, x_n)$ и $y = (y_1, \ldots, y_n)$ определяется равенством

$$B(x, y) = x_1 + \ldots x_p y_p - x_{p+1} y_{p+1} - \ldots - x_n y_n.$$

Ортогональная группа пространства $\mathbb{R}^{p,q}$ обозначается через $O(p, q, \mathbb{R})$. Она состоит из всех матриц, для которых

$$O(p, q, \mathbb{R}) = \quad g \in \mathrm{GL}(n, K) \quad g \begin{matrix} e_p & 0 \\ 0 & -e_q \end{matrix} g^t = \begin{matrix} e_p & 0 \\ 0 & -e_q \end{matrix} \quad .$$

В случае $q = 0$ пространство, $\mathbb{R}^n$ называется **эвклидовым**. В этом случае ортогональная группа обозначается просто $O(n, \mathbb{R})$ и называется **классической ортогональной группой**; по определению она состоит из всех $g \in \mathrm{GL}(n, \mathbb{R})$ таких, что $gg^t = e$. Как обычно, $\mathrm{SO}(p, q, \mathbb{R}) = O(p, q, \mathbb{R}) \cap \mathrm{SL}(n, \mathbb{R})$ и $\mathrm{SO}(n, \mathbb{R}) = O(n, \mathbb{R}) \cap \mathrm{SL}(n, \mathbb{R})$

2. Группы движений плоскости. Сейчас мы рассмотрим **эвклидову плоскость** $\mathbb{R}^2$ и **гиперболическую плоскость** $\mathbb{R}^{1,1}$. С точки зрения дальнейших многомерных обобщений нас интересуют группы $O(2, \mathbb{R})$ и $O(1, 1, \mathbb{R})$. Между этими группами есть существенное различие. Группа $\mathrm{SO}(2, \mathbb{R})$ совпадает с группой **эвклидовых вращений**

$$\mathrm{SO}(2, \mathbb{R}) = \begin{matrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{matrix} \quad \varphi \in \mathbb{R} \quad .$$

Группа $O(2, \mathbb{R})$ порождается $\mathrm{SO}(2, \mathbb{R})$ и любым отражением, например, $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$.

В то же время группа **лоренцевых вращений**

$$\mathrm{SO}^+(1, 1, \mathbb{R}) = \begin{matrix} \mathrm{ch}(\varphi) & \mathrm{sh}(\varphi) \\ \mathrm{sh}(\varphi) & \mathrm{ch}(\varphi) \end{matrix} \quad \varphi \in \mathbb{R} \quad .$$

имеет индекс 2 в $\mathrm{SO}(1,1,\mathbb{R})$ так как $-e \in \mathrm{SO}(1,1,\mathbb{R}) \setminus \mathrm{SO}^+(1,1,\mathbb{R})$ (в самом деле, $\mathrm{ch}(\varphi) \geq 1$). Тем самым $\mathrm{SO}^+(1,1,\mathbb{R})$ имеет индекс 4 в $O(1,1,\mathbb{R})$, и чтобы породить $O(1,1,\mathbb{R})$ кроме лоренцевых вращений нужны еще две матрицы, скажем $-e$ и любое отражение.

Группа собственных эвклидовых движений плоскости порождается $\mathrm{SO}(2,\mathbb{R})$ и группой трансляций. Она изоморфна группе 3×3 матриц

$$\left\{ \begin{pmatrix} \cos(\varphi) & \sin(\varphi) & a \\ -\sin(\varphi) & \cos(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix} \quad \varphi, a, b \in \mathbb{R} \right\}.$$

Полная группа эвклидовых движений плоскости порождается $O(2,\mathbb{R})$ и группой трансляций. Она изоморфна

$$\left\{ \begin{pmatrix} \cos(\varphi) & \pm\sin(\varphi) & a \\ -\sin(\varphi) & \pm\cos(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix} \quad \varphi, a, b \in \mathbb{R} \right\}$$

(знаки пробегаются одновременно).

3. Группа эвклидовых движений. Полная группа изометрий эвклидова пространства $V = \mathbb{R}^n$ называется **группой эвклидовых движений** и обозначается $\mathrm{Isom}(\mathbb{R}^n)$. Эвклидово движение является композицией вращения (собственного или зеркального) и параллельного переноса и задается символом Зейтца $\{g|u\}$, где теперь $g \in O(n,R)$. Подгруппа $\mathrm{Isom}^+(\mathbb{R}^n)$, состоящая из движений с определителем 1, называется группой собственных движений.

4. Группа Лоренца. В специальной теории относительности рассматривается 4-мерное **пространство Минковского** $\mathbb{R}^{3,1}$. Как множество оно совпадает с 4-мерным пространством $\mathbb{R}^4$, но координаты вектора x в нем обычно нумеруются (x_0, x_1, x_2, x_3), где x_0 обозначает временную, а x_1, x_2, x_3 — пространственные координаты. Однако, в качестве метрики в пространстве рассматривается не обычная эвклидова метрика, а **псевдоэвклидова метрика**, задаваемая скалярным произведением $B(x,y) = -x_0y_0 + x_1y_1 + x_2y_2 + x_3y_3$. Иными словами, квадрат длины вектора x равен $x^2 = B(x,x) = -x_0^2 + x_1^2 + x_2^2 + x_3^2$.

Гендрик Антон Лоренц (`Hendrik Antoon Lorentz`, 18 июля 1853, Арнхем — 4 февраля 1928, Гарлем) — замечательный голландский физик, один из классиков XIX века, создатель электродинамики движущихся сред и электронной теории, один из творцов специальной теории относительности. В 1902 году Лоренц получил одну из первых Нобелевских премий по физике за свою теорию электрона. Большая часть его жизни связана с Лейденским университетом. После окончания этого университета в 1875 году в 1878–1912 годах он был там профессором. В 1912 году он оставил свою кафедру Эренфесту, а сам стал директором исследовательского института в Гарлеме. Много понятий в физике носят его имя. В нашем курсе встречаются группа Лоренца, преобразования Лоренца, лоренцевы вращения, лоренцевы решетки и т. д.

Герман Минковский (Hermann Minkowski, 22 июня 1864, Алексотас, под Каунасом — 12 января 1909, Геттинген) — гениальный российский математик, работавший в Германии, основные работы которого относятся к теории чисел, геометрии, теории квадратичных форм и математической физике, создатель **геометрии чисел**. После получения в 15 лет аттестата гимназии в Кенингсберге он учился в Кенигсберге и Берлине. В 1883 году Минковский выиграл Grand Prix Парижской Академии наук за (студенческую!!) работу по теории квадратичных форм. Уже в 1885 году ему был присужден **докторат** в Кенигсберге, а в 1887 **хабилитация** в Бонне. После этого он работал профессором в Бонне, Кенигсберге и Цюрихе, а с 1902 года в Геттингене. Минковский был ближайшим другом Давида Гильберта, и Брауэр (Brouwer!!) постоянно инсинуировал, что многие из работ Гильберта, "не являются его собственными", намекая на знаменитые прогулки Гильберта, Минковского и Гурвица, во время которых они беседовали о математике. В 1907 году Минковский осознал, что работу Лоренца, Пуанкаре и Эйнштейна по специальной теории относительности естественнее всего формулировать в терминах четырехмерного пространства—времени. Работы Минковского по математическим основаниям электродинамики и теории относительности (*Raum und Zeit*, *Zwei Abhandlungen über die Grundgleichungen der Elektordynamik*) оказали огромное влияние на все последующее развитие физики. В нашем курсе упоминяются сложение и умножение по Минковскому, пространство Минковского, неравенство Минковского, функционал Минковского, теорема Минковского—Хассе и другие восходящие к нему понятия и результаты. Минковский умер на взлете своего таланта в 44 года от перитонита.

Группа изометрий $\mathcal{L}$ пространства $\mathbb{R}^{3,1}$ называется **группой Лоренца** (или, иногда **полной группой Лоренца**). Иными словами, после подходящего выбора базиса в $\mathbb{R}^{3,1}$ группа Лоренца $\mathcal{L}$ может быть отождествлена с множеством всех матриц $g \in M(4,\mathbb{R})$ таких, что $gfg^t = f$, где $f = \operatorname{diag}(-1,1,1,1)$. Это значит, что с точки зрения теории пространств со скалярным произведением, которую мы изучаем в книге IV, группа Лоренца представляет собой группу $O(3,1,\mathbb{R})$. Укажем шесть типичных элементов группы Лоренца, первые три из которых являются обычными эвклидовыми вращениями пространства, а остальные три — **лоренцевыми вращениями**:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\varphi) & \sin(\varphi) & 0 \\ 0 & -\sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\varphi) & 0 & \sin(\varphi) \\ 0 & 0 & 1 & 0 \\ 0 & -\sin(\varphi) & 0 & \cos(\varphi) \end{pmatrix},$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(\varphi) & \sin(\varphi) \\ 0 & 0 & -\sin(\varphi) & \cos(\varphi) \end{pmatrix}, \quad \begin{pmatrix} \operatorname{ch}(\varphi) & \operatorname{sh}(\varphi) & 0 & 0 \\ \operatorname{sh}(\varphi) & \operatorname{ch}(\varphi) & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} \operatorname{ch}(\varphi) & 0 & \operatorname{sh}(\varphi) & 0 \\ 0 & 1 & 0 & 0 \\ \operatorname{sh}(\varphi) & 0 & \operatorname{ch}(\varphi) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \operatorname{ch}(\varphi) & 0 & 0 & \operatorname{sh}(\varphi) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \operatorname{sh}(\varphi) & 0 & 0 & \operatorname{ch}(\varphi) \end{pmatrix}.$$

Если варьировать здесь φ, то эти 6 типов преобразований порождают подгруппу индекса 4 в группе Лоренца, называемую **собственной группой Лоренца** и обозначаемой $\mathcal{L}_{+\uparrow}$. Следующие четыре матрицы являются представителями смежных классов группы Лоренца $\mathcal{L}$ по модулю собственной группы Лоренца $\mathcal{L}_{+\uparrow}$:

$$\begin{matrix} 1 & 0 \\ 0 & e \end{matrix}, \quad \begin{matrix} -1 & 0 \\ 0 & e \end{matrix}, \quad \begin{matrix} 1 & 0 \\ 0 & -e \end{matrix}, \quad \begin{matrix} -1 & 0 \\ 0 & -e \end{matrix},$$

где e обозначает единичную матрицу порядка 3. Подгруппа в $\mathcal{L}$, порожденная собственной группой Лоренца $\mathcal{L}_{+\uparrow}$ и $\mathrm{diag}(1,-e)$, обозначается $\mathcal{L}_{\uparrow}$ и называется **ортохронной группой Лоренца**, а подгруппа, порожденная $\mathcal{L}_{+\uparrow}$ и $\mathrm{diag}(-1,-e)$, обозначается $\mathcal{L}_{+}$ и называется **специальной группой Лоренца**. Таким образом, $\mathcal{L}_{\uparrow}$ — это в точности подгруппа в $O(3,1,\mathbb{R})$, состоящая из матриц $g=(g_{ij})$ с положительным коэффициентом g_{00}, с физической точки зрения, это в точности, преобразования, сохраняющие направление времени (но, возможно, меняющая ориентацию пространства). С другой стороны $\mathcal{L}_{+}=\mathrm{SO}(3,1,\mathbb{R})$ – это в точности подгруппа в $O(3,1,\mathbb{R})$, состоящая из матриц с определителем 1, которые либо сохраняют как направление времени, так и ориентацию пространства, либо одновременно меняют и то и другое. Легко видеть, что $\mathcal{L}_{+\uparrow}=\mathcal{L}_{\uparrow}\cap\mathcal{L}_{+}$. Ясно, что в группе Лоренца есть еще одна подгруппа индекса 2, порожденная $\mathcal{L}_{+\uparrow}$ и матрицей $\mathrm{diag}(-1,e)$, сохраняющая ориентацию пространства (но, возможно, меняющая направление времени), но физиков, похоже, она не очень интересует, потому что устойчивого общепринятого названия у нее нет.

Комментарий. Группу Лоренца определил Анри Пуанкаре в 1905 году. Многие физики называют пространством Минковского не пространство $\mathbb{R}^{3,1}$, а пространство $\mathbb{R}^{1,3}$. Это значит, что скалярное произведение задается равенством $B(x,y)=x_0y_0-x_1y_1-x_2y_2-x_3y_3$. Ясно, однако, что это не влияет на группу Лоренца: $O(1,3,\mathbb{R})=O(3,1,\mathbb{R})$. Вообще, терминологию нельзя признать полностью установившейся. Например, иногда группой Лоренца называют не саму группу $O(3,1,\mathbb{R})$, а какую-то из указанных выше подгрупп индекса 2 или 4. Некоторые авторы называют собственной группой Лоренца $\mathcal{L}_{+}$, а не $\mathcal{L}_{+\uparrow}$, etc. Наша терминология следует книге Мессиа [81]. Вообще у физиков есть отдельное название для *каждой* вещественной ортогональной (или, как они говорят, *псевдоортогональной*) группы $\mathrm{SO}(p,q,\mathbb{R})$. Так, например, они называют группу $\mathrm{SO}(4,1,\mathbb{R})$ (однородной) **группой де Ситтера**, группу $\mathrm{SO}(4,2,\mathbb{R})$ — **конформной группой** и т. д.

Отступление. С топологической точки зрения собственная группа Лоренца $\mathcal{L}_{+\uparrow}$ связна — в действительности это *в точности* связная компонента 1 в группе Лоренца $\mathcal{L}$. В то же время, она не является односвязной, а изоморфна факторгруппе односвязной группы $\mathrm{SL}(2,\mathbb{C})$ по подгруппе $\{\pm e\}$. В действительности, в релятивистской квантовой механике (Мессия, l.c.) электрон считает, что группой движений пространства—времени является именно универсальная накрывающая группы Лоренца $\mathrm{SL}(2,\mathbb{C})$, а вовсе не сама группа Лоренца $\mathcal{L}$.

5. Группа Пуанкаре. Как и выше, расмотрим пространство Минковского $\mathbb{R}^{3,1}$ и группу движений этого пространства, которая порождается группой Лоренца и всеми трансляциями пространства—времени. Эта группа называется **группой Пуанкаре** $\mathcal{P}$ (alias, **неоднородной группой Лоренца**). С точки зрения своего строения группа Пуанкаре является **полупрямым произведением** $\mathcal{P}=\mathcal{L}\leftthreetimes\mathcal{T}$

Анри Пуанкаре (Henri Poincaré, 29 апреля 1854, Нанси — 17 июля 1912, Париж) — самый знаменитый и продуктивный среди математиков конца XIX века, автор более 500 работ, в том числе множества книг. Работы Пуанкаре охватывают практически всю математику: теорию автоморфных функций, геометрию, топологию, теорию дифференциальных уравнений и уравнений с частными производными и многие разделы астрономии, математической и теоретической физики. Независимо от Эйнштейна создал специальную теорию относительности, по крайней мере в ее математических аспектах. После учебы в Политехнической школе Пуанкаре заканчивает Горную школу и несколько месяцев работает горным инженером — более того, как упоминает Гастон Жюлиа [82], в списках министерства общественных работ Пуанкаре числится как инженер, с 1893 года как старший инженер, а с 1910 года как генеральный инспектор шахт. Однако, фактически уже в 1879 году он защищает диссертацию и с 1881 года преподает в Парижском университете, где в 1886 году становится профессором (по кафедре математической астрономии и небесной механики, которую занимал до самой смерти). Много введенных им понятий встречаются в курсах геометрии, топологии и теории обыкновенных дифференциальных уравнений: гипотеза Пуанкаре, модель Пуанкаре, фундаментальная группа, комплекс Пуанкаре, двойственность Пуанкаре, классификация особых точек, теорема Пуанкаре о возвращении, etc. Камиль Жордан так отозвался о работе Пуанкаре об особых точках дифференциальных уравнений: «Она выше всяких похвал, к ней в полной мере можно отнести слова, некогда написанные Якоби об Абеле: “Ее автору удалось решить задачу, о которой до него никто не смел и мечтать”». На русский переведено большое количество книг Пуанкаре, как научных [83], [84], так и философских и научно-популярных, в том числе: [85]–[88]. Эти книги *в основном* вошли в том [89]. Большое количество его статей вошло в собрание [90]–[92]. Третий том избранных трудов содержит также чрезвычайно интересные статьи Гастона Жюлиа, Жака Адамара, Андре Вейля, Ганса Фрейденталя, Лорана Шварца и Луи де Бройля, посвященные жизни Пуанкаре и его вкладу в математику и физику. Один из двоюродных братьев Анри Пуанкаре, Раймон Пуанкаре был знаменитым политиком, президентом и председателем совета министров Франции, а другой, Люсьен Пуанкаре — известным физиком, ректором Парижского университета.

группы трансляций $\mathcal{T}$ и группы Лоренца $\mathcal{L}$. Иными словами, $\mathcal{P} = \mathcal{L}\mathcal{T}$, причем $\mathcal{T} \trianglelefteq \mathcal{P}$ и $\mathcal{L} \cap \mathcal{T} = 1$.

Комментарий. В *старинных* учебниках, например в [**217**], группой Пуанкаре называется первая гомотопическая группа, т. е. то, что сегодня принято называть **фундаментальной группой** многообразия. Однако в этом смысле выражение **группа Пуанкаре** ни разу не употреблялось уже лет 40.

§ 15◇. Групповые кольца

Сейчас мы объясним, что — по крайней мере формально — теория групп является разделом теории ассоциативных колец.

1. Групповая алгебра. Пусть G — группа, а R — коммутативное

ассоциативное кольцо с 1. В большинстве обычных приложений предполагается, что $R = K$ — поле или $R = \mathbb{Z}$ — кольцо целых чисел. Сейчас мы свяжем с парой (G, R) кольцо $R[G]$, называемое **групповым кольцом** группы G над R (или с коэффициентами из R). Элементами этого кольца являются *формальные линейные комбинации* элементов группы G с коэффициентами из R. По существу это понятие ввел Молин, позже его стали систематически использовать Фробениус и Шур.

Исайа Шур (`Isaia Schur`, 10 января 1875, Могилев — 10 января 1941, Тель Авив) — гениальный белорусский алгебраист, работавший в Германии. Основные работы Шура относятся к теории групп, в первую очередь теории представлений и теории линейных групп, теории матриц, алгебраической теории чисел, теории степенных рядов, теории функций и теории интегральных уравнений. Шур учился в Берлине и в 1901 защитил диссертацию под руководством Фробениуса. В 1903 году Шур получил позицию в Берлине, где и работал, за исключением 1911–1916 годов, когда он был в Бонне. Однако только в 1919 году он стал профессором Берлинского университета. Первая попытка отстранить его от должности была предпринята уже в 1933 году, но тогда многие, в том числе Бибербах, выступили в его защиту, и в результате его отставка была приостановлена. Вальтер Ледерман вспоминает, что в ноябре 1933 года его экзаменовали Шур вместе с Бибербахом в нацистской униформе!! В это время Шуру поступило несколько приглашений из США и Великобритании, от которых он отказался, так как надеялся на **`изменение ситуации`** в Германии!!! Однако вместо этого в 1935 году его окончательно отстранили от должности, а в 1938 году — изгнали из Прусской Академии и в 1939 году Шур эмигрировал в Палестину. Последние годы его жизни омрачены болезнью, тяжелой депрессией и нищетой настолько полной, что он вынужден был продать свою научную библиотеку Институту высших научных исследований в Принстоне!!! В нашем курсе встречаются проективные представления, лемма Шура, мультипликатор Шура, теорема Шура о коммутанте, теорема Шура—Цассенхауза, теоремы Шура о линейных группах и большое количество теорем Шура в теории матриц. Кроме того, в теории представлений и алгебраической комбинаторике рассматриваются функции Шура и кольца Шура (S-кольца). Все, кто встречал Шура в лучшие годы в Берлине, вспоминают его как харизматического научного руководителя и *гениального* преподавателя, чьи лекции собирали человек по 200, так что тем, кто опоздал к началу, приходилось пользоваться театральным биноклем. Среди непосредственных учеников Шура такие выдающиеся алгебраисты, как Рихард Брауэр и Альфред Брауэр, Бернард Нойман и Ханна Нойман, Лев Аркадьевич Калужнин, Хельмут Виландт, Курт Хирш и Вальтер Ледерман.

Обозначим через $R[G]$ множество функций $G \longrightarrow R$ *с конечным носителем*. Иными словами, элементами множества $R[G]$ являются всевозможные функции $a : G \longrightarrow R$ такие, что $a(g) = 0$ для всех

$g \in G$, кроме конечного числа. В теории групп значение функции $a(g)$ обычно обозначается через a_g. Функция a обычно представляется следующим образом. Для каждого $h \in G$ можно определить δ-функцию $e_h : G \longrightarrow R$, которая принимает значение 1 в $g = h$ и 0 во всех остальных элементах: $e_h(g) = \delta_{gh}$. Ясно, что любая функция $a \in R[G]$ представляется как линейная комбинация δ-функций: $a = \sum a_g e_g$. Заметим, что во многих книгах e_g отождествляется с g и, таким образом, G рассматривается как подмножество в $R[G]$.

Сложение в $R[G]$ задается как **сумма функций**: если $a = \sum a_g e_g$ и $b = \sum b_g e_g$, то

$$a + b = \sum (a_g + b_g) e_g.$$

С другой стороны, умножение в $R[G]$ задается как **свертка функций**:

$$\sum a_g e_g \cdot \sum b_g e_g = \sum_{g \in G} \left(\sum_{fh=g} a_f b_h \right) e_g.$$

Стандартные вычисления, которые мы приводим в книге III, показывают, что эти операции превращают $R[G]$ в ассоциативное кольцо с единицей $1 = e_1$. Если положить, кроме того, $\lambda \sum a_g e_g = \sum \lambda a_g e_g$, то $R[G]$ превращается в R**-алгебру**.

Во всей этой конструкции δ-функции e_g использовались только для того, чтобы придать точный математический смысл понятию формальной линейной комбинации. После того, как это однажды сделано, мы можем встать на классическую точку зрения и отождествить G с ее образом в $R[G]$ полагая $e_g = g$. Иными словами, мы считаем, что элементы группы G образуют базис $R[G]$ как свободного R-модуля. В соответствии с приведенной формулой для свертки это **мультипликативный базис**. Иными словами, произведение двух базисных элементов снова является базисным элементом (а не просто какой-то линейной комбинацией базисных элементов), при этом умножение базисных элементов — это просто их умножение в группе G. Начиная с этого момента мы пишем $\sum a_g g$ вместо $\sum a_g e_g$.

Сопоставление $G \rightsquigarrow R[G]$ задает функтор из категории групп в категорию R-алгебр. Для этого нужно заметить, что групповому гомоморфизму $\phi : H \longrightarrow G$ можно сопоставить гомоморфизм R-алгебр

$$\widetilde{\phi}\Big(\sum a_h h \Big) = \sum a_h \phi(h),$$

причем это сопоставление обладает обычными свойствами, в частности, $\widetilde{\mathrm{id}}_G = \mathrm{id}_{R[G]}$ и $\widetilde{\phi\psi} = \widetilde{\phi}\widetilde{\psi}$.

Групповые кольца замечательны тем, что они позволяют истолковать (конечные) *подмножества* — и, в действительности, все *мультимножества*, составленные из элементов группы G — как *элементы* кольца $R[G]$ и проводить с ними все обычные вычисления, притом *с учетом кратности*. При этом подмножеству $X = \{g_1, \dots, g_n\} \subseteq G$ сопоставляется элемент $e_X = g_1 + \dots + g_n \in R[G]$.

Предостережение. В анализе групповым кольцом *топологической группы* чаще всего называются *другие* объекты, а именно **пополнения** группового кольца $\mathbb{C}[G]$, относительно подходящих топологий! Чаще всего по умолчанию аналитики обозначают через $\mathbb{C}[G]$ то, что алгебраисты называют **групповым $\mathbb{C}^*$-кольцом**.

Много конкретных примеров групповых (и полугрупповых) алгебр приведено в книге III. Ограничимся поэтому несколькими простейшими примерами. Вот как выглядят, скажем, групповые кольца циклических групп:

• $R[\mathbb{Z}] \cong R[x, x^{-1}]$ есть кольцо многочленов Лорана;

• $R[C_n] \cong R[x]/(x^n - 1)$ есть кольцо векторов длины n относительно циклической свертки.

Первый из этих примеров естественно обобщается на групповые кольца свободных групп:

• $R[\mathbb{Z}^n] \cong R[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ есть кольцо многочленов Лорана от n переменных;

• $R[F_n] \cong R\langle x_1^{\pm 1}, \dots, x_n^{\pm 1}\rangle$ есть кольцо многочленов Лорана от n *некоммутирующих* переменных.

Групповые алгебры представляют собой интереснейшие примеры колец и с ними связано много классических вопросов, часть из которых не решена в полной общности и сегодня. Одной из самых знаменитых проблем, на много десятилетий определивших развитие теории, была **проблема изоморфизма**. Что можно сказать о (конечных) группах H и G, если $K[H] \cong K[G]$? В частности, верно ли, что $H \cong G$? В общем случае ответ оказался отрицательным.

2. Групповая алгебра как пример алгебры Хопфа. Для тех, кто слышал о тензорных произведениях, отметим, что *в действительности* групповая алгебра $R[G]$ является не просто ассоциативной алгеброй. На ней естественно определяется гораздо более богатая алгебраическая структура. Сейчас мы введем на $R[G]$ дополнительные алгебраические операции, превращающие ее в **алгебру Хопфа**. Наряду с универсальной обертывающей алгеброй $U(L)$ алгебры Ли и структурным кольцом аффинной алгебраической группы — это один из основных примеров алгебр Хопфа.

• Самой важной из этих операций является **диагональное отображение**, аналогичное умножению, но действующее в обратном направлении, часто называемое

Хайнц Хопф (Heinz Hopf, 19 октября 1894, Грэбшен, Бреслау — 3 июня 1971, Цолликон) — замечательный немецкий математик, внесший определяющий вклад в формирование алгебраической топологии и связанных с ней разделов алгебры, в частности, гомологической алгебры. Отец Хопфа был евреем, но под влиянием жены обратился в лютеранство. В 1913 году Хопф поступил во Вроцлавский университет — явный анахронизм: в 1913 году университет назывался Schlesische Friedrich Wilhelms Universität Breslau — но в мою бытность там носил название Uniwersytet Wrocławski im. Bolesława Bieruta — *the slow one now will later be fast, as the present now will later be past, the order is rapidly fadin', and the first one now will later be last, for the times they are a-changin'.* Там он учился у Кнезера и Шмидта, но посещал также лекции Дена и Штейница в Политехническом институте. В 1914 году он немедленно записался добровольцем и сражался на западном фронте, но после войны продолжил учебу вначале в снова во Вроцлавском университете, а потом в Гейдельберге и Берлине, где слушал лекции Шура и, наконец, в 1925 году получил докторат за работу по топологии многообразий. После этого он уезжает в Геттинген, где попадает под влияние Эмми Нетер. Там же начинается его многолетняя дружба и сотрудничество с Павлом Сергеевичем Александровым. В 1931 году Хопф занимает кафедру в Цюрихе, которую до этого занимал Герман Вейль. В дальнейшем Хопф неоднократно использовал свое влияние, чтобы помогать оказавшимся в трудном положении немецким коллегам. Однако технически он сам оставался германским подданным и, когда нацисты потребовали, чтобы он вернулся в Германию, тут же подал прошение о швейцарском гражданстве и на удивление быстро его получил! После войны Хопф сыграл громадную роль в возрождении научной жизни в Германии, в частности, в создании Математического института в Обервольфахе. Многие понятия в алгебраической топологии связаны с его именем, в нашем курсе кроме алгебр Хопфа встречается теорема Хопфа, хопфовы группы и т. д.

Однако Хайнц Хопф не имеет никакого отношения к уравнению Винера—Хопфа, которое названо так в честь *австрийского* математика **Эберхарда Хопфа** (Eberhard Frederich Ferdinand Hopf, 4 апреля 1902, Зальцбург — 24 июля 1983), биография которого еще более живописна: в то время, как Хайнц Хопф уехал из Германии, Эберхард Хопф в 1936 году *переехал в Германию* и, после службы в Германском институте воздухоплавания, в 1944 году стал профессором в Мюнхене. Этого многие не смогли ему простить и, как следствие, его результаты по эргодической теории игнорировались или приписывались другим, но, впрочем, это не имеет отношения к нашему сюжету.

также **копроизведением**:

$$\Delta : R[G] \longrightarrow R[G] \otimes R[G], \qquad \sum a_g g \mapsto \sum a_g g \otimes g.$$

• Аналогом обращения в группе является **антипод**

$$\eta : R[G] \longrightarrow R[G], \qquad \sum a_g g \mapsto \sum a_g g^{-1}.$$

• Наконец, понятием, аналогичным понятию 1, является **аугментация**, извест-

ная также как **пополняющее отображение** или **коединица**:

$$\epsilon : R[G] \longrightarrow R, \qquad \sum a_g g \mapsto \sum a_g.$$

Конечно, теперь элементы группы G могут быть охарактеризованы как **групповые элементы** (`group-like elements`) алгебры $\mathbb{Z}[G]$, т. е. такие элементы, что $\Delta(x) = x \otimes x$. Это значит, что если $Z[H] \cong \mathbb{Z}[G]$ *как алгебры Хопфа*, то $H \cong G$.

§ 16✠. Группы в алгебре

В § 8 приведены примеры групп, возникающих как группы автоморфизмов различных структур, рассматривающихся в алгебре, геометрии, топологии и анализе. Группы автоморфизмов являются важнейшим, но далеко не единственным источником примеров групп. В настоящем и следующем параграфах мы обсудим несколько важнейших примеров групп, которые строятся не как группы автоморфизмов. Понимание изложенных в настоящем параграфе примеров требует знания рудиментов линейной алгебры, до понятия тензорного произведения модулей включительно.

1. Группа Брауэра. Пусть K — поле. Если A и B — *конечномерные* алгебры над K, то их тензорное произведение $A \otimes B$ как векторных пространств превращается в алгебру, если положить $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2$. Получающаяся так алгебра называется **тензорным произведением** алгебр A и B. Алгебра A называется **центральной**, если ее центр совпадает с K, и **простой**, если в A ровно 2 двусторонних идеала, а именно 0 и сама алгебра A.

По **теореме Веддербарна** каждая конечномерная центральная простая алгебра A над K изоморфна полной матричной алгебре $M(m, D)$ над некоторым центральным телом D конечного ранга над K, причем тело D определено однозначно с точностью до изоморфизма. Легко проверить, что тензорное произведение центральных простых алгебр само является центральной простой алгеброй. В частности, если D_1, D_2 — два центральных тела конечного ранга над K, то их тензорное произведение $D_1 \otimes D_2$ имеет вид $M(m, D)$ для некоторого центрального тела D конечного ранга. Тело D определено однозначно с точностью до изоморфизма и называется **произведением Брауэра** тел D_1 и D_2. Легко видеть, что это произведение превращает множество классов изоморфизма центральных тел конечного ранга над K в группу, называемую **группой Брауэра** поля K и обозначаемую $\mathrm{Br}(K)$. В самом деле, корректность определения вытекает из теоремы Веддербарна, тензорное произведение ассоциативно с точностью до изоморфизма, единицей группы Брауэра является класс самого поля K, а классом обратным к классу тела D является класс противоположного тела D^o.

Группа Брауэра является важнейшим арифметическим инвариантом поля K. Например, так как поле $\mathbb{C}$ алгебраически замкнуто, то $\mathrm{Br}(\mathbb{C}) = 1$. **Теорема Фробениуса** о гиперкомплексных системах может быть сформулирована следующим образом: $\mathrm{Br}(\mathbb{R}) = C_2$, причем нетривиальный элемент этой группы задается телом кватернионов $\mathbb{H}$. **Малая теорема Веддербарна** о коммутативности конечных тел утверждает в точности, что $\mathrm{Br}(\mathbb{F}_q) = 1$. Утверждение, что если

Рихард Дагоберт Брауэр (Richard Dagobert Brauer, 10 февраля 1901, Шарлоттенбург, сегодня район Берлина — 17 апреля 1977, Белмонт, Массачусеттс, США) — гениальный немецкий алгебраист, создатель теории модулярных представлений конечных групп. В 1919 году он поступил в Берлинский университет, где его учителями были Бибербах, Эйнштейн и Шур. В 1921 году он вместе со старшим братом Альфредом решил одну из проблем Шура, и это окончательно определило его выбор в пользу алгебры (интересно, что в ту же неделю эту проблему Шура независимо решил Хайнц Хопф!). После защиты диссертации в 1926 году Брауэр получил позицию в Кенигсберге, где он выполнил свои знаменитые работы по теории алгебр — именно в этих работах введена группа, названная впоследствии группой Брауэра. Однако весной 1933 года из-за еврейского происхождения Брауэр был отстранен от преподавания. Он тут же занялся поисками позиции за границей и уже весной 1934 года вывез свою семью в США (его брат Альфред смог бежать из Германии в 1939 году, но их сестра Алиса погибла в концентрационном лагере). Вскоре он стал ассистентом Германа Вейля в ИАС в Принстоне. В 1935 году они написали знаменитую работу по теории спиноров, которая послужила основой релятивистской квантовой теории Дирака. Позже Вейль вспоминал, что совместная работа с Брауэром была самым удачным примером научного сотрудничества в его жизни. В 1935 году Брауэр получил постоянную позицию в университете Торонто. Именно там он создал свою знаменитую теорию модулярных представлений (теория модулярных характеров, теория блоков, и т. д.) В 1952 году Брауэр стал профессором в Гарварде, где оставался до конца жизни. В это время он получил несколько великих результатов по теории конечных групп и сформулировал первую реальную программу классификации конечных простых групп. Большое впечатление производит чтение списка выполненных под руководством Брауэра диссертаций. Среди его прямых учеников Несбитт, Роберт Стейнберг, Фаулер, Уолтер Файт, Джон Уолтер, Поль Фонг, Мортон Харрис, Мартин Айзекс, Леонард, Линдси, Пассман, Луи Соломон, Девид Уэйлс, Уоррен Уонг и другие замечательные специалисты по теории представлений. Оба сына Брауэра, Джордж Ульрих Брауэр и Фред Гюнтер Брауэр тоже стали профессиональными математиками.

Рихарда Брауэра не следует путать с его старшим братом **Альфредом Теодором Брауэром** (Alfred Theodore Brauer 9 апреля 1894, Берлин — 1985), тоже весьма известным математиком и тоже учеником Шура, его основные работы относятся к теории чисел и теории матриц. Будучи старше, чем Рихард, Альфред все четыре года Первой мировой войны служил в армии и был очень серьезно ранен, именно поэтому в 1933 году ему позволили еще какое-то время остаться на преподавательской работе. В 1938 году американское консульство в Берлине отказывалось выдать Альфреду Брауэру профессорскую визу, так как эта виза полагалась только тем, кто имел академическую позицию последние два года, в то время как он был уволен с такой позиции осенью 1935 года!!! Тем не менее в 1939 году он смог наконец получить разрешение на въезд в США и тоже стал ассистентом Германа Вейля в ИАС!

Тем более не следует путать Рихарда Брауэра со специалистом по интуиционистским инсинуациям **Люйтценом Брауэром** (Luitzen Brouwer), который ему не только не брат, но даже и не однофамилец.

Джозеф Генри Маклаген Веддербарн (Joseph Henry Maclagen Wedderburn, 2 февраля 1882, Форфар, Ангус, Шотландия — 9 октября 1948, Принстон) — знаменитый шотландский математик, один из классиков алгебры, с именем которого связано много замечательных результатов теории колец, теории алгебр и теории матриц. В 1895–1903 годах он учился в колледже, а потом Университете Эдинбурга, где выполнил свои первые самостоятельные работы, относившиеся к теории дифференциальных уравнений. После этого в 1903–1904 годах он продолжил обучение в Германии, Лейпциге и Берлине, где попал под влияние Фробениуса и Шура. В 1904 году получив стипендию для поездки в США, он поехал в Чикаго, где начал сотрудничество с Веблеином, Муром и Диксоном, которые в то время интересовались конечными телами и геометриями. В 1905 году Веддербарн вернулся в Эдинбург. В том же году он нашел то, что *он считал* доказательством **малой теоремы Веддербарна** о коммутативности конечных тел. В действительности, одновременно тот же результат получил Диксон, который *тоже* считал первое доказательство Веддербарна правильным, и поэтому признал приоритет Веддербарна. Ознакомившись с доказательством Диксона, Веддербарн предложил еще два правильных доказательства. В 1907 году Веддербарн опубликовал свою знаменитую работу по теории полупростых алгебр, в которой доказано то, что теперь известно как большая теорема Веддербарна, которая потом выросла в теорему Веддербарна—Артина. В 1909 году он принял временную позицию в Принстоне, а в 1914 году ушел добровольцем в Британскую армию, где служил до самого конца войны. В 1920 году он возвращается в Принстон, где вскоре получает постоянную позицию *доцента*. Веддербарн никогда не был женат и после того, как он ушел на пенсию в 1945 году, жил совершенно один. Объявление 9 октября 1948 года днем его смерти достаточно условно, так как это тот день, когда садовник нашел его труп; вероятно смерть наступила за несколько дней до этого. Архив Веддербарна оказался выморочным имуществом и был уничтожен!!! Среди учеников Веддербарна в Принстоне было несколько замечательных алгебраистов, в том числе Натан Джекобсон.

поле K алгебраически замкнуто, то $\mathrm{Br}(K(t)) = 1$ известно как **теорема Тзена** [93]. Доказательство того, что для поля p-адических чисел $\mathbb{Q}_p$ имеет место изоморфизм $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, является одним из центральных результатов **локальной теории полей классов** [94]. Вычисление $\mathrm{Br}(\mathbb{Q})$ является уже достаточно нетривиальной задачей и составляет важную часть современного подхода к описанию абелевых расширений поля $\mathbb{Q}$ известного как **глобальная теория полей классов** [95]. Это вычисление теснейшим образом связано со следующими двумя ключевыми результатами, каждый из которых весьма небанален, а именно **теоремой Алберта—Брауэра—Хассе—Нетер** и **законом взаимности Артина**.

2. Группа Пикара. Пусть R — коммутативное кольцо. В этом и следующем примерах мы рассматриваем конечно-порожденные модули над R. Напомним, что модуль изоморфный модулю столбцов R^n называется **свободным**. Прямые слагаемые свободных модулей называются проективыми модулями. Иными словами, модуль P в том и только том случае **проективен**, когда существует такой модуль Q, что $P \oplus Q \cong R^n$. Проективный модуль P называется **обратимым**, если

Абрахам Алберт (Abraham Adrian Albert 9 ноября 1905, Чикаго — 6 июня 1972, там же) — замечательный алгебраист, один из классиков теории ассоциативных и неассоциативных колец. Его родители, Илья Альберт и Фанни Фрадкина были русскими, но сам он родился уже в Чикаго, где и провел почти всю свою жизнь. Его руководителем в университете Чикаго был Леонард Диксон. Основные ранние работы Алберта посвящены теории тел (**алгебр с делением**). В 1939 году он опубликовал классическую книгу Structure of Algebras. В 1930-е годы под влиянием Германа Вейля он заинтересовался алгебрами Ли и йордановыми алгебрами, для которых он тоже получил основополагающие результаты.

Хельмут Хассе (Helmut Hasse, 25 августа 1898, Кассель — 26 декабря 1979, Аренсбург) — замечательный немецкий алгебраист и теоретико-числовик. Во время первой мировой войны он пошел добровольцем во флот и, пока его часть стояла в Киле, слушал там лекции Отто Теплица. После этого его учителями в Геттингене были Ландау, Гильберт, Эмми Нетер и Гекке. В 1920 году он уехал в Марбург, где работал под руководством Гензеля. В октябре 1920 года он открыл прославивший его локально-глобальный принцип (принцип Хассе, принцип Минковского—Хассе). В 1922 году он переехал в Киль, чтобы работать со своими гамбургскими коллегами Артином, Шрайером и Гекке. В 1925 году он стал профессором в Халле, откуда в 1930 году снова вернулся в Марбург, где он стал преемником Гензеля и написал свою знаменитую совместную с Брауэром и Эмми Нетер статью, ставшую одной из основ современной глобальной теории полей классов, и блистательную работу по аналогу гипотезы Римана для эллиптических кривых. В 1934 после отставки Германа Вейля он стал его преемником в Геттингене и вскоре возглавил математический институт. Положение Хассе во время нацизма было двояким, с одной стороны, он с глубочайшим пиететом относился к своему учителю Гензелю, который согласно расовым законам был Volljude (как, кстати, соавторы Хассе по нескольким работам Брауэр и Нетер!). С другой стороны, Хассе не скрывал своих *крайне* националистических взглядов и с 1939 по 1945 год вернулся к службе во флоте, где он занимался вопросами баллистики, и даже подал заявление о приеме в НСДАП (но не был принят, как Achteljude!). В результате в 1945 году британские оккупационные власти отрешили его от всех постов и единственное место, где он мог преподавать, был Восточный Берлин! Только в 1950 году ему было разрешено снова преподавать в Гамбурге. Он доказал несколько центральных результатов, относящихся к теории квадратичных форм, таких как теоремы Минковского—Хассе, Хассе—Витта, Хассе—Артина и т. д. В нашем курсе встречаются диаграммы Хассе. На русский переведен его классический учебник по теории чисел. Среди других заслуг Хассе перед математическим сообществом следует отметить, что в течение 50 лет (!!) он был редактором *Journal für die reine und angewandte Mathematik*.

найдется такой проективный модуль Q, что $P \otimes Q \cong R$. Легко проверить, что проективный модуль в том и только том случае обратим, когда его **ранг равен 1**, т. е. при любом гомоморфизме R в поле K, модуль P переходит в одномерное векторное пространство над K, иными словами, $P \otimes_R K \cong K$. В этом случае мож-

Эмми Нетер (Emmy Noether, 23 марта 1882, Эрланген — 14 апреля 1935, Брин Мор) — гениальный немецкий математик, один из основателей (основательниц?) современной алгебры, оказавшая огромное влияние на развитие математики в XX веке. Дочь Макса Нетера и ученица Гильберта она, вероятно, самая замечательная женщина во всей истории математики. Ее главной заслугой является эксплицирование и систематизация алгебраических понятий, возникших в конце XIX века и начале XX века в работах Кронекера, Дедекинда, Вебера, Гильберта, Штейница, Фробениуса и других. В долговременном плане это изменило сам язык и стиль алгебры — и всей математики. Там, где до Нетер говорили о **числах** Бетти, теперь говорят о **группах** гомологий; там, где говорили о **матрицах**, теперь говорят о **модулях** и т. д. Переход на инвариантную структурную точку зрения можно приветствовать, можно с ним полемизировать, как это делает Арнольд, но то, что Нетер сыграла в этом процессе такую же роль, как Гильберт или Бурбаки, не подлежит сомнению. В более конкретном плане ей принадлежат замечательные результаты в теории коммутативных колец (примарные разложения, теоремы Ласкера—Нетер, и т. д.), которые позволили алгебраизовать и поставить на твердую основу алгебраическую геометрию. Среди ее учеников и коллег, входивших в ее непосредственное окружение и находившихся под ее огромным влиянием, — **мальчиков**, как их называли в Геттингене, — Эмиль Артин, Бартельс ван дер Варден, Эрнст Витт, Вольфганг Крулль и многие другие классики алгебры XX века, которые уважительно называли ее der Noether. Нетер принадлежат также ключевые соображения по применению алгебры к физике (теорема Нетер о законах сохранения). В качестве темы для размышления о справедливости жизни можно вспомнить, что Нетер никогда не имела академической позиции, соответствующей ее квалификации. То, что она была выдающимся математиком, да к тому же женщиной, да к тому же еврейкой, да к тому же состояла в социал-демократической партии, вряд ли прибавляло ей популярности среди немецких коллег. Когда зашла речь о ее хабилитации в Геттингене, один из коллег возразил, что Fräulein Нетер никак нельзя присуждать хабилитацию, потому что тогда она сможет стать **экстраординарным**, а *со временем* даже **ординарным** профессором и *войти* в сенат (**Der Senat eintreten**). Комментарий Гильберта стал знаменит: “Meine Herren! Der Senat ist keine Badeanstalt!” — “Господа! Сенат это не мужская баня!”. В результате Fräulein Нетер все же стала первой женщиной в истории, получившей хабилитацию в немецком университете, и могла читать лекции под своим именем, но все еще без оплаты! Только в 1923 году, в возрасте 41 года она получила от университета первую зарплату. Однако 25 апреля 1933 года ее **послали в отпуск**, или, говоря по-русски, уволили. В отличие от многих коллег она сразу поняла, что к чему, и тут же уехала в Америку, вернувшись в Германию в 1934 году только чтобы отказаться от аренды квартиры и упаковать свои вещи. Еще поразительнее, что и в Америке она не получила регулярной профессорской **позиции** и преподавала в женском колледже в Брин Мор — ставшем благодаря ей знаменитым! В нашем курсе встречаются нетеровы кольца и модули, несколько десятков(!!) общих теорем о группах, кольцах и других алгебраических системах, которые стали настолько привычными, что обычно цитируются без ее имени: например, теоремы Нетер о гомоморфизме и изоморфизме обычно называются просто теоремами о гомоморфизме и изоморфизме, и т. д. Эмми Нетер умерла в результате осложнений после операции по удалению опухоли мозга.

Отцом Эмми Нетер был замечательный алгебраический геометр **Макс Нетер** (Max Noether, 24 сентября 1844, Маннхейм — 13 декабря 1921, Эрлангген). Макс Нетер учился в Гейдельберге, Гиссене и Геттингене, с 1871 года работал в Геттингене, а с 1875 года — в Эрлангене, где в 1888 году стал профессором. Нетер внес глубокий вклад в теорию алгебраических функций, теорию исключения, теорию форм и т. д.

Приведем небольшой штрих, показывающий, насколько велик престиж Эмми Нетер в математическом бессознательном: многие результаты Макса Нетера (такие, как лемма Нетера о нормализации) рутинно приписывают его дочери. Младший брат Эмми, **Фритц Нетер** тоже стал известным математиком, профессором в Бреслау. Фритц придерживался левых убеждений и с приходом к власти нацистов решил эмигрировать в СССР. Судьба есть реализация характера, и Фритц погиб в концентрационном лагере, хотя и не в немецком.

но положить $Q = P^* = \mathrm{Hom}(P, R)$. Множество классов изоморфизма обратимых R-модулей относительно тензорного произведения обозначается $\mathrm{Pic}(R)$ и называется **группой Пикара** кольца R. Иными словами, произведение P и Q в группе Пикара равно $P \otimes Q$, единицей является класс модуля R, а $P^{-1} = P^*$.

3. Группа Гротендика. Пусть, по-прежнему, R – коммутативное кольцо. Основой линейной алгебры над полем являются следующие два утверждения: 1) каждый модуль свободен, 2) ранг свободного модуля (называемый в этом случае размерностью) определен однозначно. В общем случае обобщение первого из этих утверждений на все R-модули абсолютно бесперспективно, так как теперь уже совершенно не очевидно, что подмодули (и даже прямые слагаемые) свободных модулей свободны. С другой стороны, для модулей *бесконечного* ранга второе утверждение справедливо в силу очевидных теоретико-множественных соображений — the infinite we'll do right away, the finite may take a little bit longer. Сейчас мы введем группу, которая измеряет отклонение от стандартных ответов в случае конечно порожденных *проективных* модулей.

Для этого рассмотрим множество X *классов изоморфизма* конечно порожденных проективных модулей над кольцом R. По отношению к операции прямой суммы $(P, Q) \mapsto P \oplus Q$ это множество образует моноид, нейтральным элементом которого является класс 0. В книге I мы связали с каждым коммутативным моноидом некоторую группу, называемую его группой Гротендика. Группа Гротендика моноида X обозначается $K_0(R)$ и называется **группой Гротендика** кольца R. Опишем группу $K_0(R)$ подробнее. Каждому классу P изоморфизма конечно порожденных проективных R-модулей отвечает элемент $[P]$ группы $K_0(R)$, причем $X \longrightarrow K_0(R)$, $P \mapsto [X]$, является гомоморфизмом моноидов, т. е. $[P]+[Q] = [P \oplus Q]$. При этом каждый элемент $K_0(R)$ представляется в виде $[P] - [Q]$. Напомним, что проективные модули P и Q называются **стабильно изоморфными**, если существует такой свободный модуль R^n, что $P \oplus R^n \cong Q \oplus R^n$. Можно доказать, что элементы $[M] - [N]$ и $[P] - [Q]$ в том и только том случае совпадают в группе $K_0(R)$, когда модули $M \oplus Q$ и $N \oplus P$ стабильно изоморфны (см., например, **[136]**, лемма 1.1).

Группа $K_0(R)$ отражает, насколько линейная алгебра в классе проективных модулей над кольцом R близка линейной алгебре над полем. Например, если R поле, кольцо главных идеалов или локальное кольцо, то $K_0(R) \cong \mathbb{Z}$.

Эмиль Артин (Emil Artin, 3 марта 1898, Вена — 20 декабря 1962, Гамбург) — гениальный австрийский математик, внесший фундаментальный вклад в развитие алгебры, топологии и теории чисел. В 1916 году он поступил в Университет Вены, но после одного семестра был призван в армию, где служил до конца войны. В 1919 году Артин продолжил обучение в Лейпцигском университете и уже в 1921 году защитил диссертацию в области алгебраической теории чисел под руководством Густава Герглотца. В 1925 году Артин стал профессором в Гамбурге.

Рихард Брауэр в своей статье об Артине [96] пишет, что в истории математики найдется немного примеров, когда математик работал бы с той же интенсивностью и размахом, как Артин в 1921–1931 годах. Андре Вейль вспоминает, что в те годы в каждом номере трудов математического семинара Гамбургского математического института появлялись блестящие работы Артина, на самые разнообразные темы. В нашем курсе упоминаются артиновы кольца и модули, группа кос, теорема Артина об альтернативных кольцах и многие другие принадлежащие ему результаты. Самые глубокие результаты Артина относятся к теории алгебр и алгебраической теории чисел, в первую очередь к теории полей классов: закон взаимности Артина, ζ-функции Артина и т. д. Несколько совершенно замечательных работ написаны Артином совместно с Отто Шрайером: расширения Артина—Шрайера, теория Артина—Шрайера формально вещественных полей и т. д.

Сам Артин был арийцем, но его жена Наташа подпадала под действие расовых законов. Хельмут Хассе (который сам имел еврейских предков, но был лоялен режиму), предлагал Артину переехать в Геттинген, обещая, что его дети будут официально провозглашены арийцами. Тем не менее, в 1937 году Артин эмигрировал в США, где работал в университете штата Индиана и в Принстоне. Написанные им книги по теории Галуа и (совместно с его американским учеником Джоном Тейтом) теории полей классов стали каноническими источниками, на которых основаны все последующие изложения.

Сотрудничество Артина и Тейта является еще одним блестящим подтверждением теории о том, что математические способности передаются от тестя к зятю, так как после женитьбы на дочке Артина **Джон Тейт** тоже стал совершенно гениальным математиком. Впрочем в данном конкретном случае *в порядке исключения* математические способности передались и *от отца к сыну*, так как сын Эмиля Артина **Майкл Артин** тоже стал замечательным алгебраистом и алгебраическим геометром.

Трудно описать впечатление, которое производят работы Артина, точнее, чем это сделал Анри Картан: Emil Artin fut un mathematicien genial. C'etait aussi un artiste et, pour tout dire, un homme complet [97]. А вот еще две мемориальные статьи, написанные людьми, близко знавшими Артина [98], [99]. Артин интересовался многими вещами, кроме математики, виртуозно играл на флейте и клавесине, мастерил телескопы и т. д. Прямыми учениками Артина были Макс Цорн, Ганс Цассенхауз, Джон Тейт, Серж Ленг, О. Т. О'Мира, Бернард Дворк и многие другие выдающиеся алгебраисты и теоретико-числовики. На русский язык переведена блистательная книга Артина *Геометрическая алгебра*.

4. Группа классов идеалов. Напомним, что если $A, B \trianglelefteq R$ — два идеала коль-

Шарль Эмиль Пикар (24 июля 1856, Париж — 11 декабря 1941, Париж) — замечательный французский математик, основные работы которого относятся к теории функций комплексного переменного, алгебраической геометрии и теории дифференциальных уравнений. В школе Пикар ненавидел геометрию, но однажды на каникулах ему случайно попалась книга по алгебре, и он неожиданно увлекся математикой и сдал экзамены в École Politechnique и École Normale — соответственно вторым и первым среди всех поступавших! После окончания Ecole Normale — первым в своем году!! — он короткое время преподавал в Тулузе, но вскоре вернулся в Париж. В 1881 году Пикар женился на дочери Эрмита — и тут же доказал свои знаменитые теоремы о распределении значений аналитических функций (здесь для большей наглядности *я слегка* подправляю историю в духе Фоменко: теорему о значениях целых функций Пикар доказал уже в 1879 году). В том же году в возрасте 25 лет он был выдвинут в Парижскую Академию (впрочем, избрали его туда только через 8 лет). Именно отсюда пошла поговорка о том, что МАТЕМАТИЧЕСКИЕ СПОСОБНОСТИ ПЕРЕДАЮТСЯ ОТ ТЕСТЯ К ЗЯТЮ!!!

Впрочем, это далеко не единственный подобный случай: семейство Адамар — Поль Леви — Лоран Шварц — У. Фриш является еще более поразительным примером того, как математические способности — и место в Парижской Академии — передавались от тестя к зятю *в течение четырех поколений*. Впрочем, не следует думать, что этот феномен ограничен Парижем и Парижской Академией наук. Аналогичное поразительное природное явление наблюдалось в Берлине и Прусской Академии наук: Герман Шварц был зятем Куммера. Впрочем, я слышал и более произаическое объяснение, состоящее в том, что все зятья имели *некоторые* математические способности еще до брака и женились на дочке научного руководителя, чтобы не отвлекаться от научной работы (`utile cum dulce = Schnaps mit Zucker`).

Бывают и случаи, когда математические способности *в порядке исключения* передаются от отца к сыну, так Лионс младший получил Филдсовскую медаль в бытность Лионса старшего Президентом Международного математического союза. Впрочем, Арнольд со свойственной ему наблюдательностью (которую люди ей не обладающие принимают за цинизм) утверждает, что последний случай иллюстрирует все же не передачу математических способностей, а общий беспрецедентный уровень коррупции, царящей ныне в европейской науке.

Исследования Пикара по аналитическим и топологическим аспектам теории алгебраических поверхностей сыграли огромную роль в развитии алгебраической геометрии. Теория Пикара—Вессио дифференциальных уравнений стала отправной точкой для развития дифференциальной алгебры и теории алгебраических групп. В нашем курсе термин `группа Пикара` встречается в двух различных смыслах. Кроме того, Пикар интересовался математическими аспектами теории упругости, теплопроводности и электромагнетизма. В 1891–1896 годах он опубликовал замечательный трехтомный *Traité d'analyse*. С 1917 по 1941 год Пикар был непременным секретарем Парижской Академии. Жизнь Пикара протекала в интересный период европейской истории: его отец погиб в 1870 году во время немецкой осады Парижа, все трое его детей погибли в Первую мировую войну, а внуки были ранены и попали в плен во время Второй мировой войны.

ца R, то их **произведением** называется идеал AB, порожденный как аддитивная подгруппа всевозможными произведениями вида ab, $a \in A$, $b \in B$. Область целостности R называется **дедекиндовым кольцом**, если для любых ненулевых идеалов $B \geq A$ существует единственный идеал C такой, что $A = BC$, см. [**136**], с. 19. Сейчас мы воспроизведем более привычное определение дедекиндовых колец, но для этого нам придется напомнить еще несколько определений. Пусть R — нетерова область целостности, K — ее поле частных. Ненулевой конечно порожденный R-подмодуль I в K называется **дробным идеалом** кольца R; в дальнейшем мы часто называем дробные идеалы кольца R просто идеалами. Легко видеть, что в этом случае $I^{-1} = \{x \in K \mid xI \leq R\}$ тоже является дробным идеалом. Дробный идеал называется **обратимым**, если $II^{-1} = R$. Так вот, дедекиндово кольцо это в точности нетерова область целостности, все дробные идеалы которой обратимы, [**5**], с. 19–21. Все дробные идеалы дедекиндова кольца R образуют группу относительно умножения. Говорят, что дробные идеалы A и B кольца R принадлежат одному и тому же **классу идеалов**, если $A = Bz$ для некоторого $z \in K^*$. Выразив $z = y/x$, это условие можно переписать в виде $xA = yB$ для некоторых $x, y \in R^\bullet = R \setminus \{0\}$. Легко видеть, что класс произведения AB двух дробных идеалов A, B зависит не от самих идеалов, а только от их классов. Таким образом, классы идеалов дедекиндова кольца R образуют группу, называемую **группой классов идеалов** и обозначаемую $\mathrm{Cl}(R)$. Единицей этой группы служит класс идеала R, состоящий из **главных идеалов**, а класс, обратный к классу идеала I — это класс идеала I^{-1}. Группа $\mathrm{Cl}(R)$ является важнейшим арифметическим инвариантом кольца R, показывающим, насколько R близко к кольцу главных идеалов. В частности, дедекиндово кольцо R в том и только том случае является кольцом главных идеалов, когда оно **одноклассное**, т. е. когда $\mathrm{Cl}(R) = 1$.

§ 17✠. Группы в топологии

В настоящем параграфе мы расскажем о том, как возникают группы в топологии.

1. Фундаментальная группа. Пусть $\mathbb{I} = [0, 1]$ — отрезок, а X — топологическое пространство. Непрерывное отображение $f : \mathbb{I} \longrightarrow X$ называется **путем** в X. При этом $x = f(0)$ называется **началом** пути, а $y = f(1)$ — его **концом**. Путь, для которого $x = f(1) = f(0)$, называется **замкнутым** путем или **петлей** в точке x. Рассмотрим два пути $f, g : \mathbb{I} \longrightarrow X$, начала и концы которых совпадают, т. е. $f(0) = g(0)$ и $f(1) = g(1)$. Эти пути называются **гомотопными**, если существует непрерывное отображение $h : \mathbb{I} \times \mathbb{I} \longrightarrow X$, такое, что $h(s, 0) = f(s)$ и $h(s, 1) = g(s)$ для всех $s \in \mathbb{I}$. Любое такое отображение h называется **гомотопией** между путями f и g. Мы будем рассматривать *только* гомотопии **с закрепленными концами**, для которых, кроме того, $h(0, s) = f(0) = g(0)$ и $h(1, s) = f(1) = g(1)$ для всех $t \in \mathbb{I}$. Иными словами, два пути гомотопны, если один из них можно непрерывно продеформировать в другой в пространстве X так, чтобы их начала и концы все время оставались неподвижными, в этом случае мы будем писать $f \sim g$. Ясно, что гомотопия является отношением эквивалентности на множестве путей с началом x и концом y. Классы этой эквивалентности называются **гомотопическими классами** путей с началом x и концом y. Мы обозначим гомотопический класс отображения f через $[f]$. Пусть теперь $f, g : \mathbb{I} \longrightarrow X$ — два пути такие, что начало второго из них совпадает с концом первого, $g(0) = f(1)$. **Произведение** путей f, g

определяется как

$$(f \cdot g)(t) = \begin{cases} f(2t), & 0 \le t \le 1/2, \\ g(2t-1), & 1/2 \le t \le 1. \end{cases}$$

Легко видеть, что произведение путей неассоциативно, т. е., вообще говоря, $(f \cdot g) \cdot h \neq f \cdot (g \cdot h)$. Однако это легко исправить. Дело в том, что гомотопия является конгруэнцией по отношению к произведению путей, если $f \sim f'$ и $g \sim g'$, то $f \cdot f' \sim g \cdot g'$. Таким образом, произведение путей *корректно* определяет произведение гомотопических классов путей, $[f][g]$. Так вот, *с точностью до гомотопии* произведение путей уже ассоциативно: $(f \cdot g) \cdot h \sim f \cdot (g \cdot h)$, при условии, что хотя бы одно из этих произведений определено. Таким образом, произведение гомотопических классов путей уже ассоциативно, $([f][g])[h] = [f]([g][h])$. Постоянные пути $e_x : \mathbb{I} \mapsto X$, $f(t) = x$ для всех t, являются левыми/правыми нейтральными элементами по отношению к умножению путей *с точностью до гомотопии*. Точнее, если f — путь с началом x и концом y, то $e_y \cdot f \sim f \sim f \cdot e_x$ или, иными словами, $[e_y][f] = [f] = [f][e_x]$. Для пути f с началом x и концом y определяется **обратный** путь f^{-1} с началом y и концом x. А именно, $f^{-1}(t) = f(1-t)$. Путь f^{-1} действительно *с точностью до гомотопии* является обратным к пути f, а именно, $f \cdot f^{-1} \sim e_x$ и $f^{-1} \cdot f \sim e_y$ или, что то же самое, $[f][f^{-1}] = [e_x]$ и $[f^{-1}][f] = [e_y]$.

Зафиксируем точку $x \in X$. Резюмируя сказанное выше, мы видим, что гомотопические классы петель в точке x образуют группу относительно произведения. Эта группа называется **фундаментальной группой** пространства X в точке x и обозначается $\pi_1(X, x)$. Фундаментальная группа ведет себя **функториально**, т. е. для любого непрерывного отображения $f : X \longrightarrow Y$ определяет гомоморфизм групп $\pi_1(f) : \pi_1(X, x) \longrightarrow \pi_1(Y, f(x))$. Если пространство X линейно связно (т. е. любые две его точки можно соединить путем), то *с точностью до изоморфизма* фундаментальная группа $\pi_1(X, x)$ не зависит от выбора точки x и называется просто фундаментальной группой пространства X. Эта группа является одним из важнейших инвариантов пространства X. С одной стороны, исторически это первое реальное приложение теории групп в топологии, открытое Анри Пуанкаре. С другой стороны, эта конструкция имеет замечательные приложения в самой теории групп. Дело в том, что фундаментальная группа, вообще говоря, весьма неабелева. Например, знаменитая **теорема ван Кампена** утверждает, что фундаментальная группа букетного произведения пространств является свободным произведением фундаментальных групп сомножителей. В частности, фундаментальная группа букета n окружностей — это свободная группа ранга n. Большинство результатов, относящихся к свободным группам, естественнее всего доказываются именно на этом языке.

2. Гомотопические группы. В 1930-х годах В.Гуревич предложил следующее многомерное обобщение понятия фундаментальной группы. Так как получающиеся при этом группы $\pi_n(X)$, $n \ge 2$, абелевы, то первоначально многие топологи считали, что это неправильное обобщение, которое не содержит ничего нового по сравнению с понятием групп гомологий, но, как мы теперь знаем, они заблуждались.

Пусть, по-прежнему, X — топологическое пространство, а $x \in X$ — точка. Для любого $n \ge 2$ определение гомотопической группы $\pi_n(X, x)$ совершенно аналогично определению фундаментальной группы $\pi_1(X, x)$. Единственная разница состоит в том, что единичный отрезок $\mathbb{I} = \mathbb{I}^1$ заменяется n-мерным единичным кубом $\mathbb{I}^n$.

Эгберт Рудольф ван Кампен (Egbert Rudolf van Kampen, 28 мая 1908, Берхем — 11 февраля 1942, Балтимор) — замечательный голландский математик, основные работы которого относятся к алгебраической топологии и топологической алгебре. Тот факт, что ван Кампен родился в Бельгии, не может изменить того, что он голландский математик, если бы он считал себя бельгийским математиком, мы бы знали его как Ван Кампена!! В 1924 году он поступил в Лейденский университет, а в 1927 поехал продолжать образование в Геттинген, где познакомился с ван дер Варденом и Александровым и Гамбург, где работал под руководством Артина. После защиты диссертации он еще несколько лет работает как ассистент Схоутена в Дельфте, но в 1931 году принимает решение эмигрировать в США и начинает преподавать в университете Джона Хопкинса в Балтиморе. Зариский, который в это время занимается алгебраическими кривыми, предлагает ему задачу о фундаментальной группе дополнения к кривой — именно отсюда возникает знаменитая теорема ван Кампена. Остальные работы ван Кампена относятся к теории топологических групп, анализу, теории дифференциальных уравнений, аналитической теории чисел и математической статистике. Всего за свою короткую жизнь — 12 лет исследовательской работы — Ван Кампен публикует 54 статьи! В 33 года ван Кампен умирает в результате осложнений после операции по удалению опухоли.

Витольд Гуревич (Witold Hurewicz, 29 июня 1904, Лодзь — 06 сентября 1956, Уксмаль, Мексика) — замечательный польский тополог. Он учился в Вене под руководством Ганса Хана и Карла Менгера и получил **докторат** в 1926 году. Его ранние работы относятся к области теоретико-множественной топологии. В 1927–1936 годах Гуревич был ассистентом Брауэра в Амстердаме. Именно там он выполнил свои самые знаменитые работы по теории размерности и определил высшие группы гомотопий. В 1937 году он на год поехал в Принстон, но решил не возвращаться в Европу ввиду ухудшавшейся обстановки. Во время Второй мировой войны он занимался оборонными исследованиями в области прикладной математики, а начиная с 1945 года работал в MIT. Гуревич погиб во время международной топологической конференции в Мексике упав с пирамиды.

Обозначим через $d\mathbb{I}^n$ границу куба, состоящую из всех точек $t = (t_1, \dots, t_n) \in \mathbb{I}^n$, для которых какая-то из координат t_i равна 0 или 1. Рассмотрим всевозможные непрерывные отображения $f : \mathbb{I}^n \longrightarrow X$ такие, что $f(d\mathbb{I}^n) = x$. Как и выше, мы можем определить произведение таких отображений, полагая

$$(f \cdot g)(t_1, \dots, t_n) = \begin{cases} f(2t_1, t_2, \dots, t_n), & 0 \le t_1 \le 1/2, \\ g(2t_1 - 1, t_2, \dots, t_n), & 1/2 \le t_1 \le 1. \end{cases}$$

Как и выше, мы можем рассмотреть гомотопии таких отображений с закрепленной границей, пусть $\pi_n(X, x)$ — множество получающихся гомотопических классов. Легко проверить, что гомотопия является конгруэнцией относительно так определенного произведения отображений, что позволяет корректно определить произведение в $\pi_n(X, x)$. Как и выше, моментально проверяется, что это произведение ассоциативно с точностью до гомотопии, так что $([f][g])[h] = [f]([g][h])$, имеет нейтральный элемент, а именно, класс постоянного отображения $e = e_x : \mathbb{I}^n \longrightarrow X$,

$f(t) = x$ для всех $t \in \mathbb{I}^n$ и, наконец, для любого $[f] \in \pi_n(X, x)$ существует обратный элемент, а именно, класс отображения $f^{-1} : \mathbb{I}^n :\longrightarrow X$, $t \mapsto f(1 - t_1, t_2, \ldots, t_n)$. Таким образом, $\pi_n(X, x)$ образует группу, которая называется **n-й гомотопической группой** пространства X в точке x. Замечательное отличие случая $n \geq 2$ от случая $n = 1$ состоит в том, что все группы $\pi_n(X, x)$, $n \geq 2$, абелевы. Гомотопические группы топологических пространств являются одним из самых важных и интересных объектов в математике и имеют совершенно замечательные приложения в самой алгебре. Не будет большим преувеличением сказать, что большая часть ключевых идей, возникших в алгебре за последние 50 лет, пришла именно из гомотопической топологии.

3. Группы гомологий и когомологий. Мы не будем пытаться обсуждать как определяются группы гомологий и когомологий в алгебраической топологии. Имеются десятки различных теорий гомологий и когомологий, которые дают один и тот же ответ для классических объектов (таких как полиэдры или компактные многообразия), но, вообще говоря, не совпадают в более широких классах пространств. Детальному изложению этих конструкций посвящены целые книги. Поэтому опишем, в чем состоит основная задумка того, что делается в этих книгах, а не то, как конкретно это делается. В простейшем варианте с каждым топологическим пространством X и абелевой группой A связываются **группы гомологий** $H_n(X, A)$ и двойственные к ним **группы когомологий** $H^n(X, A)$ пространства X с коэффициентами в группе A. При этом группы гомологий ведут себя ковариантно по отношению к непрерывным отображениям топологических пространств, а группы когомологий — контравариантно. Иными словами, любому непрерывному отображению $f : X \longrightarrow Y$ топологических пространств сопоставляются гомоморфизмы

$$H_n(f) : H_n(X, A) \longrightarrow H_n(Y, A), \qquad H^n(f) : H^n(Y, A) \longrightarrow H^n(X, A)$$

абелевых групп.

Классически рассматривались группы гомологий и когомологий с целыми коэффициентами, которые обозначаются просто через $H_n(X)$ и $H^n(X)$. В самом первом приближении эти группы при $n \geq 1$ измеряют наличие n-мерных дырок в пространстве X. Например, в n-мерном шаре $\mathbb{B}^n$ не заметно вообще никаких дырок, так что $H_i(\mathbb{B}^n) = 0$ для всех $i \geq 1$. С другой стороны, для n-мерной сферы $X = \mathbb{S}^n$ имеем $H_0(\mathbb{S}^n) \cong H_n(\mathbb{S}^n) \cong \mathbb{Z}$, в то время как $H_i(\mathbb{S}^n) = 0$ для всех $i \neq 0, n$.

Вот эффектное приложение функториальности групп гомологий, с которого начинается каждый курс алгебраической топологии. Классическая **теорема Брауэра** о неподвижной точке утверждает, что каждое непрерывное отображение $f : \mathbb{B}^n \longrightarrow \mathbb{B}^n$ шара в себя имеет хотя бы одну неподвижную точку. В самом деле, предположим, что это не так, и что для каждого $x \in \mathbb{B}^n$ имеем $f(x) \neq x$. Тогда проводя луч из $f(x)$ через x до его точки пересечения $g(x)$ с $(n-1)$-мерной сферой $\mathbb{S}^{n-1}$ (являющейся границей шара $\mathbb{B}^n$), мы получили бы непрерывное отображение $\mathbb{B}^n \longrightarrow \mathbb{S}^{n-1}$ постоянное на $\mathbb{S}^{n-1}$. Но это невозможно, потому что тогда композиция $g\circ\hookrightarrow : \mathbb{S}^{n-1} \hookrightarrow \mathbb{B}^n \longrightarrow \mathbb{S}^{n-1}$ была бы тождественным отображением. Переходя к гомологиям получаем $\mathrm{id} : H_{n-1}(\mathbb{S}^{n-1}) \longrightarrow H_{n-1}(\mathbb{B}^n) \longrightarrow H_{n-1}(\mathbb{S}^{n-1})$. Иными словами, тогда тождественное отображение $\mathbb{Z}$ на себя пропускается через 0, что абсурдно.

С другой стороны, с точки зрения алгебры гораздо интереснее рассматривать не когомологии с постоянными коэффициентами, а их обобщения с коэффициентами

Люйтцен Эгбертус Ян Брауэр (Luitzen Egbertus Jan Brouwer, 27 февраля 1881, Оверсхи — 2 декабря 1966, Амстердам) — знаменитый голландский математик, логик и философ, в 1912–1951 годах профессор Амстердамского университета. В 1911–1913 годах Брауэр выполнил несколько очень важных работ по топологии, в которых он ввел понятия степени непрерывного отображения, гомотопической классификации, симплициальной аппроксимации, доказал теорему о неподвижной точке, теоремы о размерности и ряд других важных результатов, которые оказали большое влияние на развитие общей и алгебраической топологии. После этого Брауэр занимался в основном математической логикой и основаниями математики, где он был зачинщиком **интуиционизма**, состоящего в *отбрасывании* (rejection) классической математики. Ядром его философии была критика "неконструктивных" рассуждений, принципа исключенного третьего и т. д. В дальнейшем более образованная и интеллектуально развитая часть интуиционистов вернулась в лоно настоящей математики, а другая часть окончательно превратилась в клоунов, строчащих безграмотные пасквили на тему *Математика, утрата определенности* и пр. Разнузданная пропаганда Брауэром интуиционизма, деструктивная по отношению к математике позиция и фило-нацизм неминуемо привели его к конфликту со школой Гильберта, известному в математической литературе как **батрахомиомахия** или Froschmäusekrieg [100]. Эта война закончилась оргвыводами в отношении Брауэра, изгнанием его из редакции Mathematische Annalen и пр.

в локальных системах абелевых групп, наиболее важными из которых являются пучки (когомологии Чеха, когомологии Гротендика, etc.). Вообще, по крайней мере на поверхностный взгляд представляется, что когомологии являются более мощным и удобным инструментом, чем гомологии. Во-первых, они теснее связаны с классическим анализом, и — в случае многообразий — допускают прозрачную характеризацию в терминах дифференциальных форм. Во-вторых, они в меньшей степени подвержены случайностям своего происхождения. Наконец, в-третьих, в когомологиях естественно определяется произведение, которое превращает

$$H^*(X, A) = \bigoplus_{n \geq 0} H^n(X, A)$$

в кольцо, называемое кольцом когомологий. Это кольцо представляет собой более тонкий инвариант пространства X, чем группы гомологий или когомологий.

§ 18✠. Группы с дополнительными структурами, 1st installment: топологические группы

В геометрии, топологии и дисциплинах аналитического цикла группы всегда возникают не как абстрактные, а как *топологические* группы. В подавляющем большинстве случаев рассматриваемые там подгруппы замкнуты, гомоморфизмы и действия непрерывны, и т. д.

1. Топологические группы. Следующее понятие было впервые введено в 1925 году Отто Шрайером [101]. В приведенном здесь виде условие согласованности

Отто Шрайер (Otto Schreier, 03 марта 1901, Вена — 02 июня 1929, Гамбург) — гениальный австрийский алгебраист. В 1920 году Шрайер поступил в Венский университет, где он учился у Виртингера, Фуртвенглера, Хана, Райдемайстера и Вьеториса. В 1923 под руководством Фуртвенглера он защитил диссертацию на тему *Über die Erweiterungen von Gruppen*, где, собственно и ввел многие из основных конструкций, которые мы обсуждаем в главе 8! Сразу после этого Шрайер уехал в Гамбург для сотрудничества с Артином, и где он работал до своей безвременной смерти. В 1926 году он получил **хабилитацию** за свою работу *Die Untergruppen der freien Gruppe*. Кроме топологических групп он определил многие ключевые понятия теории групп и теории полей, включая расширения групп, свободные и амальгамированные произведения. В нашем курсе упоминаются *десятки* его теорем и восходящих к нему понятий: Verfeinerungssatz, теорема Нильсена—Шрайера, формула Шрайера, теорема Шрайера—ван дер Вардена, метод Райдемайстера—Шрайера, расширения Артина—Шрайера, теория Артина—Шрайера формально вещественных полей, шрайеровские трансверсали, шрайеровские системы образующих и т. д. В прискорбно юном возрасте 28 лет Отто Шрайер умер от **общего заражения крови**. Если бы антибиотики были открыты за несколько лет до того, как они фактически были открыты, это радикально изменило бы дальнейшее развитие алгебры, а может быть и математики в целом. На русский язык переведены его совместные с Эммануэлем Шпернером книги *Теория матриц* и *Введение в линейную алгебру в геометрическом изложении*.

групповой и топологической структуры было сформулировано польским математиком Франтишком Лейа [102].

Начиная с 1930-х годов это понятие систематически изучалось многими ведущими математиками, в том числе Германом Вейлем, Давидом ван Данцигом, Альфредом Хааром, Джоном фон Нейманом, Андре Вейлем Львом Семеновичем Понтрягиным и многими другими.

Давид ван Данциг (David van Dantzig, 23 сентября 1900, Роттердам — 22 июля 1959, Амстердам) — замечательный голландский математик, основные работы которого относятся к топологической алгебре, дифференциальной геометрии, математической физике и теории вероятностей. После окончания Университета Амстердама в 1927 году он становится ассистентом Схоутена в Дельфте и в 1931 году получает докторат за диссертацию под названием 'Штудии по топологической алгебре' — именно ван Данциг впервые употребил выражение **топологическая алгебра**. В 1938 году он становится профессором в Дельфте, но когда весной 1940 года германские войска оккупировали Нидерданды, он был отстранен от должности и вынужден был переехать в Амстердам. После войны ван Данциг становится профессором Университета Амстердама, где он работал до своей кончины.

Определение. Топологической группой *называется множество, которое несет две согласованные структуры, группы и топологического пространства.* **Согласованность** *означает, что*

Альфред Хаар (Alfred Haar, 11 ноября 1885, Будапешт — 16 марта 1933, Сегед) — замечательный венгерский математик, основные работы которого относятся к анализу, теории уравнений в частных производных и вариационному исчислению. С 1904 по 1909 год Хаар учился в Геттингене под руководством Гильберта и в 1909 году получил степень за диссертацию по теории ортогональных систем функций. Сегодня Хаар известен главным образом благодаря своим результатам о мере Хаара, которые легли в основу построенного Германом Вейлем, Джоном фон Нейманом, Понтрягиным и Андре Вейлем абстрактного гармонического анализа.

Джон (aka Янош aka Иоганн) фон Нейман (John von Neumann, 28 декабря 1903, Будапешт — 08 февраля 1957, Вашингтон) — один из самых блестящих, разносторонних и влиятельных математиков XX века, автор почти 200 статей и 10 книг по различным вопросам математики и ее приложений. С 1927 года преподавал в Берлине и Гамбурге, а в 1930 году эмигрировал в США, где работал в Принстоне, сначала в Принстонском университете, а начиная с 1933 в Institute for Advanced Studies (вот полный список первых шести постоянных профессоров IAS: Дж. Александер, А. Эйнштейн, М. Морс, О. Веблен, Дж. фон Нейман, Г. Вейль). После ранних работ по основаниям теории множеств и логике фон Нейман заинтересовался функциональным анализом, в особенности в его алгебраических аспектах. Среди вершин его творчества в этом направлении можно упомянуть спектральную теорему для операторов в гильбертовом пространстве, эргодическую теорему и теорию колец операторов (C^*-алгебры, факторы, ...). С большим успехом он применил эти понятия в классической и квантовой механике, и в настоящее время операторные методы стали одним из главных инструментов теоретической физики. Именно фон Нейману и Г. Вейлю принадлежит математическая формулировка квантовой механики в терминах операторов в гильбертовом пространстве. Другие работы фон Неймана относятся к топологическим группам, непрерывным геометриям и т. д. Помимо работ по чистой математике и физике Джон фон Нейман был основателем нескольких громадных направлений в computer science и прикладной математике, в том числе теории автоматов и теории игр. Начиная с 1940-х годов был одним из ключевых участников американского ядерного проекта, директором бюро по проектированию электронных вычислительных машин. Фон Нейман высказал много проникновенных мыслей по поводу математики, самая знаменитая среди которых звучит следующим образом: In Mathematics you don't understand things, you just get used to them. На русский язык переведены его книги [103], [104] и основные статьи по алгебрам операторов [105], [106].

- *умножение* $\mathrm{mult} : G \times G \longrightarrow G$ *непрерывно;*
- *взятие обратного* $\mathrm{inv} : G \longrightarrow G$ *непрерывно.*

/ В терминах открытых множеств эти условия можно сформулировать следующим образом. Первое условие означает, что для любой окрестности U элемента gh существует такая окрестность V элемента g и такая окрестность W элемента h, что $VW \subseteq U$. Второе условие означает, что для любой окрестности U элемента g^{-1} существует такая окрестность V элемента g, что $V^{-1} \subseteq U$. Эти условия мож-

Андре Вейль (Andre Weil, 6 мая 1906, Париж — 6 августа 1998, Принстон) — гениальный французский математик, признанный классик теории чисел, алгебраической геометрии, топологии, гармонического анализа и комплексного анализа, один из основателей Бурбаки. Основные достижения Вейля относятся к теории алгебраических кривых и абелевых многообразий, диофантовой геометрии, анализу на топологических группах, теории алгебраических групп, После окончания Ecole Normale Вейль поехал продолжать образование в Риме и Геттингене, где получил первые существенные результаты по теории алгебраических кривых и уже в 1928 году защитил диссертацию в Парижском университете под руководством Адамара. После этого он преподавал в различных университетах, главным образом в Страсбурге.

Жизнь Вейля хорошо известна из его мемуаров, *блистательной* французской прозы, contes cruelles, не уступающей по точности *языка* Нервалю, Готье, Бодлеру и Валери — что касается содержания и не/двусмысленного юмора, я оставляю их as is. Вот *типичный* комментарий Вейля о коллегах, *один из самых мягких*: когда бог пожалел о своей ошибке, в том, что заставил Куранта родиться в Германии, а не в Америке, он специально прислал Гитлера, чтобы исправить эту ошибку. А вот еще более зловещий образчик его **макабричного** юмора, как-то разбирая книги Вейль решил отнести избранные труды Гильберта в офис, со следующим диагнозом: он недостаточно оригинален.

С началом войны Вейль, чтобы избежать призыва в армию, бежал в Финляндию к Рольфу Неванлинне, но, поскольку в его комнате нашли *бумаги на русском языке* (письма от Понтрягина!), его посадили в тюрьму как **советского шпиона**, и уже собирались расстрелять (как все это похоже на историю Ли!), Неванлинне все же удалось убедить финские власти заменить расстрел на **эквивалентное наказание** — депортацию во Францию, что и было незамедлительно исполнено. Французские власти, *естественно*, тут же посадили Вейля в тюрьму как **дезертира**. В этот момент Вейль решил, что в армии безопаснее, чем в тюрьме, но, будучи **пацифистом**, при первой возможности сбежал в США, где долго не мог получить достойной позиции. После работы в Сан Пауло в 1947 году он наконец получает позицию в Университете Чикаго, а в 1958 году переезжает в Институт высших научных исследований в Принстоне. На русский язык переведено несколько очень широких по замыслу и глубоких по содержанию, но тяжелых для чтения книг **[49]**, [107]–[110].

В широких кругах гораздо более знаменита, чем сам Андре Вейль, его младшая сестра **Симона Вейль** (1909 — 1943), литератор и философ, которая обратилась в католицизм мистического толка настолько радикальный, что даже во время войны выступала с резко антисемитскими сочинениями, за что была канонизирована Ватиканом.

но объединить в одно, потребовав, чтобы отображение $G \times G \longrightarrow G$, $(h, g) \mapsto hg^{-1}$ было непрерывным. Для любого элемента $g \in G$ левая трансляция $L_g : G \mapsto G$, $x \mapsto gx$ и правая трансляция $R_g : G \mapsto G$, $x \mapsto xg$ непрерывны. Так как, кроме того, биективны, и обратные к ним $L_{g^{-1}}$ и $R_{g^{-1}}$, то они являются гомеоморфизмами пространства G на себя. Это значит, что *как топологическое пространство* топологическая группа выглядит одинаково в окрестности каждой точки и все ло-

Лев Семенович Понтрягин (3 сентября 1908, Москва — 3 мая 1988, Москва) — гениальный русский математик, которому принадлежат фундаментальные результаты в области алгебры, топологии, дифференциальных уравнений и оптимального управления. В результате несчастного случая в 14 лет Понтрягин полностью ослеп, и его мать стала его личным секретарем. В 1925 году Понтрягин поступил в Московский университет, где подпал под влияние Павла Сергеевича Александрова и заинтересовался топологией. Уже в 1927 году он получает первые важные результаты по двойственности Александера, и после окончания университета в 1929 году начинает работать там, а с 1934 года, кроме того, в Математическом институте АН СССР. Среди наиболее знаменитых работ Понтрягина его теория двойственности для локально компактных групп (двойственность Понтрягина, решение пятой проблемы Гильберта для абелевых групп) и работы по гомотопической топологии и теории характеристических классов. Эти работы принесли Понтрягину мировую известность. В 1952 году Понтрягин полностью меняет направление своей научной деятельности, переключаясь на качественную теорию дифференциальных уравнений и вариационное исчисление (теорию оптимальных процессов). В этой области он получает другой свой знаменитый результат, принцип максимума Понтрягина. Понтрягин написал несколько книг, сыгравших в свое время чрезвычайно большую роль в развитии алгебраической топологии и топологической алгебры, в том числе **[153]**, [111], , а также учебник [112]. Кроме того в соавторстве со своими учениками В. Г. Болтянским, Р. В. Гамкрелидзе и Е. Ф. Мищенко в 1961 году он публикует знаменитую книгу [113] и в 1980-е годы серию научно-популярных книг. В Успехах математических наук опубликована чрезвычайно живописная автобиография Понтрягина [114], которая целиком разобрана на цитаты: посредственный математик, но активный сионист и т. д.

кальные свойства достаточно изучать только в окрестности e.

Если топологическая группа удовлетворяет какой-нибудь аксиоме отделимости, скажем, T_0, то она автоматически удовлетворяет T_2, т. е. хаусдорфова. Как правило, в теории топологических групп рассматривают только **отделимые группы**, т. е. предполагается, что G является хаусдорфовым топологическим пространством. Так как топология топологической группы полностью определяется системой окрестностей e, для проверки отделимости достаточно проверить, что множество $\{e\}$ замкнуто. Группа G называется **связной группой**, **компактной группой**, **локально компактной группой** и т. д., если она обладает соответствующим свойством *как топологическое пространство*.

В действительности на топологической группе естественно задаются структуры равномерного пространства. Чтобы проиллюстрировать, как некоммутативность скажется на развитии анализа, приведем определение равномерно непрерывной функции. Функция $f : G \longrightarrow \mathbb{R}$ называется **равномерно непрерывной слева**, если для любой окрестности $0 \in U \subseteq \mathbb{R}$ существует окрестность $e \in V \subseteq G$ такая, что если $x^{-1}y \in V$, то $f(x) - f(y) \in U$. Аналогично, функция $f : G \longrightarrow \mathbb{R}$ называется **равномерно непрерывной справа**, если для любой окрестности U существует такая окрестность V, что если $xy^{-1} \in V$, то $f(x) - f(y) \in U$.

2. Первые примеры топологических групп. Начнем с двух очевидных

(контр)примеров.

• Любая группа G, снабженная дискретной топологией, превращается в топологическую группу, называемую **дискретной группой**. Основной текст настоящей книги относится к изучению дискретных групп. Дискретная группа в том и только том случае компактна, когда она конечна. Большая часть общей теории конечных групп без труда переносится на случай компактных групп.

• Бесконечная группа G снабженная **коконечной топологией**, открытыми множествами в которой являются пустое множество и такие подмножества, дополнения к которым конечны, не может быть топологической группой. Дело в том, что эта топология удовлетворяет T_1, но не T_2.

Мы не будем приводить витиеватые, экзотические и/или бесконечномерные примеры, а ограничимся лишь несколькими простейшими — и именно поэтому наиболее важными! — примерами **локально компактных** топологических групп. Заметим, что **все** эти примеры одновременно являются примерами вещественных или комплексных групп Ли.

• Группа $\mathbb{R}$ вещественных чисел по сложению с обычной вещественной топологией. Иными словами, вычитание $\mathbb{R}\times\mathbb{R}\longrightarrow\mathbb{R}$, $(x,y)\mapsto x-y$, непрерывно как функция двух аргументов.

• Группа $\mathbb{R}^*$ ненулевых вещественных чисел по умножению с обычной вещественной топологией. Иными словами, деление $\mathbb{R}^*\times\mathbb{R}^*\longrightarrow\mathbb{R}^*$, $(x,y)\mapsto x/y$, непрерывно как функция двух аргументов.

• Группы $\mathbb{C}$ и $\mathbb{C}^*$ с обычной комплексной топологией.

• Группа $\mathbb{T}$ вместе с комплексной топологией; эта группа компактна.

• Векторные группы $\mathbb{R}^n$ и $\mathbb{C}^n$ относительно операции сложения векторов.

• Вещественный тор $\mathbb{T}^n$ с покомпонентным умножением; это компактная группа.

• Полные линейные группы $\mathrm{GL}(n,\mathbb{R})$ и $\mathrm{GL}(n,\mathbb{C})$ вместе с обычной вещественной или комплексной топологией.

• Специальные линейные группы $\mathrm{GL}(n,\mathbb{R})$ и $\mathrm{GL}(n,\mathbb{C})$ с топологией индуцированной с $\mathrm{GL}(n,\mathbb{R})$ и $\mathrm{GL}(n,\mathbb{C})$.

• Вообще, все классические группы над $\mathbb{C}$ или $\mathbb{R}$, в частности, симплектические группы $\mathrm{Sp}(2l,\mathbb{C})$ и $\mathrm{Sp}(2l,\mathbb{R})$, ортогональные группы $\mathrm{SO}(n,\mathbb{C})$ и $\mathrm{SO}(p,q,\mathbb{R})$ и унитарные группы $\mathrm{SU}(p,q,\mathbb{C})$. Группы $\mathrm{SO}(n,\mathbb{R})$ и $\mathrm{SU}(n,\mathbb{C})$ компактны.

3. Абстрактное versus топологического. Все понятия в теории топологических групп должны учитывать наличие топологии на G. Например, в теории топологических групп обычно рассматривают **замкнутые подгруппы** (любая **открытая подгруппа** автоматически замкнута!). В действительности, мы *вынуждены* ограничиться рассмотрением замкнутых подгрупп $H\le G$, если хотим, чтобы фактор-пространства G/H тоже были хаусдорфовыми. Точно так же, в теории топологических групп *обычно* рассматривают только **непрерывные гомоморфизмы** и **топологические изоморфизмы** — изоморфизм групп $\phi: H\longrightarrow G$ называется топологическим, если как ϕ, так и ϕ^{-1} непрерывны.

На самом деле большинство математиков — и даже многие профессиональные алгебраисты — никогда не задумывались над тем, что у топологических групп

бывают изоморфизмы, не являющиеся топологическими! Так, в книге IV мы докажем, что группы $\mathbb{T}$ и $\mathbb{C}^*$ изоморфны *как абстрактные группы* — разумеется, этот изоморфизм не может быть топологическим! Кроме того, его построение основано на выборе базиса Гамеля в $\mathbb{R}$ и, тем самым, использует аксиому выбора.

4. Мера Хаара. Для большинства приложений в анализе, геометрии, теории дифференциальных уравнений наиболее важен класс локально компактных групп, который совершенно замечателен тем, что он предоставляет ЕСТЕСТВЕННУЮ ОБЩНОСТЬ ДЛЯ ПОСТРОЕНИЯ АНАЛИЗА. Подавляющая часть тех фактов, которые в преподавании математического анализа *преподносятся* как относящиеся к функциям вещественного аргумента, в действительности справедливы для функций на любой локально компактной группе. Более того, некоммутативность придает изучению таких функций структурное богатство и некоторую дополнительную пикантность. Основой для построения анализа в этом классе групп является существование на любой локально компактной группе аналога меры Лебега. А именно, если G — локально компактная группа, то на σ-алгебре ее подмножеств, порожденной компактными подмножествами, существует такая положительная мера $\mu \neq 0$, что для любого измеримого множества $X \subseteq G$ и любого $g \in G$ множество $gX = \{gx \mid x \in X\}$ тоже измеримо и $\mu(gX) = \mu(X)$. Такая мера называется **левоинвариантной мерой Хаара**. Ясно, что в этом случае мера $\nu(X) = \mu(X^{-1})$ будет **правоинвариантной мерой Хаара** в том смысле, что $\nu(Xg) = \nu(X)$ для любых $X \subseteq G$ и $g \in G$. Основной результат состоит в том, что на любой локально компактной группе G существует левоинвариантная мера Хаара, причем такая мера единственна с точностью до скалярного множителя. Для компактных групп это было доказано еще в знаменитой работе Ф.Петера и Г.Вейля 1927 года [115]. Ключевой шаг был сделан в 1933 году Альфредом Хааром [116], который доказал существование и единственность меры Хаара при дополнительном предположении, что группа G сепарабельна. Наконец, в полной общности результат впервые доказан в 1940 году в книге Андре Вейля [**49**] Весьма интересен вопрос, когда на группе существует **двусторонне инвариантная мера Хаара**, т. е. когда $\mu(X^{-1}) = \mu(X)$ для любого измеримого $X \subseteq G$. Такая группа G называется **унимодулярной**. Вот несколько важнейших классов унимодулярных локально компактных групп:

- компактные,
- дискретные,
- абелевы,
- полупростые группы Ли.

§ 19✠. Группы с дополнительными структурами, 2nd installment: группы Ли

> Les groupes de Lie sont devenus le centre de mathématique. On ne peut plus faire rien de serieux sans eux.*
>
> Jean Dieudonné

*Группы Ли стали самым центром математики. Без них теперь невозможно сделать ничего серьезного.

В анализе и геометрии чаще всего возникают такие топологические группы, в которых операции не просто непрерывны, а являются дифференцируемыми или аналитическими отображениями.

1. Группы Ли. Пусть K — полное локально компактное нормированное поле, например, $K = \mathbb{R}$, $\mathbb{C}$ или $\mathbb{Q}_p$.

Определение. Группой Ли *называется множество, которое несет две согласованные структуры, группы и аналитического многообразия.* **Согласованность** *означает, что*

- *умножение* $\mathrm{mult} : G \times G \longrightarrow G$ *аналитическое,*
- *взятие обратного* $\mathrm{inv} : G \longrightarrow G$ *аналитическое.*

Такие группы часто называются также **аналитическими группами**, в этом случае термин **группы Ли** применяется к формально более общему (но по сути эквивалентному) понятию. В соответствии с тем, структуру многообразия над каким полем несет группа Ли, она называется **вещественной**, **комплексной** или **p-адической**. Всякая комплексная группа Ли автоматически является также вещественной группой Ли, если мы забудем о ее комплексной структуре. **Морфизм групп Ли** — это такой гомоморфизм групп, который одновременно является *аналитическим* отображением.

Простейшие примеры групп Ли были уже фактически приведены нами в предыдущем параграфе. Все приведенные там примеры — в частности, $\mathbb{R}$, $\mathbb{R}^*$, $\mathbb{T}$, $\mathbb{R}^n$, $\mathbb{T}^n$, $\mathrm{GL}(n,\mathbb{R})$, $\mathrm{SL}(n,\mathbb{R})$, $\mathrm{Sp}(2l,\mathbb{R})$, $\mathrm{SO}(p,q,\mathbb{R})$, $\mathrm{SU}(p,q,\mathbb{C})$ — являются вещественными группами Ли, а $\mathbb{C}$, $\mathbb{C}^*$, $\mathbb{C}^n$, $\mathrm{GL}(n,\mathbb{C})$, $\mathrm{SL}(n,\mathbb{C})$, $\mathrm{Sp}(2l,\mathbb{C})$, $\mathrm{SO}(n,\mathbb{C})$, *кроме того*, — и комплексными группами Ли. Обратите внимание, что $\mathrm{SU}(p,q,\mathbb{C})$ и, в частности, компактная форма $\mathrm{SU}(n,\mathbb{C})$ являются *вещественными* группами; комплексной структуры на них нет!

2. Локальные группы Ли. Сам Ли никогда не изучал группы Ли как глобальные объекты. Он рассматривал то, что сегодня называется **локальными группами Ли** или **групускулами Ли**. А именно, локальная группа Ли — это аналитическое многообразие, вместе с выделенным элементом e и двумя аналитическими отображениями $\mathrm{mult} : U \longrightarrow G$, $(x,y) \mapsto xy$, и $\mathrm{inv} : V \longrightarrow G$, $x \mapsto x^{-1}$, где U — некоторая открытая окрестность (e,e) в $G \times G$, содержащая $G \times \{e\}$ и $\{e\} \times G$, а V — открытая окрестность, причем в G *локально* выполняются аксиомы группы. Иными словами, предполагается, что окрестности U и V и отображения mult, inv удовлетворяют следующим аксиомам:

• **Локальная ассоциативность:** *если* оба произведения $(xy)z$ и $x(yz)$ определены, то $(xy)z = x(yz)$;

• **Существование нейтрального элемента:** $eg = g = ge$ для любого $g \in G$;

• **Локальное существование обратного элемента:** для любого $g \in V$ пары (x, x^{-1}), (x^{-1}, x) попадают в U и $xx^{-1} = e = x^{-1}x$.

Пусть теперь H и G — две локальные группы Ли. *Аналитическое* отображение $f : H \longrightarrow G$ называется **гомоморфизмом** локальных групп, если $f(e) = e$ и для любых $h, g \in H$, для которых произведение hg определено, произведение $f(h)f(g)$ также определено и равно $f(hg)$. Гомоморфизм локальных групп $f : H \longrightarrow G$

называется **изоморфизмом**, если он биективен, причем не только f, но и f^{-1} является аналитическим отображением.

Пусть теперь G — настоящая группа Ли. Тогда любая открытая окрестность U элемента $e \in G$ является локальной группой Ли. Две группы Ли H и G называются **локально изоморфными**, если в них существуют открытые окрестности e изоморфные как локальные группы. Разумеется, для дискретных групп это понятие не имеет никакого смысла, так как *любые* две дискретные группы локально изоморфны. Даже для топологических групп локальный изоморфизм представляет собой довольно слабое понятие. Но ведь в группах Ли операции задаются аналитическими отображениями, для которых выполнен принцип аналитического продолжения! Это значит, что локально изоморфные группы Ли устроены практически одинаково и, как мы увидим в следующем пункте, отличаются *лишь* глобальными топологическими инвариантами $\pi_0(G)$ и $\pi_1(G)$. В частности, две связные односвязные группы Ли тогда и только тогда локально изоморфны, когда они изоморфны.

3. Теория Ли. В конце XIX века Софус Ли построил совершенно замечательную теорию, которая полностью сводит *локальное* изучение групп Ли к изучению гораздо более простого чисто алгебраического объекта — алгебр Ли.

Пусть временно R — произвольное коммутативное кольцо. Модуль L над R называется **алгеброй Ли**, если на нем задано билинейное умножение $[\ ,\ ] : L \times L \longrightarrow L$, удовлетворяющее следующим двум замечательным тождествам, первое из которых является аналогом ассоциативности, а второе — коммутативности:

тождество Якоби: $[[x,y],z] + [[x,y],z] + [[x,y],z] = 0$;

антикоммутативность: $[x,x] = 0$.

Пусть теперь L, M — две алгебры Ли. Гомоморфизм R-модулей $f : L \longrightarrow M$ называется **гомоморфизмом алгебр Ли**, если $f([x,y]) = [f(x), f(y)]$ для любых $x, y \in L$.

В **теории Ли** каждой (локальной) группе Ли G над полем K сопоставляется алгебра Ли $L(G)$ над этим полем, называемая **алгеброй Ли группы Ли** G, а каждому локальному гомоморфизму $f : H \longrightarrow G$ — гомоморфизм $df = L(f) : L(H) \longrightarrow L(G)$ алгебр Ли, называемый **дифференциалом** f. В качестве $L(G)$ можно взять алгебру Ли левоинвариантных векторных полей на G относительно операции коммутирования векторных полей. Мы не можем здесь описать детали этого сопоставления, так как оно требует техники дифференциальной геометрии (либо какой-то другой техники дифференцирования, ну там, формальных групп или чего-то в таком духе). Сопоставление $G \quad L(G)$ обладает прекрасными функториальными свойствами. Вот несколько типичных утверждений.

• Две группы Ли H и G тогда и только тогда локально изоморфны, когда их алгебры Ли $L(H)$ и $L(G)$ изоморфны.

Роль условий связности и односвязности определяется следующим:

• Пусть $\phi, \psi : H \longrightarrow G$ — два гомоморфизма *связной* группы Ли H в группу Ли G. Если $d\phi = d\psi$, то $\phi = \psi$.

• Пусть $\psi : L(H) \longrightarrow L(G)$ — гомоморфизм алгебры Ли группы Ли H в алгебру Ли группы Ли G. Если H *односвязна* то существует гомоморфизм $\phi : H \longrightarrow G$ такой, что $d\phi = \psi$.

• Для любой конечномерной вещественной алгебры Ли L существует такая группа Ли G, что $L(G) \cong L$ (это утверждение традиционно называется **третьей теоремой Ли**, но в действительности оно было доказано только в 1930 году Эли Картаном).

Эли Жозеф Картан (Elie Joseph Cartan, 9 апреля 1869, Доломье, Савойя — 6 мая 1951, Париж) — гениальный французский математик, основные работы которого относятся к алгебре, геометрии и теории дифференциальных уравнений. После окончания Ecole Normale в 1894 году он защищает знаменитую диссертацию, в которой завершает классификацию простых комплексных алгебр Ли. Совершенно очевидно, что получение этой классификации, известной как **классификация Картана—Киллинга**, является самым важным событием фаустовского тысячелетия 1001–2000. После этого в 1894–1909 годах он преподает в Монпелье, Лионе и Нанси, в эти годы он занимается вначале классификацией ассоциативных алгебр, а потом представлениями полупростых алгебр Ли. Позже эта теория была завершена Вейлем и известна как **теория Картана—Вейля**.

В начале XX века Картан обращается к теории обыкновенных дифференциальных уравнений, а после того, как в 1909 году он получает позицию в Париже, его основные работы связаны с теорией вещественных алгебр Ли и дифференциальной геометрией, в основном теорией симметрических римановых пространств. Ему удается полностью классифицировать простые вещественные алгебры Ли и некоторые классы подалгебр в них и тем самым получить полную классификацию симметрических римановых пространств. Этим он завершает решение задачи, которая находилась в центре интересов многих лучших геометров XIX века. С другой стороны, кроме своего непосредственного влияния на теорию групп Ли и дифференциальную геометрию, работа Картана послужила отправной точкой для многих современных исследований в теории представлений, гармоническом анализе и алгебраической геометрии. По любым критериям это одно из центральных достижений математики XX века.

Еще одним замечательным достижением Картана является открытие замечательных классов бесконечномерных групп и алгебр Ли, **алгебр картановского типа**. По своему происхождению это бесконечномерные алгебры Ли векторных полей, заданные на конечномерном пространстве. Оказалось, что аналоги этих алгебр в положительной характеристике становятся конечномерными; алгебрами из списка Картана—Киллинга и деформации алгебр картановского типа исчерпываются простые алгебр Ли в характеристиках $p \geq 7$. В математике встречается много понятий, связанных с именем Картана, картановская подалгебра, картановская подгруппа, матрица Картана, числа Картана, разложение Картана и т. д.

Один из его сыновей, **Анри Картан**, тоже стал гениальным математиком, внесшим крупнейший вклад в теорию функций многих комплексных переменных, топологию и алгебру, одним из основателей Бурбаки. Другой его сын, **Луи Картан**, физик, в 1942 был арестован немцами и после 15 месяцев заключения казнен. На русский переведено несколько книг Картана и цикл его статей о бесконечномерных группах [117].

• $L(H \times G) \cong L(H) \times L(G)$ и т. д.

4. Классификация Картана—Киллинга. Изучение групп Ли сводится к двум противоположным случаям: разрешимые и полупростые группы. Индивидуально разрешимые группы Ли устроены весьма просто, но об их классификации не может быть и речи. С другой стороны, строение полупростых групп Ли достаточно замысловато, но зато имеется их полный список. При этом группа Ли называется **разрешимой**, если она разрешима как абстрактная группа. Группа Ли называется **простой**, если ее размерность > 0 и у нее нет нормальных подгрупп положительной размерности. Группа Ли называется **полупростой**, если у нее нет *разрешимых* нормальных подгрупп положительной размерности.

Следующий список, известный как **список Картана—Киллинга**, является, несомненно, самой важной классификацией, до сих пор полученной в истории математики. В этом списке мы указывает односвязные комплексные простые группы Ли. Здесь фигурируют спинорные группы $\mathrm{Spin}(n, \mathbb{C})$. Это односвязные накрывающие ортогональных групп $\mathrm{SO}(n, \mathbb{C}) = \mathrm{Spin}(n, \mathbb{C})/\{\pm 1\}$, которым они локально изоморфны. Таким образом, тот, кто еще не знает, что такое спинорные группы, и не настаивает на том, чтобы указывать односвязную группу каждого типа, может взять $\mathrm{SO}(2l+1, \mathbb{C})$ и $\mathrm{SO}(2l, \mathbb{C})$ как представители типов B_l и D_l.

- $\mathrm{SL}(l+1, \mathbb{C})$, тип A_l
- $\mathrm{Spin}(2l+1, \mathbb{C})$, тип B_l
- $\mathrm{Sp}(2l, \mathbb{C})$, тип C_l
- $\mathrm{Spin}(2l, \mathbb{C})$, тип D_l
- пять исключительных групп типов E_6, E_7, E_8, F_4, G_2

Совершенно замечательно, что точно тем же списком описываются и *компактные* простые вещественные группы Ли.

3. Пятая проблема Гильберта. Во многих книгах *вещественные* группы Ли определяются более широко, чем это сделали мы. А именно, требуют, чтобы G несло на себе структуру гладкого (класса C^∞), дифференцируемого (класса C^r, $1 \le r < \infty$) или даже просто топологического (класса C^0) многообразия, а умножение mult и обращение inv имели соответствующий класс гладкости. Вопрос о том, действительно ли эти определения эквивалентны определению в терминах аналитических отображений, известен как **пятая проблема Гильберта**.

Вот еще одна традиционная эквивалентная переформулировка этого вопроса: на любой ли локально эвклидовой — т. е. *локально гомеоморфной* $\mathbb{R}^n$ — топологической группе можно ввести аналитическую структуру так, чтобы она стала группой Ли? В классе компактных групп эту проблему положительно решил Джон фон Нейман в 1933 году [127], а в классе коммутативных локально компактных групп — Лев Семенович Понтрягин в 1934 году [128]. Однако общий случай ждал окончательного решения еще почти 20 лет [129], [130].

Теорема Глисона—Монтгомери—Циппина. *Любая локально эвклидова топологическая группа есть вещественная группа Ли.*

Говорят, что в топологической группе есть **малые подгруппы**, если в любой окрестности 1 содержится подгруппа $H \ne 1$. Общая идея доказательства сформулированной выше теоремы состоит в следующем: доказывается, что локально компактная группа без малых подгрупп есть группа Ли, а группы с малыми подгруппами не являются локально эвклидовыми.

Вильгельм Киллинг (Wilhelm Killing, 10 мая 1847, Бурбах, Вестфалия — 11 февраля 1923, Мюнстер) — гениальный немецкий математик, один из классиков алгебры и геометрии. В конце 1870-х годов Киллинг независимо от Ли — и из других соображений! — пришел к понятию алгебры Ли и в 1888–1890 годах классифицировал простые комплексные алгебры Ли. Для достижения этой цели он совершил САМОЕ ВАЖНОЕ ОТКРЫТИЕ ФАУСТОВСКОГО ТЫСЯЧЕЛЕТИЯ 1001–2000 — открыл исключительные алгебры Ли типов E_6, E_7, E_8, F_4, G_2. Большая часть математики XX века зависела от этого открытия и/или вдохновлялась им. Киллинг начал свою учебу в Мюнстере, но вскоре переехал в Берлин, где стал учеником Вейерштрасса и Куммера. Его диссертация посвящена геометрическим применениям "жордановой формы". Однако еще 20 лет после защиты Киллинг не мог получить университетской позиции, с 1868 по 1882 год он преподавал в школах в Берлине и Вестфалии, а с 1882 по 1892 — в гимназии в Браунсберге (по нынешним временам Braniewo в Ольштынском воеводстве)! В это время он и выполняет свои самые важные работы, в частности, классификацию Картана–Киллинга. Правда при этом он не замечает, что E_4 и F_4 изоморфны, так что в его классификации **шесть** исключительных алгебр, а не пять. Это обстоятельство было использовано как предлог для травли Киллинга и полного замалчивания его достижений. Только в 1892 году он наконец становится профессором в Мюнстере. Сама жизнь Киллинга тоже была произведением искусства на тему *подражание святому Франциску Ассизскому*. В приложение к своей феерической научной деятельности, 36 часам педагогической нагрузки в неделю (!!!) — кто из современных математиков мог бы писать какие-то статьи, не такие статьи как Киллинг, а вообще *какие-то* при подобной нагрузке? — и административным обязанностям (ректор колледжа, член городского совета, член церковного совета, ...) Киллинг был *ревностным* католиком, в возрасте 39 лет он и жена — от которой у него к этому моменту было 7 детей — вступили в орден францисканцев — IT'S PEOPLE LIKE THAT WHO MAKE YOU REALISE HOW LITTLE YOU HAVE ACCOMPLISHED!!! Работы Киллинга подвергались остракизму: определяющую роль в этом сыграла ревность Ли, который тщательно оберегал свой приоритет и постоянно искал у Киллинга ошибки — из восьми ссылок на Киллинга в трактате Ли семь резко негативные! С другой стороны, во Франции, следуя Пуанкаре, было принято приписывать **все** заслуги по классификации Картану (СТРОЖАЙШИМ ОБРАЗОМ ЗАПРЕЩАЕТСЯ ЦИТИРОВАТЬ ИНОСТРАНЦЕВ). Между тем, алгебры Картана и матрицы Картана, группы Вейля, элементы Коксетера и числа Коксетера введены уже в работах Киллинга 1888–1890 годов! С другой стороны, в качестве блестящей иллюстрации принципа Арнольда, форму Киллинга ввел Картан — для доказательства критериев Картана! Кстати, самого Картана, как раз, *никак* нельзя обвинить в игнорировании работ Киллинга или замалчиваний его достижений. В его диссертации, которая считается каноническим источником по классификации простых алгебр Ли, работы Ли цитируются 20 раз, в то время как работы Киллинга — 63 раза! В связи с прочими вещами, которые появляются в нашем курсе, можно упомянуть, что именно Киллинг ввел термин **характеристическое уравнение**.

Давид Гильберт (David Hilbert, 23 января 1862, Кенигсберг — 14 февраля 1943, Геттинген) — самый значительный математик первой половины XX века, внесший огромный вклад практически во все разделы математики, включая алгебру, алгебраическую и аналитическую теорию чисел, алгебраическую геометрию, геометрию, функциональный анализ, теорию интегральных уравнений, математическую физику, вариационное исчисление, математическую логику и основания математики. Гильберт учился в Университете Кенигсберга под руководством фон Линдеманна и получил степень в 1885 году за работу по теории инвариантов. После этого он еще 10 лет работает в Кенигсберге, именно здесь формируется его дружба с Адольфом Гурвицем и Германном Минковским, которая сыграла такую роль в истории математики. Однако в 1895 году Клейну удается переманить его в Геттинген.

Начиная с 1880-х годов деятельность Гильберта преобразует одну область математики за другой. Вначале это теория инвариантов (теорема Гильберта о базисе), потом алгебраическая теория чисел, где он дает почти современную формулировку теории полей классов (*Zahlbericht*), потом основания геометрии (*Grundlagen der Geometrie* [118]). В 1900 году на Втором Конгрессе Математиков в Париже Гильберт произносит свой знаменитый доклад [119], в котором формулирует 23 проблемы, в значительной степени определившие развитие математики в XX веке: wir mussen wissen, wir werden wissen — мы должны знать и мы *будем* знать. В 1909 году Гильберт решает проблему Варинга, остававшуюся неприступной с XVIII века.

Его работы в области интегральных уравнений приводят к кристаллизации понятия гильбертова пространства и формированию функционального анализа. Эти исследования отражены в монументальном двухтомнике Куранта—Гильберта *Методы математической физики* [120], [121]. Кстати, в годы нацизма говорили, что Гильберт единственный арийский математик в Геттингене, но в его жилах течет еврейская кровь: во время операции ему сделали переливание крови от Куранта. В 1910-е и 1920-е годы Гильберт обращается к физике: die Physik ist fur die Physiker eigentlich *viel* zu schwer — физика слишком трудна для физиков. Наконец, в 1920-е и 1930-е годы его основные интересы связаны с попыткой финитистского обоснования математики. Эти работы отражены в фундаментальных книгах Гильберта—Бернайса *Основания математики* [122], [123]. Кроме того, на русский переведены его основные статьи [124], [125] и замечательная научно-популярная книга [126].

Среди его непосредственных учеников такие выдающиеся математики, как Отто Блюменталь, Макс Ден, Эмми Нетер, Герман Вейль, Рихард Курант, Эрхард Шмидт, Эрих Гекке, Альфред Хаар, Андреас Шпайзер, Хельмут Кнезер, Гуго Штейнгауз и многие другие, еще больше тех, кто не был его непосредственным учеником, но находился под его влиянием.

§ 20✠. Группы с дополнительными структурами, 3rd installment: алгебраические группы

> I believe in a heliocentric view of the Universe, with linear groups playing the role of the Sun.
>
> John Thompson

С современной точки зрения теория групп Ли в значительной степени поглощена теорией алгебраических групп. С одной стороны, каждая вещественная или комплексная алгебраическая группа является группой Ли. В свою очередь, два наиболее важных класса групп Ли, а именно,

- компактные вещественные группы Ли и
- комплексные полупростые группы Ли

являются линейными алгебраическими группами. Теория линейных алгебраических групп как раз и представляет собой обобщение наиболее содержательной части теории групп Ли — теории полупростых групп — на случай *произвольного* основного поля. Теория алгебраических групп играет для **всех** наук алгебраического цикла — самой алгебры, теории чисел, алгебраической геометрии — такую же роль, как теория групп Ли для наук аналитического цикла — анализа, теории дифференциальных уравнений, дифференциальной геометрии. Изначально эта теория возникла в конце XIX начале XX века в контексте теории Пикара—Вессио дифференциальных уравнений, однако в дальнейшем ее развитие приостановилось почти на полвека. Современная теория алгебраических групп была создана Элиасом Колчиным, Клодом Шевалле, Арманом Борелем, Андре Вейлем, Марвином Розенлихтом в 1940-е и 1950-е годы. В 1960-х ключевую роль в ее дальнейшем развитии сыграли многие замечательные математики, в том числе Жан-Пьер Серр, Тони Спрингер, Жак Титс и Роберт Стейнберг.

1. Аффинные алгебраические группы. Пусть K — алгебраически замкнутое поле. В самом общем смысле аффинное алгебраическое многообразие над K следует понимать как множество решений некоторой системы алгебраических уравнений над K. Полиномиальное отображение одного аффинного алгебраического многообразия в другое называется регулярным (или морфизмом многообразий). Вообще алгебраическим многообразием называется объект, склееный из аффинных кусков при помощи регулярных отображений. Определение алгебраических групп параллельно определению топологических групп, с заменой топологических пространств на алгебраические многообразия.

Определение. Алгебраической группой *называется множество, которое несет две согласованные структуры, группы и алгебраического многообразия.* **Согласованность** *означает, что*

- *умножение* $\mathrm{mult} : G \times G \longrightarrow G$ *регулярно;*
- *взятие обратного* $\mathrm{inv} : G \longrightarrow G$ *регулярно.*

Гомоморфизм $\phi : H \longrightarrow G$ называется морфизмом алгебраических групп, если он, кроме того, является регулярным отображением. Подгруппа $H \leq G$ называется алгебраической подгруппой, если она является замкнутым подмногообразием в G.

Предостережение. Более квалифицированные читатели знают, что алгебраические многообразия снабжаются топологией Зариского. Стоит подчеркнуть, что за исключением тривиального случая конечных групп с дискретной топологией алгебраическая группа *никогда* не является топологической группой. Это обстоятельство фактически уже отмечалось в § 14. Дело в том, что алгебраическое многообразие размерности ≥ 1 удовлетворяют аксиоме отделимости T_1, но не T_2.

Изучение алгебраических групп разбивается на изучение групп двух принципиально различных типов:

Клод Шевалле (Claude Chevalley, 11 февраля 1909, Йоханнисбург, Трансвааль — 20 июня 1984, Париж) — гениальный французский математик, создатель теории алгебраических групп, внесший ключевой вклад в развитие алгебраической теории чисел, алгебраической геометрии, теории представлений, линейной алгебры и коммутативной алгебры; младший по возрасту из первоначального состава Бурбаки. После окончания Ecole Normale под руководством Пикара он поехал продолжать свое образование в Германии, вначале у Артина в Гамбурге, а потом защитил диссертацию в Марбурге под руководством Хассе. В 1938 году Шевалле уезжает в США, в Институт Высших Научных Исследований, при этом он преподавал в Принстонском Университете. В 1949 году Шевалле становится профессором Колумбийского Университета в Нью-Йорке, но в середине 1950-х годов возвращается в Париж. Введенные им в 1930-х годах понятия аделя и иделя являются ключом к современной формулировке теории полей классов. Его работа 1940-х годов в области локальной алгебры и оснований алгебраической геометрии, наряду с работой Зарисского и Андре Вейля послужила основой для полной перестройки алгебраической геометрии в 1950-х годах Гротендиком, Серром и Дьедонне. Книга Шевалле, в которой впервые дано глобальное изложение теории групп Ли, и его работы 1950-х годов по классификации полупростых алгебраических групп и их неприводимых представлений, подняли на совершенно новый уровень доставшуюся нам от Ли, Киллинга, Картана и Германа Вейля традицию теории Ли. Именно Шевалле доказал большую часть основополагающих результатов в теории линейных алгебраических групп и их представлений и записки его семинаров 1956–1958 годов [**251**], среди специалистов цитируются как **Библия**: первые 15–20 теорем в любом курсе линейных алгебраических групп называются примерно так: теорема Шевалле — теорема Шевалле — теорема Бореля — теорема Шевалле — теорема Шевалле — ... Более того, *в качестве побочного продукта* эти работы привели — после полувекового перерыва!! — к открытию новых серий конечных простых групп и, тем самым, послужили отправной точкой классификации конечных простых групп, и последовавшего преобразования всей конечной математики. С его именем связаны группы Шевалле, коммутационная формула Шевалле, схемы Шевалле—Демазюра, разложение Жордана—Шевалле, формула Шевалле—Титса, разложение Шевалле—Мацумото и многие другие понятия. Он написал несколько *совершенно блистательных* книг, непревзойденной ясности, включая трехтомник [**217**], а также [131] и, к сожалению не переведенные на русский [132]–[134].

• **абелевых многообразий**, для которых G полно как алгебраическое многообразие,

• **линейных алгебраических групп**, для которых многообразие G аффинно.

Теорема Шевалле—Розенлихта утверждает, что в каждой алгебраической группе G существует единственная нормальная линейная алгебраическая подгруппа H, фактор-группа по которой G/H является абелевым многообразием. Абелевы многообразия действительно является абелевыми группами весьма предсказуемого строения, но с ними связаны совершенно нетривиальные геометрические вопросы. С другой стороны, геометрия линейных алгебраических групп значительно проще, а в наиболее важном случае полупростых групп над алгебраически замкнутым

полем вообще никакой геометрии нет — геометрия полупростых групп полностью определяется их алгеброй. Но зато алгебраическое строение линейных алгебраических групп весьма богато и сложно.

2. Примеры алгебраических групп. Теория алгебраических групп достаточно детально обсуждается в книге IIB, поэтому ограничимся пока несколькими простейшими примерами, параллельными встречавшимся нам примерах групп Ли.

• Любая конечная группа G является линейной алгебраической группой над произвольным полем K. Пусть G — произвольная линейная алгебраическая группа, а G^0 — связная компонента 1 в группе G. Тогда $G^0 \trianglelefteq G$, причем фактор-группа G/G^0 конечна. Поэтому в теории алгебраических групп принято ограничиваться изучением **связных** групп.

• Аддитивная группа G_a, группа точек которой равна K. Ясно, что $x+y$ и $-x$ — многочлены от x и y.

• Мультипликативная группа G_m, группа точек которой равна K^*. На первый взгляд кажется, что G_m задается *неравенством* $\{x \in K \mid x \neq 0\}$, а x^{-1} не является многочленом от x. Однако это зависит от того, *куда* мы пытаемся поселить G_m. На самом деле правильно реализовывать G_m как $\{(x,y) \in K^2 \mid xy = 1\}$. В этом случае $(x,y)(u,v) = (xu, yv)$ и $(x,y)^{-1} = (y,x)$ задаются многочленами.

Группы G_a и G_m являются единственными одномерными связными линейными алгебраическими группами. Интересно, что жесткое различие между G_a и G_m свойственно именно алгебраической ситуации. Как группы Ли G_a и G_m локально изоморфны, но этот изоморфизм в одну сторону задается экспонентой, а в другую — логарифмом. А это ряды, а не многочлены.

• Векторная группа $G_a^n = G_a \times \ldots \times G_a$.

• Алгебраический тор $G_m^n = G_m \times \ldots \times G_m$.

Следующий пример является универсальным.

• Полная линейная группа $\mathrm{GL}(n,K)$. Как и в случае G_m, чтобы операции в $\mathrm{GL}(n,K)$ задавались многочленами, нужно увеличить число параметров на 1, добавив еще одну переменную $y = \det(x_{ij})^{-1}$.

Полная линейная группа замечательна тем, что — как говорит само название — любая алгебраическая группа, многообразие которой аффинно, может быть вложена в группу $\mathrm{GL}(n,K)$ при подходящем n. Опять здесь проявляется коренное различие с группами Ли, так как например, (топологическая) универсальная накрывающая группа $\widetilde{\mathrm{SL}(2,\mathbb{R})}$ группы $\mathrm{SL}(2,\mathbb{R})$ не является линейной, т. е. не вкладывается ни в одну из групп $\mathrm{GL}(n,\mathbb{R})$.

С другой стороны, в алгебраическом случае большинство естественно возникающих подгрупп в $\mathrm{GL}(n,K)$ являются алгебраическими. В частности, это относится к уже встречавшимся нам группам $\mathrm{SL}(n,K)$, $\mathrm{Sp}(2l,K)$, $\mathrm{SO}(n,K)$ и т. д. В 1957 году Шевалле доказал совершенно удивительный результат, утверждающий, что классификация простых алгебраических групп не зависит от выбора алгебраически замкнутого поля K. В частности, с точностью до локального изоморфизма (который в алгебраической ситуации называется **изогенией**), мы снова получаем список Картана—Киллинга A_l, B_l, C_l, D_l, E_6, E_7, E_8, F_4, G_2.

3. Алгебраические группы и конечные группы. Мы уже заметили, что формально каждая конечная группа является алгебраической. Однако в отличие

от, скажем, теории конечных групп и теории компактных групп, взаимоотношения теории конечных групп и теории алгебраических групп не представляют собой дорогу с односторонним движением. Наоборот, в настоящее время можно однозначно сказать, что теория конечных групп в *значительно* большей степени зависит от теории алгебраических групп, чем наоборот, — хотя в самое последнее время появились и новые **спектакулярные** приложения классификации простых конечных групп в структурной теории алгебраических групп!

Побочным продуктом работы Шевалле по классификации простых алгебраических групп было открытие — после пятидесятилетнего перерыва! — новых бесконечных серий конечных простых групп, **групп Шевалле** типов E_7, E_8 и F_4 над конечным полем. В течение нескольких лет после этого грандиозного прорыва Стейнберг и Титс построили дальнейшие серии простых конечных групп — **скрученные группы Шевалле** типов ${}^2E_6$ и ${}^3D_4$, а потом Судзуки и Ри — **группы Судзуки** ${}^2B_2$ и **группы Ри** ${}^2G_2$, ${}^2F_4$, отвечающие неалгебраическим скручиваниям. Вместе эти три типа групп:

- группы Шевалле, включая классические серии и группы типов E_6 и G_2, открытые Диксоном в 1905 году;
- скрученные группы Шевалле, включая классические серии;
- группы Судзуки и Ри

называются конечными **группами типа Ли**. Они образуют основную массу конечных простых групп.

В последние 20–30 лет стало ясно, что первым шагом к решению *любой* разумной, но достаточно сложной, задачи про простые конечные группы является решение аналогичного вопроса для простых алгебраических групп. В частности, это относится к таким проблемам как:

- описание максимальных подгрупп;
- описание классов сопряженных элементов;
- описание комплексных представлений

и ко многим другим важнейшим вопросам. Так, в настоящее время из теорий Делиня—Люстига и Люстига мы знаем неприводимые комплексные представления групп типа Ли. Но эти теории критическим образом опираются на изучение алгебраических групп и весьма глубокую алгебраическую геометрию, лишь для очень немногих групп (группа $\mathrm{GL}(n,q)$ и некоторые группы совсем маленьких рангов) известно описание их представлений, не зависящее от изучения алгебраических групп над алгебраическим замыканием поля $\mathbb{F}_q$. Поэтому каждый, кто *серьезно* интересуется конечными группами и их приложениями в теории чисел, комбинаторике, конечных геометриях, теории решеток и т. д., должен как можно раньше овладеть основными понятиями и техникой теории алгебраических групп.

§ 21♠. Квазигруппы и латинские квадраты

> Нет сомнения, что время так же относится к весу, как бремя к бесу.
>
> Велимир Хлебников. *Ka*

Как мы знаем, ассоциативность произвольной операции трудно усмотреть из таблицы Кэли. Однако два другие условия, входящие в определение группы, моментально усматриваются из ее таблицы Кэли. В этом параграфе произойдет нечто совершенно удивительное. Оказывается, при наличии сокращения существует простой критерий, позволяющий проверить ассоциативность умножения.

1. Латинские квадраты. А именно, как мы знаем, в группе возможно сокращение на любой элемент как слева, так и справа. Возможность сокращения слева означает в точности, что строки таблицы Кэли состоят из попарно различных элементов, а возможность сокращения справа эквивалентна аналогичному условию для столбцов. Например, в полугруппе левых нулей возможно сокращение справа, но не слева, а в полугруппе правых нулей, соответственно, слева, но не справа. Это значит, что для группы все строки и все столбцы ее таблицы Кэли состоят из попарно различных элементов. Такие таблицы встречаются настолько часто, что имеют специальное название.

Рассмотрим n-элементное множество X. Расположение элементов множества X в квадратную таблицу размера $n \times n$ таким образом, чтобы каждый элемент множества X встречался ровно по одному разу в каждой строке и каждом столбце, называется **латинским квадратом**. Таким образом, в терминологии главы 5 каждая строка и каждый столбец латинского квадрата являются перестановками множества X. Число n называется порядком латинского квадрата.

Легко построить латинский квадрат любого порядка, для этого достаточно расположить элементы X в первой строке произвольным образом, а каждую следующую строку строить из предыдущей применением длинного цикла `RotateRight`. Получающаяся таблица является таблицей Кэли циклической группы порядка $n = |X|$.

Комментарий. Латинские квадраты были введены Эйлером и Мак-Магоном и играют громадную роль не только в комбинаторике и теории групп, но и в статистике и планировании экспериментов. Их часто использовали в агротехнических экспериментах, с чем связан сельскохозяйственный характер сложившейся терминологии [135]. Для их построения широко используются методы, связанные с конечными полями и геометриями, к чему мы вернемся в дальнейшем.

2. Квазигруппы. Таблица умножения группы обязана быть латинским квадратом. Однако, будучи необходимым, это условие далеко не достаточно. Например, рассмотренная в [136] таблица

*	a	b	c	d
a	a	b	d	c
b	b	c	a	d
c	c	d	b	a
d	d	a	c	b

является латинским квадратом, но не задает группу, по двум причинам. Во-первых, в таблице с таким умножением нет нейтрального элемента (для нейтрального элемента соответствующая строка и столбец должны совпадать с исходным расположением элементов множества X). Во-вторых, задаваемое этой таблицей умножение неассоциативно: $(ab)d = bd = d$, в то время как $a(bd) = ad = c$.

В действительности, латинские квадраты это *в точности* таблицы Кэли квазигрупп. Множество G с (не обязательно ассоциативной!) бинарной операцией называется **квазигруппой**, если в нем возможно сокращение на любой элемент слева и справа, т. е. если для любых $x, y, z \in G$ каждое из равенств $zx = zy$ и $xz = yz$ влечет равенство $x = y$. Квазигруппа с нейтральным элементом называется **лупой**.

Задача. Введем в группе G новую операцию $\circ$, полагая $x \circ y = xy^{-1}$. Покажите, что $(G, \circ)$ квазигруппа. При каком условии эта квазигруппа является лупой? При каком условии операция $\circ$ ассоциативна? Коммутативна?

3. Критерий квадрата. Как уже отмечалось, в общем случае для проверки ассоциативности разумнее использовать не таблицу Кэли, а другие средства. С другой стороны, из таблицы Кэли моментально усматривается, что задаваемая ею алгебраическая система является лупой. Оказывается, в этом случае сравнительно несложно установить и наличие или отстутствие ассоциативности.

Задача. Для того, чтобы проверить, что лупа является группой, достаточно убедиться в выполнении следующего условия: если элементы, стоящие в трех парах вершин двух квадратов, совпадают, то совпадают и элементы, стоящие в их четвертых вершинах.

Для любителей наукообразия переведем это условие с обычного алгебраического языка на язык формул. Для того, чтобы лупа G была группой, необходимо и достаточно, чтобы для любых 8 элементов $x_i, y_i, u_i, v_i \in G$, где $i = 1, 2$, выполнялось следующее условие: если $x_1u_1 = x_2u_2$, $x_1v_1 = x_2u_2$, $y_1u_1 = y_2u_2$, то и $y_1v_1 = y_2v_2$.

Приведем, в заключение, две такие таблицы, первая из которых изображает **циклическую** группу порядка 4, а вторая — наименьшую *нециклическую* группу, так называемую **четверную группу** Клейна, обычно обозначаемую V (читается `фау`, от немецкого `Vierergruppe`) или E_4:

$*$	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

$*$	a	b	c	d
a	a	b	b	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Разумеется, и в той и в другой таблице a играет роль нейтрального элемента. Даже невооруженным глазом видно, насколько эти таблицы симметричнее, чем приведенная выше, изображающая квазигруппу.

4. Дистрибутивные квазигруппы. Квазигруппа называется **дистрибутивной**, если операция в ней **автодистрибутивна**, т. е. дистрибутивна слева и справа относительно самой себя: $x(yz) = (xy)(xz)$ и $(xy)z = (xz)(yz)$.

Задача. Покажите, что операция взятия **среднего арифметического**

$$(x, y) \mapsto S_1(x, y) = \frac{x + y}{2}$$

определяет на $\mathbb{Q}$ структуру коммутативной дистрибутивной квазигруппы.

Задача. Убедитесь, что каждый элемент дистрибутивной квазигруппы идемпотентен, т.е. $x^2 = x$.

В частности, дистрибутивная квазигруппа, содержащая больше одного элемента, не может быть группой.

Задача. Докажите, что в конечной коммутативной квазигруппе нечетное число элементов.

Задача. Введем в группе G операцию $*$, полагая $x * y = {}^x y = xyx^{-1}$. Покажите, что для $*$ выполнено левое сокращение: из $x * y = x * z$ вытекает $y = z$. Кроме того, эта операция автодистрибутивна слева: $x * (y * z) = (x * y) * (x * z)$. Будет ли группа G квазигруппой относительно этой операции? Выполняется ли для нее правая автодистрибутивность?

§ 22✠. Инверсные полугруппы, группоиды, гипергруппы

В настоящем параграфе мы обсудим дальнейшие обобщения понятия группы, получающиеся отбрасыванием одной из аксиом группы, или ее части. В предыдущем параграфе мы уже выяснили, что получается, если отбросить ассоциативность.

Формально, можно конечно, отбросить аксиому о существовании обратного и сказать, что **моноид** является обобщением группы. Однако, я так не считаю. В действительности, существование обратных — это *единственная* аксиома, которую не хотелось бы отбрасывать, потому что именно она придает необходимую жесткость понятию группы. Понятие моноида является настолько аморфным, что ни о какой осмысленной структурной теории моноидов — даже конечных моноидов — не может быть и речи. Моноиды — это объект, который можно изучать и даже использовать, но классифицировать их нельзя.

В этот момент новичок может испытать некоторое недоумение: ведь больше в определении группы отбрасывать нечего! Существование обратных зависит от существования нейтрального элемента, а других аксиом в определении группы нет! — Errore! Errore! Во-первых, существование обратных никак не зависит от существования нейтрального элемента: отбрасывая предположение о существовании единственного нейтрального элемента, мы приходим к понятию инверсной полугруппы. Во-вторых, в определении группы спрятана еще одна аксиома, с которой как раз и стоит поиграть. Вот эта аксиома, с проверки которой и нужно начинать проверку того, что G группа!

G0. Определение произведения: Для *любых* $x, y \in G$ определено *единственное* $xy \in G$.

Вот эту аксиому мы сейчас и ослабим: не для любых — или не единственное! На этом пути мы получим еще два важнейших обобщения понятия группы: группоиды и гипергруппы.

1. Инверсные полугруппы. Пусть G — *полугруппа*. Элемент $y \in G$ называется **инверсным** (или **обобщенно обратным**) к элементу $x \in G$, если $xyx = x$ и $yxy = y$. Вообще говоря, из существования инверсного элемента еще совершенно не следует его единственность. Более того, легко построить примеры полугрупп, в которых любые два элемента инверсны друг другу!

Полугруппа G называется **инверсной**, если для любого $x \in G$ существует *единственный* инверсный элемент, который в этом случае обозначается через x^{-1}. Напомним, что **идемпотентом** полугруппы называется любой элемент $e \in G$ такой,

что $e^2 = e$. Нейтральный элемент группы является ее единственным идемпотентом. Группы, как раз, и могут быть охарактеризованы как инверсные полугруппы с единственным идемпотентом. Инверсные полугруппы начали систематически изучать В. В. Вагнер [137], который называл их **обобщенными группами**, и Гордон Престон [138].

Инвертирование в инверсной полугруппе обладает всеми свойствами обращения в группе и с инверсными элементами можно работать почти точно так же, как с обратными.

Задача. Докажите, что в инверсной полугруппе выполняются тождества

$$(x^{-1})^{-1} = x, \qquad (xy)^{-1} = y^{-1}x^{-1}, \qquad xx^{-1}yy^{-1} = yy^{-1}xx^{-1}.$$

Верно ли, что $xx^{-1} = x^{-1}x$?

Многие авторы как раз и определяют инверсную полугруппу $(G, \mathrm{mult}, \mathrm{inv})$ как множество G с двумя операциями $\mathrm{mult} : G \times G \longrightarrow G$, $(x, y) \mapsto xy$, и $\mathrm{inv} : G \longrightarrow G$, $x \mapsto x^{-1}$ такими, что $(xy)z = x(yz)$, $xx^{-1}x = x$ и выполняются первые три тождества, приведенные в этой задаче. То, что силится определить Мальцев в своей книге, представляет собой группы в сигнатуре инверсных полугрупп. Для этого он добавляет аксиому $xx^{-1}y = y = yxx^{-1}$ для любых $x, y \in G$.

Задача. Докажите, что если в инверсной полугруппе выполняется тождество $xx^{-1}y = y = yxx^{-1}$, то для любых $x, y \in G$ имеем $xx^{-1} = yy^{-1}$.

Типичным примером инверсной полугруппы является **симметрическая инверсная полугруппа**. Пусть X — произвольное множество. Рассмотрим множество J_X всех биективных *частичных* преобразований $X \dashrightarrow X$, т. е. объединение всех $\mathrm{Bij}(Y, Z)$, где $Y, Z \subseteq X$, включая, разумеется, пустую биекцию $\varnothing \in \mathrm{Bij}(\varnothing, \varnothing)$. Тогда относительно композиции частичных отображений J_X образует инверсную полугруппу. При этом инверсным к преобразованию $\phi \in \mathrm{Bij}(Y, Z)$ является обратное преобразование $\phi^{-1} \in \mathrm{Bij}(Z, Y)$. Эта инверсная полугруппа универсальна в том смысле, что имеет место следующий аналог теоремы Кэли — называемый в этом случае **теоремой Вагнера—Престона** — произвольная инверсная полугруппа G вкладывается в симметрическую инверсную полугруппу J_G.

В отличие от произвольных полугрупп инверсные полугруппы допускают весьма глубокую структурную теорию. Петербургским математикам Иосифу Соломоновичу Понизовскому и Анатолию Владимировичу Руколайне удалось построить чрезвычайно красивую теорию представлений конечных инверсных полугрупп, полностью параллельную обычной теории представлений конечных групп.

2. Группоиды. Еще одно важнейшее обобщение понятия группы было предложено в 1927 году Брандтом [139] и Лёви [140].

Альфред Лёви (`Alfred Loewy`, 20 июня 1873, Равитч, ныне Равич под Познанью — 25 января 1935, Фрайбург) — замечательный немецкий математик, основные работы которого относятся к теории групп, теории представлений и теории дифференциальных уравнений. Начиная с 1897 года он работает во Фрайбургском университете и в 1919 году становится там профессором, однако в 1933 году подпадает под действие расовых законов и вынужден досрочно уйти на пенсию. Одним из самых известных его сочинений является *Lehrbuch der Algebra*.

Брандт называл получающееся при этом понятие **группоидами**, а Лёви — **смешанными группами** (`Mischgruppen`), но А. К. Сушкевич заметил, что это одно и то же [**178**]. Некоторые писатели довольно долго настаивали на употреблении термина **группоид** в смысле **бинар**, т. е. множество с одной произвольной (но всюду определенной) бинарной операцией. При этом группоиды в смысле Брандта назывались **группоидами Брандта**. Однако в настоящее время употребление термина **группоид** в любом другом смысле, кроме **группоид Брандта**, рассматривается как красноречивое свидетельство **ретардации**.

Проще всего определить группоиды в терминах категорий. Группа представляет собой категорию с одним объектом, все морфизмы которой являются изоморфизмами. Определить **группоид** на таком языке гораздо проще — это любая категория, в которой все морфизмы являются изоморфизмами! Иными словами, для любого морфизма x существует единственный обратный морфизм x^{-1}, для которого xx^{-1} и $x^{-1}x$ представляют собой тождественные морфизмы. Однако, вообще говоря, это два разных тождественных морфизма e и f разных объектов!

Перевод этого понятия обратно на теоретико-множественный язык с непривычки выглядит достаточно коряво. Итак, **группоид** G является множеством с одной *частичной* бинарной операцией $\mathrm{mult} : X \times X \dashrightarrow X$, $(x, y) \mapsto xy$, удовлетворяющей следующим аксиомам.

Gr1. Сильная ассоциативность: Для любых $x, y, z \in G$ имеют место следующие утверждения.

• Если оба произведения xy и yz определены, то произведения $(xy)z$ и $x(yz)$ тоже определены и имеет место равенство $(xy)z = x(yz)$.

• Если оба произведения xy и $(xy)z$ определены, то произведения yz и $x(yz)$ тоже определены и имеет место равенство $(xy)z = x(yz)$.

• Если оба произведения yz и $x(yz)$ определены, то произведения xy и $(xy)z$ тоже определены и имеет место равенство $(xy)z = x(yz)$.

Gr2. Для любого $x \in G$ существует единственное $x^{-1} \in G$ такое, что для него

• оба произведения $e = xx^{-1}$ и $f = x^{-1}x$ определены,

• при этом выполняются тождества $e^2 = e$, $f^2 = f$, $ex = x = xf$ и $x^{-1}e = x^{-1} = fx^{-1}$.

Сам Брандт требовал, кроме того, чтобы группоид был **связен**, т. е. чтобы все объекты категории были изоморфны. На теоретико-множественном языке это значит, что выполняется следующая аксиома.

Gr3. Для любых двух идемпотентов $e, f \in G$ существует хотя бы один элемент $x \in G$ такой, что оба произведения ex и xf определены и равны x.

В настоящее время это требование обычно не включается в определение группоида.

Задача. Докажите, что в равенстве $xy = z$ каждый из трех элементов однозначно определяется двумя другими.

Как обычно, группа представляет собой группоид с единственным идемпотентом. Изучение группоидов в общем случае эквивалентно изучению инверсных полугрупп.

Задача. Докажите, что если добавить к группоиду G не принадлежащий ему элемент 0 и ввести на множестве $G^0 = G \cup \{0\}$ всюду определенное умножение, полагая $0x = 0 = x0$ для всех $x \in G^0$, и $xy = 0$ каждый раз как $x, y \in G$, и их

произведение не определено в G, то G^0 превращается в инверсную полугруппу. Чему равно 0^{-1}?

Получающаяся таким образом инверсная полугруппа называется **полугруппой Брандта**.

В природе группоиды возникают, например, так. Как и в § 17 рассмотрим топологическое пространство X. Определение фундаментальной группы зависит от выбора точки $x \in X$. Устранить эту зависимость можно, если не фиксировать точку x, а рассматривать гомотопические классы всевозможных путей, начинающихся и заканчивающихся в различных точках! При этом, конечно, произведение двух путей определено не всегда, а только если конец первого из них совпадает с началом второго. Обратным к пути является тот же путь, проходимый в обратном направлении, а идемпотентами будут в точности постоянные пути e_x, $x \in X$. Получающийся так группоид называется **фундаментальным группоидом** пространства X, он связен в том и только том случае, когда пространство X линейно связно. Для фундаментальных группоидов выполняются аналоги всех обычных утверждений о фундаментальных группах, например, теорема ван Кампена. Многие математики, в том числе Александр Гротендик и Рональд Браун учат, что именно фундаментальный группоид, а не фундаментальная группа является правильным понятием, с которого должен начинаться курс алгебраической топологии.

3. Гипергруппы. Самое интересное, но и самое трудное обобщение понятия группы получится, если отказаться от требования однозначности произведения. Разумеется, недостаточно просто констатировать, что произведение двух элементов определено неоднозначно. Структура **гипергруппы** на множестве G задается тем, что для любых трех элементов $x, y, z \in G$ указывается *вероятность* m^z_{xy}, с которой произведение xy принимает значение z. В терминах этих вероятностей естественно выражаются аналоги аксиом группы. Фактически это понятие находится между понятием группы и алгебры. В конечном случае понятие гипергруппы теснейшим образом связано с изучаемым в алгебраической комбинаторике **схемами отношений**. Разумеется, еще интересней это понятие в бесконечном случае, где гипергруппы определяются в терминах свертки вероятностных мер.

There is much Obi-Wan did not tell you.

Darth Vader

Глава 2. ПОДГРУППЫ И СМЕЖНЫЕ КЛАССЫ

В предыдущей главе мы обсуждали контекст, примеры и приложения. Теперь мы начинаем систематически конкретизировать для групп основные конструкции общей алгебры. В этой и двух следующих главах мы определим

- подобъекты,
- фактор-объекты,
- морфизмы.

В настоящей главе мы изучим подгруппы и свяжем с каждой подгруппой два отношения эквивалентности.

§ 1♢. Подгруппы

Подобъект группы называется подгруппой. Определение подгруппы позволит нам еще раз задуматься над тем, сколько, все-таки, операций в группе.

1. Подгруппы. Напомним, что структура группы на G определяется **тремя** операциями: бинарной операцией умножения, унарной операцией взятия обратного и нульарной операцией e. Следующее понятие было введено Галуа.

Определение. *Подмножество $H \subseteq G$ называется* **подгруппой** *в G, если оно само является группой относительно тех же операций. Иными словами, для того, чтобы H было подгруппой, необходимо выполнение следующих трех условий:*

i) $h, g \in H \Longrightarrow hg \in H$,

ii) $h \in H \Longrightarrow h^{-1} \in H$,

iii) $e \in H$.

В терминах книги I это означает, что подгруппа **замкнута** относительно произведения, перехода к обратному и нейтрального элемента. Чтобы подчеркнуть, что H является подгруппой в G, а не просто подмножеством, в этом случае вместо $H \subseteq G$ обычно пишут $H \leq G$. В современных текстах термин *подгруппа* (`subgroup`, `Untergruppe`, `sous-groupe`, `sottogruppo`) является единственно употребительным. В то

же время, в немецких и французских текстах XIX века подгруппы, особенно подгруппы конечных групп, часто назывались *делителями* (`T(h)eiler`, `diviseur`), этот архаизм до сих пор сохранился в выражении *нормальный делитель* (`Normalteiler`). Запись $G \geq H$ имеет тот же смысл, что и $H \leq G$, любая группа G, содержащая H в качестве подгруппы, называется **надгруппой** H. Заметим, что правильный перевод этого термина на английский — `overgroup`, употребление в этом контексте термина `supergroup` производит на понимающего человека совершенно анекдотическое впечатление.

Непустое подмножество группы, удовлетворяющее условию i) называется **подполугруппой**, а условию ii) — **симметричным** подмножеством. Условия i) и ii) независимы. Пусть, например, $G = \mathbb{Z}^+$ — аддитивная группа целых чисел. Тогда $\mathbb{N}^+$ является подполугруппой в $\mathbb{Z}^+$, а $\{\pm 1\}$ — симметричным подмножеством, но, очевидно, ни то ни другое множество не является подгруппой. Для конечных групп аналог первого из этих примеров построить не удастся.

Задача. Проверьте, что если группа G периодическая (например, конечная), то для того, чтобы убедиться в том, что непустое подмножество $H \subseteq G$ подгруппа в G, достаточно проверить условие i).

В то же время, для *непустых* подмножеств условие iii) автоматически вытекает из условий i) и ii). В самом деле, если $H \neq \varnothing$, то найдется $h \in H$ так что $h^{-1} \in H$ по ii) и, значит, $e = hh^{-1} \in H$ по i). Поэтому часто в определении подгруппы условие iii) заменяется более слабым условием $H \neq \varnothing$.

Мы знаем из главы 1, что как произведение, так и взятие обратного выражаются через операцию левого деления. Поэтому условия i) и ii) можно объединить в одно условие: подгруппа замкнута относительно *левого* деления, т. е.

iv) $h, g \in H \Longrightarrow h^{-1}g \in H$.

Разумеется, это эквивалентно замкнутости H относительно *правого* деления:

v) $h, g \in H \Longrightarrow hg^{-1} \in H$.

2. Произведение подмножеств группы. Пусть $X, Y \subseteq G$ — два подмножества группы. Тогда **произведением** XY называется их *произведение по Минковскому*

$$XY = \{xy \mid x \in X, y \in Y\}.$$

Аналогично, множество

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

— это **обратное по Минковскому** к множеству X.

В терминах этих операций определение подгруппы выглядит следующим образом. Условие i) означает, что $HH \subseteq H$, а условие ii) — что $H^{-1} \subseteq H$. Разумеется, если для непустого множества H выполнены *оба эти условия*, то включения здесь можно заменить на равенства, так как тогда $1 \in H$. На самом деле, как мы знаем, достаточно даже требовать лишь выполнения включения $HH^{-1} \subseteq H$.

§ 2♢. Первые примеры подгрупп

1. Простейшие примеры. Приведем несколько простейших примеров подгрупп. В дальнейшем мы встретим много гораздо более интересных примеров в группах перестановок, группах матриц и т. д.

• **Тривиальная и несобственная подгруппы.** В каждой группе G есть по крайней мере две подгруппы. А именно, очевидно, что $\{e\} \leq G$. Эта подгруппа называется **тривиальной** и часто обозначается просто e или 1, а в случае аддитивной записи, естественно, 0; обычно это не ведет к недоразумениям. Столь же очевидно, что $G \leq G$. Эта подгруппа называется **несобственной**. Все подгруппы $H < G$, отличные от G, называются **собственными**. Подгруппы 1 и G называются **очевидными** подгруппами группы G. Заметим, что в случае $G = 1$ эти подгруппы совпадают.

• Любая подгруппа в $\mathbb{Z}^+$ имеет вид $m\mathbb{Z}$ для некоторого $n \in \mathbb{Z}$.

• Любая подгруппа в $\mathbb{Q}^+$ имеет вид

$$A_M = \{x \in \mathbb{Q} \mid \forall p \in \mathbb{P}, v_p(x) \geq m_p\},$$

для некоторого семейства $M = (m_p)_{p\in\mathbb{P}}$ элементов множества $\{-\infty\} \sqcup \mathbb{Z} \sqcup \{\infty\}$, индексированное натуральными простыми, а v_p — p-адический показатель, который определен в главе 4.

• Знакопеременная группа является подгруппой симметрической группы: $A_n \leq S_n$.

• Много примеров подгрупп $\mathrm{GL}(n, K)$ приведено в книгах IV и IIbis, для $n = 2$ некоторые из этих примеров уже встречались нам в главе 1.

• **Транзитивность.** Пусть $F \leq H \leq G$. Тогда $F \leq G$. В частности, $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$ являются подгруппами в $\mathbb{C}^+$.

• **Положительные числа.** Произведение двух положительных чисел положительно, обратное к положительному числу положительно, поэтому $\mathbb{R}_+ = \{\lambda \in \mathbb{R} \mid \lambda > 0\}$ — подгруппа в $\mathbb{R}^*$.

• **Подгруппы Q.** Всего в группе кватернионов Q имеется 6 подгрупп, из которых следующие 4 неочевидные:

$$\{\pm 1\},\quad \{\pm 1,\pm i\},\quad \{\pm 1,\pm j\},\quad \{\pm 1,\pm k\}.$$

• **Подгруппы $\mathbf{S_4}$.** Всего в группе S_4 имеется 24 подгруппы, из которых 22 неочевидных. Перечислим эти подгруппы с точностью до сопряженности (i,j,h,k здесь обозначают попарно различные индексы):

- 6 циклических подгрупп порядка 2, вида $\{e,(ij)\}$;
- 3 циклических подгруппы порядка 2, вида $\{e,(ij)(hk)\}$;
- 4 циклических подгруппы порядка 3, вида $\{e,(ijh),(hji)\}$;
- 3 циклических подгруппы порядка 4, вида

$$\{e,(ijhk),(ih)(jk),(ikhj)\};$$

- 1 нециклическая подгруппа порядка 4, а именно, четверная группа

$$V=\{e,(12)(34),(13)(24),(14)(23)\};$$

- 4 подгруппы порядка 6, изоморфных S_3, а именно,

$$\{e,(ij),(ih),(jh),(ijh),(hji)\};$$

- 1 подгруппа порядка 12, а именно знакопеременная группа

$$A_4=\{e,(123),(132),(124),(142),(134),(143),(234),(243),\\ (12)(34),(13)(24),(14)(23)\}.$$

Упражнение. Проследите, какие их этих подгрупп содержатся в A_4.

Еще несколько аналогичных примеров детально разбираются в § 9 в связи с описанием решетки подгрупп.

2. Центр. Множество элементов, коммутирующих со всеми элементами G, называется **центром** группы G и обозначается $C(G)$ (от английского `centre` или американского `center`):

$$C(G)=\{g\in G\mid \forall x\in G, gx=xg\}.$$

В старинных книгах центр обычно обозначается через $Z(G)$ (от немецкого `Zentrum`). Элементы $C(G)$ называются **центральными**. Легко

видеть, что $C(G) \leq G$. В действительности, как мы узнаем в главе 3, центр является даже *нормальной* подгруппой, $C(G) \trianglelefteq G$. Любая подгруппа $H \leq C(G)$ называется **центральной подгруппой** в G. Группа G в том и только том случае абелева, когда $G = C(G)$. Группа G, для которой $C(G) = 1$, называется группой **с тривиальным центром** или, без затей, **группой без центра**. Например, центр неабелевой простой группы тривиален.

- $C(S_n) = 1$ для $n \geq 3$
- $C(A_n) = 1$ для $n \geq 4$
- $C(\mathrm{GL}(n, R)) = R^*e$ — скалярные матрицы

§ 3◇. Централизатор элемента

В этом и следующем параграфах мы введем несколько конструкций, которые позволят строить много интересных примеров подгрупп в неабелевых группах.

1. Централизатор элемента. Пусть $x \in G$. Определим **централизатор** элемента x в группе G следующим образом:

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Легко проверить, что $C_G(x) \leq G$.

Лемма. *Для любого $x \in G$ имеем $C_G(x) \leq G$.*

Доказательство. В самом деле, $x1 = x = 1x$, поэтому $C_G(x) \neq \varnothing$. Если $h, g \in C(G)$, то $(hg)x = h(gx) = h(xg) = (hx)g = (xh)g = x(hg)$, так что $hg \in C(G)$. С другой стороны, если $h \in C(G)$, то умножая равенство $hx = xh$ на h^{-1} справа и слева, получаем $xh^{-1} = h^{-1}x$, так что $h^{-1} \in C(G)$.

Отсюда, конечно, сразу следует, что $C(G) \leq G$. В самом деле, $C(G) = \bigcap C_G(x)$, где пересечение берется по всем $x \in G$. Как мы узнаем в § 5, любое пересечение подгрупп является подгруппой.

Задача. Убедитесь, что если $H \leq G$, $x \in H$ и $g \in G$, то i) $C_G(x^g) = C_G(x)^g$, ii) $C_H(x) = G_G(x) \cap H$.

2. Примеры централизаторов. Вычислим централизаторы некоторых матриц.

• **Централизатор регулярной полупростой матрицы**. Диагональная матрица $d = \mathrm{diag}(\varepsilon_1, \ldots, \varepsilon_n)$ называется **регулярной**, если все элементы ε_i попарно различны. Для регулярной диагональной

матрицы имеет место равенство

$$C_{\mathrm{GL}(n,K)}(\mathrm{diag}(\varepsilon_1,\dots,\varepsilon_n)) = D(n,K)$$

(так как диагональные матрицы коммутируют, то $D(n,K)$ содержится в централизаторе любой диагональной матрицы. Проверьте, что если диагональная матрица d регулярна, то она не может коммутировать с матрицей $x=(x_{ij})$ у которой $x_{ij}\neq 0$ для каких-то $i\neq j$.)

• **Централизатор регулярной унипотентной матрицы**. Проверьте, что

$$C_{\mathrm{GL}(n,K)}\begin{pmatrix} 1 & 1 & \dots & 0 & 0\\ 0 & 1 & \ddots & 0 & 0\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ 0 & 0 & \dots & 1 & 1\\ 0 & 0 & \dots & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b & \dots & c & d\\ 0 & a & \ddots & \ddots & c\\ \vdots & \vdots & \ddots & \ddots & \vdots\\ 0 & 0 & \dots & a & b\\ 0 & 0 & \dots & 0 & a \end{pmatrix}.$$

Комментарий. Заметьте, что, как и в предыдущем примере, размерность централизатора равна n. При этом слово `размерность` здесь можно понимать *по любому*: как размерность линейной оболочки; как вещественную/комплексную размерность, если $K=\mathbb{R}$ или $\mathbb{C}$; как размерность в топологии Зариского для бесконечного поля K, или любым другим осмысленным образом. Оказывается, централизатор матрицы не может иметь размерность меньше n (матрица, централизатор которой имеет размерность n, называется **регулярной**). Однако легко построить примеры матриц, для которых централизатор имеет большую размерность.

• **Централизатор матрицы с двумя собственными числами**. Теперь пусть $p+q=n$, а $\varepsilon,\eta\in K^*$, $\varepsilon\neq\eta$. Проверьте, что

$$C_{\mathrm{GL}(n,K)}\begin{pmatrix} \varepsilon e_p & 0\\ 0 & \eta e_q \end{pmatrix} = \begin{pmatrix} \mathrm{GL}(p,K) & 0\\ 0 & \mathrm{GL}(q,K) \end{pmatrix}.$$

§ 4♢. Централизаторы, нормализаторы и соизмерители

1. Централизатор подмножества. Пусть теперь $X\subseteq G$ — любое подмножество в G. Определим **централизатор** X как $C_G(X)=\bigcap C_G(x)$, где пересечение берется по всем $x\in X$. Иными словами, $C_G(X)$ состоит из всех элементов, *поэлементно* коммутирующих с X:

$$C_G(X)=\{g\in G\mid \forall x\in X, gx=xg\}.$$

Так как пересечение любого семейства подгрупп само является подгруппой, $C_G(X)$ — подгруппа в G.

2. Нормализатор подмножества. Пусть снова $X \subseteq G$ — любое подмножество в G. Определим **нормализатор** X как множество элементов, которые коммутируют с X *в целом*:

$$N_G(X) = \{g \in G \mid gX = Xg\}.$$

Понятие нормализатора (но не соответствующий термин!) было введено Силовым [141]. Точно так же, как в пункте 2 легко убедиться, что $N_G(X)$ подгруппа в G. Совершенно ясно, что для одноэлементных подмножеств нормализатор совпадает с централизатором: если $X = \{x\}$, то $N_G(\{x\}) = C_G(x)$. В общем случае $C_G(X) \leq N_G(X)$. Как мы узнаем в следующей главе, в действительности, даже $C_G(X) \trianglelefteq N_G(X)$.

Много содержательных примеров вычисления нормализатора обсуждается в главе 5 и в книге IIbis. Вот три типичных ситуации.

• Нормализатор группы верхних унитреугольных матриц совпадает с группой верхних треугольных матриц, $N_{\mathrm{GL}(n,K)}(U(n,K)) = B(n,K)$. Замечательно, что это верно вообще для любого поля K.

• Нормализатор группы диагональных матриц совпадает с группой мономиальных матриц, $N_{\mathrm{GL}(n,K)}(D(n,K)) = N(n,K)$. Это равенство имеет место для любого K содержащего по крайней мере 3 элемента.

• Группа мономиальных матриц является **самонормализуемой**, иными словами ее нормализатор снова совпадает с группой мономиальных матриц: $N_{\mathrm{GL}(n,K)}(N(n,K)) = N(n,K)$. Это равенство имеет место для любого поля K содержащего по крайней мере 4 элемента.

Задача. Пусть $F, H \leq G$. Тогда $N_G(F) \cap N_G(H) \leq N_G(F \cap H)$. Всегда ли здесь имеет место равенство?

3. Соизмеритель подгруппы. В § 10 мы введем понятие соизмеримости подгрупп. В терминах соизмеримости можно определить следующий вариант понятия нормализатора. А именно, пусть $H \leq G$ — подгруппа в G. Определим **соизмеритель** $\mathrm{Comm}_G(H)$ подгруппы H как множество элементов $g \in G$, таких, что gHg^{-1} соизмерима с H. Соизмерители играют громадную роль в теории решеток в группах Ли [**322**], [142].

Задача. Проверьте, что $\mathrm{Comm}_G(H)$ — группа, содержащая $N_G(H)$.

§ 5◇. Порядок элемента и экспонента группы

1. Степени элемента, циклические подгруппы. Если G — любая группа, то мы можем определить степень любого элемента $g \in G$ с любым целым показателем. В самом деле, $g^0 = e$ и g^n, $n \in \mathbb{N}$, уже были определены ранее для любого моноида, а теперь для любого $n \in \mathbb{N}$ мы можем дополнительно положить $g^{-n} = (g^{-1})^n = (g^n)^{-1}$.

Ясно, что для любых $m, n \in \mathbb{Z}$ имеет место равенство $g^{m+n} = g^m g^n$. Таким образом, множество $\{g^n \mid n \in \mathbb{Z}\}$ всех степеней элемента g в действительности образует подгруппу группы G. Так как любая подгруппа, содержащая g обязана содержать также все степени g, то это *наименьшая* подгруппа, содержащая g. Эта подгруппа обозначается $\langle g \rangle$ и называется **циклической подгруппой** в G, порожденной элементом g.

Порядок $|\langle g \rangle|$ циклической подгруппы $\langle g \rangle$ обозначается через $o(g)$ или $\mathrm{ord}(g)$ (от английского `order`) и называется **порядком** элемента g. Иными словами, $o(g)$ это либо *наименьшее* натуральное число n такое, что $g^n = 1$, либо ∞. Если порожденная g подгруппа бесконечна, то говорят, что g — элемент **бесконечного порядка** и пишут $o(g) = \infty$, в противном случае g называется элементом **конечного порядка**. Группа G называется **периодической**, или **группой кручения**, если все ее элементы имеют конечный порядок. Группа G называется **группой без кручения**, если все ее неединичные элементы имеют бесконечный порядок.

2. Элементы конечного порядка. Приведенные в следующих задачах свойства порядка постоянно используются в дальнейшем без всяких специальных ссылок.

Задача. Докажите, что если $g^m = 1$, то $o(g) | m$.

Решение. Деление с остатком в $\mathbb{Z}$. Если $o(g) \not| m$, то поделив m с остатком на $o(g)$, мы видим, что $m = q \cdot o(g) + r$, где $0 < r < o(g)$. Тогда $1 = g^m = (g^{o(g)})^q g^r = g^r$, что противоречит минимальности $o(g)$.

Задача. Пусть $f : H \longrightarrow G$ — гомоморфизм групп. Покажите, что если $h \in H$ — элемент конечного порядка, то $f(h)$ — тоже элемент конечного порядка и $o(f(h))$ делит $o(h)$.

Теорема. *Пусть G — произвольная группа, $g \in G$, $o(g) = n$. Тогда порядок элемента g^m равен $n/\gcd(m, n)$.*

Доказательство. Как мы только что выяснили, порядок элемента g^m — это наименьшее натуральное число k такое, что $(g^m)^k = g^{mk} = e$. Так как $o(g) = n$, это означает, что $n | mk$, или, что то же самое, $nq = mk$ для некоторого $q \in \mathbb{Z}$. Последнее равенство можно сократить на $d = \gcd(m, n)$ и заключить, что $(n/d)q = (m/d)k$, т. е. $(n/d) | (m/d)k$. Так как $\gcd(m/d, n/d) = 1$, отсюда следует, что k делится на n/d. Но наименьшее натуральное число с таким свойством и есть n/d, таким образом, действительно, $o(g^m) = n/\gcd(m, n)$.

3. Инволюции. Особенно большое значение в теории конечных групп имеют элементы порядка 2, которые обычно называются **инволюциями**.

Задача. Пусть $A = \{g_1, \dots, g_n\}$ — конечная абелева группа. Покажите, что тогда $o(g_1 \dots g_n) \leq 2$.

Теорема Вильсона. *Если $p \in \mathbb{P}$ простое, то* $(p-1)! \equiv -1 \pmod{p}$.

Доказательство. Примените результат предыдущей задачи к группе $A = (\mathbb{Z}/p\mathbb{Z})^*$.

сэр Джон Уилсон (`sir John Wilson`, 1741, Applethwaite, Вестморленд — 1793, Kendal, ibid.) — английский юрист, врач и математик-любитель. В математике Уилсон занимался главным образом теорией чисел. Сформулированная Лейбницем и доказанная Лагранжем теорема Вильсона является единственным результатом, связанным с его именем.

Обычно фамилия `Wilson` *ошибочно* передается по-русски как **`Вильсон`** — ну да, `Watson` переводится как **`Ватсон`**, `Wallis` — как **`Валлис`**, `Waring` — как **`Варинг`** и пр. Мы сознательно сохраняем это традиционное написание, чтобы отличать сэра Джона Вильсона от одного из ведущих современных специалистов по теории бесконечных групп **Джона Уилсона** (`J. S. Wilson`), несколько теорем которого упоминаются в книге IIbis.

Следующий незамысловатый факт является отправной точкой классификации конечных простых групп.

Задача. Покажите, что в каждой группе четного порядка нечетное число инволюций. В частности, в этой группе есть хотя бы одна инволюция!

Задача. Докажите, что группа, в которой все $\neq 1$ элементы являются инволюциями, абелева.

Решение. В самом деле, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

4. Экспонента. Наименьшее $m \geq 1$ такое, что $g^m = 1$ для всех $g \in G$, называется **экспонентой** или **показателем** группы G. Такого m может не существовать, но если оно существует, то говорят, что группа G имеет **конечную экспоненту** или **конечный показатель**. Для этого необходимо, чтобы порядки всех элементов были ограничены в совокупности. В этом случае экспоненту можно определить также как наименьшее общее кратное порядков элементов группы G.

Например, в последней задаче предыдущего пункта утверждается, что группа экспоненты 2 абелева. Конечная абелева группа экспоненты p является прямой суммой циклических групп порядка p, т. е. элементарной абелевой p-группой. Всякая группа конечной экспоненты

является группой кручения, но обратное неверно: группа μ_{p^∞} периодическая, но при этом порядки ее элементов не ограничены в совокупности.

§ 6♢. Подгруппа, порожденная подмножеством

В этом параграфе мы изложим важный общий метод построения подгрупп.

1. Подгруппа, порожденная подмножеством. Сейчас мы обобщим конструкцию из предыдущего пункта на произвольные подмножества в G.

Определение. *Пусть $X \subseteq G$. Наименьшая подгруппа в G, содержащая X, называется* **подгруппой, порожденной** X *и обозначается* $\langle X\rangle$.

Так как пересечение любого множества подгрупп снова является подгруппой, то $\langle X\rangle$ действительно существует, достаточно взять пересечение *всех* подгрупп в G, содержащих X. Эта подгруппа допускает вполне конкретное описание, подобное тому, которое дано в предыдущем пункте для циклической подгруппы. А именно, пользуясь обозначениями § 1, для любого подмножества $Y \subseteq G$ обозначим через Y^n множество всех произведений элементов множества Y по n штук:

$$Y^n = \{y_1 \dots y_n \mid y_i \in Y\}.$$

Тем самым $Y^0 = \{e\}$, $Y^1 = Y$, $Y^2 = YY$ и т. д. Обозначим через $M(Y)$ множество **всевозможных** произведений образующих Y, т. е. $M(Y) = \bigcup Y^n$, $n \in \mathbb{N}_0$.

Комментарий. Иногда я могу забыться и — как это принято среди специалистов по теории групп — назвать произведение элементов Y **(полугрупповым) словом** в этих образующих. Конечно, в действительности, такое произведение является не словом, а *образом* слова относительно некоторой специализации. Кроме того, в теории групп обычно рассматривают не полугрупповые, а **групповые слова**, в которые входят не только элементы множества Y, но и обратные к ним. Именно с этим с этим обстоятельством связано появление X^{-1} в формулировке следующей теоремы.

Теорема. *Для любого подмножества $X \subseteq G$*

$$\langle X\rangle = M(X \cup X^{-1}) = \{x_1 \dots x_n \mid x_i \in X \cup X^{-1}, n \in \mathbb{N}_0\}.$$

Доказательство. Докажем вначале, что подгруппа $\langle X\rangle$ содержится в $H = M(X \cup X^{-1})$. Для этого заметим, что H — подгруппа, содержащая X. В самом деле, по условию e является пустым произведением и, следовательно, принадлежит H. С другой стороны,

если $u = x_1 \dots x_m$ и $v = y_1 \dots y_n$ — два каких-то элемента H, то $uv = x_1 \dots x_m y_1 \dots y_n$ также принадлежит H. Тем самым, $HH \subseteq H$. Далее, для $u = x_1 \dots x_m$ имеем $u^{-1} = {x_m}^{-1} \dots {x_1}^{-1}$. Тем самым, $H^{-1} = H$. Это и значит, что H есть подгруппа. Так как по определению $\langle X \rangle$ — наименьшая среди всех подгрупп, содержащих X, то $\langle X \rangle \leq H$.

Обратно, пусть теперь F — любая подгруппа, содержащая X. Тогда $X^{-1} \subseteq F^{-1} = F$. Тем самым F содержит все слова длины ≤ 1 в образующих $X \cup X^{-1}$. Далее рассуждаем индукцией по длине слова. Любое слово $w \in (X \cup X^{-1})^n$ длины $n \geq 2$ в образующих $X \cup X^{-1}$ имеет вид $w = ux$, где $u \in (X \cup X^{-1})^{n-1}$ — слово длины $n-1$ в тех же образующих, а $x \in X \cup X^{-1}$. По индукционному предположению $u \in F$, а по базе индукции $x \in F$. Тем самым $w = ux \in FF \subseteq F$. Но это значит, что $F \geq H$. Поскольку это верно для любой подгруппы, содержащей X, то $\langle X \rangle \geq H$.

В случае, когда группа G конечна — или, более общо, периодическая — вместо групповых слов достаточно ограничиться полугрупповыми.

Задача. Пусть X состоит из элементов конечного порядка. Докажите, что тогда

$$\langle X \rangle = M(X) = \{x_1 \dots x_n \mid x_i \in X, n \in \mathbb{N}_0\}.$$

Задача. Пусть $H < G$. Покажите, что $\langle G \setminus H \rangle = G$.

§ 7♢. Produktformel

Чему равен порядок произведения двух подмножеств в группе? Для подгрупп ответить на этот вопрос довольно легко. Сейчас мы проведем соответствующее рассуждение, так как оно хорошо иллюстрирует, как именно используется тот факт, что какое-то подмножество является подгруппой.

1. Формула произведения. Следующий результат был получен Фробениусом в его работе про двойные смежные классы, в § 20 мы обобщим этот результат и получим аналогичную формулу для порядка класса FgH при любом $g \in G$.

Produktformel. *Если $F, H \leq G$ — подгруппы конечной группы G, то*

$$|FH| = \frac{|F| \cdot |H|}{|F \cap H|}.$$

Пояснение. Здесь **не** предполагается, что FH – подгруппа в G.

Доказательство. Рассмотрим отображение

$$\phi : F \times H \longrightarrow FH, \qquad (f, h) \mapsto fh.$$

Так как ϕ — сюръекция, то достаточно показать, что для любого $x \in FH$ слой $\phi^{-1}(X)$ состоит из $|F \cap H|$ элементов. В самом деле, пусть $x = fh$, где $f \in F$, $h \in H$. Покажем, что тогда

$$\phi^{-1}(x) = \{(fg, g^{-1}h) \mid g \in F \cap H\}.$$

Ясно, что правая часть содержится в левой. Обратно, пусть $x = f'h'$, где $f \in F$, $h \in H$. Тогда $fh = f'h'$ и, значит, по свойствам iv) и v) из § 1 имеем $g = f^{-1}f' = h(h')^{-1} \in F \cap H$. Таким образом, $f' = fg$, $h' = g^{-1}h$, как и утверждалось.

В дальнейшем мы постоянно пользуемся этим фактом и, в особенности, следующим его частным случаем.

Следствие. *Если порядки $|F|$ и $|H|$ взаимно просты, то $|FH| = |F| \cdot |H|$.*

Доказательство. В самом деле, $F \cap H = 1$.

В следующем параграфе и в § 18 мы обсуждаем, что можно сказать о произведении FH двух подгрупп F и H в случае, когда их *индексы* $|G : F|$ и $|F : H|$ взаимно просты.

Задача (H. B. Mann). Пусть G конечная группа, $X, Y \subseteq G$, — два произвольных (не обязательно различных!) подмножества. Докажите, что либо $G = XY$, либо $|G| \geq |X| + |Y|$.

Решение. Предположим, что $|X| + |Y| > |G|$. Тогда для любого $g \in G$ по формуле включения—исключения имеем

$$|X^{-1}g \cap Y| + |G| \geq |X^{-1}g \cap Y| + |X^{-1}g \cup Y| = |X| + |Y| > |G|.$$

Таким образом, $X^{-1}g \cap Y \neq \varnothing$ и, тем самым, найдутся $x \in X$, $y \in Y$ такие, что $x^{-1}g = y$ или, что то же самое, $g = xy$. Но это как раз и значит, что $G = XY$.

Следствие. *Каждый элемент конечного поля является суммой двух квадратов.*

Доказательство. Пусть $G = \mathbb{F}_q^+$. Если $q = 2^m$, то доказывать нечего. Если $q = p^m$, где p нечетно, то полагая в предыдущей задаче $X = Y = \mathbb{F}_q^2$, мы видим, что $|X| + |Y| = q + 1 > q = |G|$.

§ 8♢. Пересечение и порождение подгрупп

Сейчас мы обсудим две операции над подгруппами, которые превращают множество всех подгрупп группы G в решетку $L(G)$, называемую решеткой подгрупп.

1. Пересечение подгрупп. Пусть $F, H \leq G$. Тогда их теоретико-множественное *пересечение* $F \cap H$ тоже является подгруппой в G, которая — естественно! — называется **пересечением подгрупп** F и H. То же верно и для любого множества подгрупп.

Напротив, *объединение* двух подгрупп *крайне* редко является подгруппой. Конечно, если $F \leq H$ или $H \leq F$, то $F \cup H = H \leq G$ или $F \cup H = F \leq G$ соответственно. Однако, если подгруппы F и H несравнимы, то $F \cup H$ *никогда* не является подгруппой. В самом деле, пусть $x \in F \setminus H$ и $y \in H \setminus F$. Что означает условие $xy \in F \cup H$?

2. Подгруппа, порожденная подгруппами. Если $X, Y \subseteq G$ — два подмножества в G, то вместо $H = \langle X \cup Y \rangle$ обычно пишут просто $H = \langle X, Y \rangle$, при этом H называют **подгруппой, порожденной** X, Y или, коротко, **порождением** X и Y (это немецкого `Erzeugnis`). Этот термин несколько двусмыслен, но достаточно удобен, если, конечно, помнить, что его обратный перевод на английский это `span`, а вовсе не `generation`. То же обозначение используется и для любого конечного семейства $X_1, \ldots, X_n$ подмножеств в G. Порождение $\langle F, H \rangle$ особенно интересно в случае когда $F, H \leq G$. По определению, $\langle F, H \rangle$ — это наименьшая подгруппа, содержащая как F, так и H. Ясно, что $FH, HF \subseteq \langle F, H \rangle$. Подгруппа $\langle F, H \rangle$ иногда обозначается еще $F \vee H$ и в этом случае называется **джойном** (`join`) подгрупп F и H.

Задача. Покажите, что если $FH \subseteq HF$ или $HF \subseteq FH$, то, в действительности, $FH = HF = \langle F, H \rangle$.

3. Перестановочные подгруппы. Иными словами, последняя задача означает, что если две подгруппы **перестановочны** (`permute`, `commute as a whole`), $FH = HF$, то их произведение FH является подгруппой. Верно и обратное. В частности, как мы увидим в главе 3, это условие *заведомо* выполнено, если хотя бы одна из подгрупп H или F нормальна в G. Конечно, это тем более верно, если эти подгруппы **коммутируют** (`commute`, `commute element-wise`), т. е. $fh = hf$ для всех $f \in F$, $h \in H$. Следующие две задачи используют понятие индекса, которое вводится ниже в § 16.

Задача. Покажите, что подгруппы $F, H \leq G$ конечной группы G тогда и только тогда перестановочны, когда $|F : F \cap H| = |\langle F, H \rangle : H|$.

Задача. Ope, [143]. Пусть G — конечная группа, $F, H \leq G$. Предположим, что индексы $|G : F|$ и $|G : H|$ взаимно просты. Тогда $FH = HF = G$.

Ойстен Ope (Oystein Ore, 7 октября 1899, Кристиания, ныне Осло, — 13 августа 1968, Осло) — замечательный норвежский математик, основные работы которого относятся к алгебре, теории чисел и комбинаторике. Ope учился в Осло у Сколема и в Геттингене у Нетер. Однако в 1927 году он эмигрировал в США и уже через два года стал профессором в Йеле, где и работал до конца жизни, возвращаясь в Осло на лето. Основные работы Ope относятся к теории алгебраических чисел, теории колец и теории групп. В этой книге мы упоминаем несколько его теорем о группах, а в книге III встречаются кольца Ope, локализация Ope, теорема Ope и другие введенные им понятия, в частности, косые многочлены. Большая часть поздних работ Ope относится к теории графов и комбинаторике. Кроме 120 статей он написал 10 замечательных математических, исторических и научно-популярных книг, в том числе биографии Абеля и Кардано, *Приглашение в теорию чисел*, *Теория графов*, *Проблема четырех красок*. Некоторые из этих книг переведены на русский.

4. Квазинормальные подгруппы. В 1939 году O. Ope (ibid.), начал изучение подгрупп $H \leq G$ таких, что H перестановочна с любой подгруппой $F \leq G$. Сам Ope называл такие подгруппы **квазинормальными**[♮]. В предыдущем пункте замечено, что любая нормальная подгруппа квазинормальна. Обратное, вообще говоря, неверно, тем не менее квазинормальные подгруппы удовлетворяют несколько более слабому условию, которое мы обсуждаем в главе 4.

Теорема Ope. *Квазинормальная подгруппа субнормальна.*

Квазинормальность согласована с переходом к подгруппам и фактор-группам [144].

Задача. Если $H \leq G$ — квазинормальная подгруппа и $F \leq G$, то $H \cap F$ квазинормальна в F.

Задача. Пусть $F \leq H \leq G$, причем $F \trianglelefteq G$. Тогда H в том и только том случае квазинормальна в G, когда H/F квазинормальна в G/F.

5. Three for two. Следующее замечательно простое рассуждение [145], известное как **аргумент Томпсона** или **three for two**, имеет важные приложения.

Аргумент Томпсона. *Пусть G — группа, $H_1, H_2, H_3 \leq G$. Предположим, что для любой перестановки $\pi \in S_3$ выполняется включение $H_{\pi(1)} \subseteq H_{\pi(2)}H_{\pi(3)}$. Тогда произведение H_iH_j является подгруппой для всех $1 \leq i \neq j \leq 3$.*

Доказательство. Пусть, например, $i = 1$, $j = 2$, доказательство для остальных случаев аналогично. Нам достаточно проверить, что $H_2H_1 \subseteq H_1H_2$, так как

[♮]В настоящее время такие группы обычно называются permutable, но перевод этого термина на русский неочевиден, поэтому мы сохраняем оригинальный термин Ope.

отсюда вытекает, что H_1H_2 подгруппа. В самом деле,

$$H_2H_1 \subseteq (H_1H_3)(H_3H_2) = H_1H_3^2H_2 = H_1H_3H_2 \subseteq H_1(H_1H_2)H_2 = H_1^2H_2^2 = H_1H_2.$$

§ 9♡. Решетка подгрупп

1. Решетка подгрупп. Через $L(G) = \{H \leq G\}$ обозначается **решетка подгрупп** группы G относительно рассмотренных в предыдущем пункте операций пересечения $\cap$ и порождения $\vee$. Как мы знаем, буква `L` здесь является сокращением английского `Lattice`.

Задача. Докажите, что G в том и только том случае конечна, когда $L(G)$ конечна.

Во многих вопросах возникает не вся решетка подгрупп, которая может быть устроена весьма сложно, а какие-то ее части. Вот два важных примера:

• Через $\Theta(G)$ обозначается **структурная решетка** группы G, состоящая из всех нормальных подгрупп.

• Через $L(D, G)$ мы обозначаем решетку **промежуточных подгрупп** (от английского `intermediate subgroups`), т. е. подгрупп в G, содержащих D. В этих обозначениях $L(G) = L(1, G)$.

Предостережение. Ровно половина авторов использует обозначение прямо противоположное нашему, т. е. обозначает решетку подгрупп, промежуточных между D и G через $L(G, D)$!

В главе 4 мы докажем **теоремы о соответствии**, которые утверждают, в частности, что если $H \trianglelefteq G$, то $L(H, G) = L(G/H)$. В то же время, если H не является нормальной подгруппой, решетка $L(H, G)$ может быть устроена *сколь угодно сложно* и ее описание представляет собой одну из самых трудных проблем теории групп.

Задача. Изобразите решетку подгрупп $L(G)$ для случая, когда G одна из следующих десяти групп: C_4, C_6, V, S_3, $C_3 \times C_3$, C_8, Q, D_4 $C_4 \times C_2$, C_2^3.

Ответ. Перечислим неочевидные подгруппы этих групп и включения между ними. В первых пяти случаях нет вообще никаких включений между неочевидными подгруппами:

◦ C_4 — одна подгруппа порядка 2;

◦ C_6 — две, порядков 2 и 3;

◦ V — три, порядка 2;

◦ S_3 — четыре, три порядка 2 и одна порядка 3;

$\circ$ $C_3 \times C_3$ — четыре, все порядка 3.

Во всех остальных случаях такие включения есть:

$\circ$ C_8 — две, порядков 2 и 4, причем подгруппа порядка 2 содержится в подгруппе порядка 4;

$\circ$ Q — четыре, одна порядка 2 и 3 подгруппы порядка 4, см. § 2.

Три последних примера уже чуточку сложнее:

$\circ$ $C_4 \times C_2$ — шесть, три порядка 2 и три порядка 4. Если $D_4 = \langle x, y\rangle$, где $x^4 = y^2 = e$, то $xy = yx$ и подгруппами порядка 4 будут четверная группа $\langle x^2, y\rangle$ и две циклические группы, порожденные x и xy, в то время как x^2, y, x^2y порождают подгруппы порядка 2. Ясно, что все они содержатся в четверной группе, но вот каждая из циклических групп порядка 4 содержит единственную подгруппу порядка 2, а именно, $\langle x^2\rangle$.

$\circ$ D_4 — восемь, из них 5 порядка 2 и 3 порядка 4. Если $D_4 = \langle x, y\rangle$, где x и y — инволюции, то $xyxy = yxyx$ и подгруппами порядка 4 будут циклическая группа $\langle xy\rangle = \{e, xy, xyxy, yx\}$ и две четверные группы: $\{e, x, yxy, xyxy\}$ и $\{\varepsilon, y, xyx, xyxy\}$, в то время как подгруппы порядка 2 порождаются x, y, xyx, yxy и $xyxy$.

Нарисуйте все включения.

$\circ$ C_2^3 — четырнадцать, 7 порядка 2 и 7 порядка 4, все четверные. Если $D_4 = \langle x, y, z\rangle$, где x, y, x — три коммутирующие инволюции, то подгруппы порядка 2 порождаются x, y, z, xy, xz, yz и xyz, в то время как подгруппы порядка 4 имеют вид $\{e, x, y, xy\}$, $\{e, x, z, xz\}$, $\{e, y, z, yz\}$, $\{e, xy, xz, yz\}$, $\{e, x, yz, xyz\}$, $\{e, y, xz, xyz\}$, $\{e, z, xy, xyz\}$. Получающаяся картинка самодвойственна: не только каждая подгруппа порядка 4 содержит ровно 3 подгруппы порядка 2, но и обратно, каждая подгруппа порядка 2 *содержится* ровно в 3 подгруппах порядка 4.

Теперь Вы в состоянии ставить перед собой более амбициозные задачи.

Задача. Изобразите решетку подгрупп $L(G)$ для группы $\overline{T}(2, 2, 3)$ и всех групп порядка 16.

Следующие задачи предполагают знакомство с результатами § 12.

Задача. Докажите, что решетка $L(C_n)$ изоморфна решетке делителей n.

Задача. Изобразите решетку $L(D_n)$ подгрупп диэдральной группы D_n.

Указание. Ответ существенно зависит от четности n.

Вычислите еще несколько примеров, но не увлекайтесь: сложность нахождения всех подгрупп группы G и всех включений между ними растет невероятно быстро. Так, например, в 1967 году — уже с использованием компьютеров!!! — Иоахим Нойбюзер получил `хабилитацию` за работу [146], в которой найдены решетки подгрупп всех групп порядка ≤ 100 *кроме* групп порядков 64 и 96. Из главы 1 мы уже знаем, что это *трудные* порядки, в первой половине XX века достаточно серьезные профессионалы не могли перечислить *группы* этих порядков, что уж говорить о включениях между их *подгруппами*!

2. Модулярный закон. Самый важный факт о решетке подгрупп состоит в следующем

Закон Дедекинда. *Пусть $F, H, K \leq G$, причем $H \leq K$. Тогда*

$$FH \cap K = (F \cap K)H.$$

Доказательство. Ясно, что $(F \cap K)H \leq FH$ и $(F \cap K)H \leq KH \leq K$. Поэтому $(F \cap K)H \leq FH \cap K$. Обратно, пусть $x \in FH \cap K$. Запишем x в виде $x = fh$, где $f \in F$, $h \in H$. Ясно, что $f = xh^{-1} \in KH = K$. Таким образом, $x \in (F \cap K)H$.

Следствие 1 (модулярный закон). *Если в условиях теоремы*

$$FH = FK \qquad \text{и} \qquad F \cap H = F \cap K,$$

то $H = K$.

Доказательство. В самом деле,

$$K = FK \cap K = FH \cap K = (F \cap K)H = (F \cap H)H = H.$$

Стоит обратить внимание, что здесь речь идет о произведении, а не о порождении подгрупп F и H!

Следствие 2. *Если в условиях теоремы F и H перестановочны, то*

$$\langle F, H\rangle \cap K = \langle F \cap K, H\rangle.$$

Рихард Юлиус Вильгельм Дедекинд (Richard Julius Wilhelm Dedekind, 6 октября 1831, Брауншвейг — 12 февраля 1916, ibid.) — общепризнанный классик науки XIX века, непосредственный ученик Гаусса и Дирихле и близкий друг Римана, Дедекинд был одним из основоположников современной алгебры и алгебраической теории чисел. После обучения в Брауншвейге, где он увлекался главным образом химией и физикой, в 1850 году Дедекинд поступил в Университет Геттингена.

В 1858 году он начал преподавать в Eidgenossische Technische Hochschule в Цюрихе. Приняв это предложение Дедекинд начал длительную традицию, когда работа в Цюрихе была для немецких алгебраистов первым шагом для получения профессорской должности в Германии. После Дедекинда тем же путем прошли Фробениус, Гурвиц, Вебер, Минковский, Герман Вейль и многие другие. В 1862 году Дедекинд вернулся в Брауншвейгский политехнический институт, где работал до самой смерти. Дедекинд первым включил в университетский курс алгебры теорию полей и теорию Галуа, ввел понятия кольца и идеала.

Вместе с Кантором Дедекинд был творцом теории множеств. В развитии алгебры второй половины XIX века отчетливо прослеживаются два направления: линия Дедекинда и линия Кронекера. При этом Дедекинд выступал за неограниченное использование бесконечных конструкций и неконструктивных рассуждений, в то время как Кронекер (в духе начала XIX века) призывал *по возможности* ограничиваться финитными процессами — конечно, без эксцессов, свойственных конструктивистам XX века. Различие их взглядов отчетливо прослеживается в дедекиндовской теории идеалов и кронекеровской теории дивизоров. Впрочем, уже с 1920-х годов все профессиональные математики воспринимали эти подходы как дополнительные, а вовсе не как противоположные. Тот факт, что некоторые философские направления и сегодня противопоставляют конструктивную и неконструктивную точки зрения, свидетельствует о серьезной задержке умственного развития.

Дедекинд много размышлял над проблемами обоснования математики и ее преподавания и известен широкой публике главным образом своей порядковой конструкцией вещественных чисел (дедекиндовы сечения). В честь него названы дедекиндовы кольца, дедекиндовы решетки. В нашем курсе встречается множество его теорем: модулярный закон, теорема Кронекера—Дедекинда, формула Мебиуса—Дедекинда, лемма Дедекинда, лемма Дедекинда—Артина и т. д., а также *десятки* введенных им терминов: отображение, идеал, коммутатор, гамильтоновы группы, ... Дедекинд был узловой фигурой, соединившей все нити развития XIX века и передавшей их XX веку. Эмми Нетер по любому поводу говорила: es steht schon alles bei Dedekind — все это есть уже у Дедекинда.

§ 10♡. Максимальные подгруппы

В настоящем параграфе мы введем важнейший класс подгрупп — максимальные подгруппы. Этот класс подгрупп играет совершенно исключительную роль в теории групп, в особенности в теории *конечных* групп. Это связано с тем, что, во-первых, в конечных груп-

пах максимальные подгруппы *существуют* и многие доказательства основаны на редукции к максимальным подгруппам. Во-вторых, максимальные подгруппы являются коатомами решетки подгрупп $L(G)$, а пересечение в этой решетке — это обычное теоретико-множественное пересечение. Поэтому знание максимальных подгрупп является серьезной заявкой на исчерпывающий — или, по крайней мере, достаточный для большинства приложений — контроль над *всеми* подгруппами группы G.

1. Максимальные подгруппы. Собственная подгруппа H группы G называется **максимальной**, если она не содержится ни в какой строго большей подгруппе. Иными словами, $H < G$, и из того что $H \leq F \leq G$ вытекает, что либо $F = G$, либо $F = H$.

Упражнение. Любая подгруппа простого индекса максимальна.

Упражнение. Докажите, что если $H \leq G$ — максимальная подгруппа в G, то она либо нормальна, либо самонормализуема.

Решение. В самом деле, так как $H \leq N_G(H) \leq G$, либо $N_G(H) = G$, либо $N_G(H) = H$.

В действительности, любая максимальная подгруппа либо нормальна, либо абнормальна.

Задача. Докажите, что любая подгруппа *конечной* группы содержится в максимальной подгруппе.

В действительности, конечность здесь, ясное дело, ни при чем, но решить следующую задачу, если Вы не верите в аксиому выбора, Вам вряд ли удастся.

Задача. Докажите, что если $G = \langle H, X\rangle$, где $H \leq G$, а $X \subseteq G$, $|X| < \infty$, то H содержится в максимальной подгруппе.

Решение. Лемма Куратовского—Цорна.

Следствие. *Если G конечно порожденная группа, то в G существует хотя бы одна максимальная подгруппа.*

Без условия конечной порожденности это утверждение безнадежно неверно.

Задача. Докажите, что в аддитивной группе $\mathbb{Q}$ нет максимальных подгрупп.

Решение. Пусть H максимальная подгруппа в $\mathbb{Q}$. Ясно, что $H \neq 0$. Так как два любых рациональных числа соизмеримы, найдутся такое $x \in \mathbb{Q}$ и такое $n \in \mathbb{Z}$, что $x \notin H$, $nx \in H$. В силу максимальности H имеем $\frac{1}{n}H = \mathbb{Q}$. Но тогда $H = \mathbb{Q}$, противоречие.

Вопрос. Как Вы думаете, почему никто специально не вводит *минимальные* подгруппы в G?

Ответ. Потому что минимальные подгруппы — это в точности циклические подгруппы простых порядков, и они, конечно же, так и называются.

2. Maximal subgroup classification project. Один из основных вопросов *конкретной* теории групп состоит в описании максимальных подгрупп группы G. Только после исчерпывающего ответа на этот вопрос мы можем утверждать, что мы понимаем, как устроена группа G. Для достаточно неабелевой группы G полное описание ее максимальных подгрупп представляет собой совсем непростую задачу. Более того, часто даже проверка максимальности совершенно конкретных подгрупп не может быть сегодня проведена внутренними средствами, а требует привлечения всей мощи геометрических методов. Приведем пару простейших примеров, десятки дальнейших примеров встретятся нам в главе 5 и книге IIbis:

- группы $B(2,K)$ и $B^-(2,K)$ максимальны в $\mathrm{GL}(2,K)$ для любого K;
- группа $N(2,K)$ максимальна в $\mathrm{GL}(2,K)$ для любого $K \neq \mathbb{F}_3, \mathbb{F}_5$.

В последние 20–25 лет основные усилия многих лучших специалистов в области теории конечных групп — Майкла Ашбахера, Гари Зейтца, Мартина Либека, Яна Саксла, Роберта Уилсона, Питера Клейдмана, Донны Тестерман, Роберта Гуральника и многих других — были сфокусированы именно на описании максимальных подгрупп в конечных простых и близких к ним группах. Это направление получило название **maximal subgroup classification project**. В самых общих чертах полученные результаты состоят в следующем. Во-первых, имеется несколько явно описываемых серий претендентов на роль БОЛЬШИХ максимальных подгрупп примерно такого типа, как в приведенных выше примерах. Для симметрической и знакопеременной групп описать эти серии совсем просто, это так называемые **классы О'Нана—Скотта**: подгруппы Юнга, сплетения и экспоненцирования симметрических групп, аффинные группы в перестановочных представлениях и еще одна серия, связанная с конечными простыми группами. Для групп типа Ли описать эти серии тоже не слишком сложно и это будет сделано в книге IIbis. Во-вторых, имеется большое количество МАЛЕНЬКИХ максимальных подгрупп, связанных с неприводимыми представлениями почти простых групп. В отличие от больших подгрупп, никакого единого описания маленьких максимальных подгрупп не существует, но для каждой конкретной группы получение их явного списка представляет собой трудную, но решаемую задачу теории представлений. Более того, для многих приложений оказывается достаточно иметь даже не списки таких подгрупп, а лишь достаточно точные оценки на их порядки и количество.

§ 11♠. Подгруппа Фраттини

подгрупп группы G обозначается $\Phi(G)$ и называется **подгруппой Фраттини** [147] группы G. Если в группе G нет максимальных подгрупп, то $\Phi(G) = G$.

Задача. Докажите, что $\Phi(G) \trianglelefteq G$.

В действительности подгруппа Фраттини является даже характеристической подгруппой группы G, см. главу 4. Так как в любой конечной группе G существуют максимальные подгруппы, то $\Phi(G) \neq G$. Это значит, что если G — конечная простая группа, то $\Phi(G) = 1$.

Оказывается, подгруппа Фраттини допускает интересную характеризацию в терминах необразующих элементов группы G. Элемент

Джованни Фраттини (08 января 1852, Рим — 21 июля 1925, Рим) — выдающийся итальянский математик. Фраттини учился в университете Рима у Бельтрами и Кремона и уже в 1875 году получил **докторат**. После нескольких лет работы в школах на Сицилии и в Витербо в 1881 году он возвращается в Рим, где преподает в военной школе. Именно в это время (1883–1886 годы) он публикует статьи по теории групп, которые приносят ему всемирную известность. Эти статьи, посвященные транзитивным группам и порождению групп, содержат, в частности, определение подгруппы Фраттини и аргумент Фраттини. Остальные работы Фраттини относятся к дифференциальной геометрии. Из-за своего антиклерикализма Фраттини так никогда и не получил университетской позиции.

$g \in G$ называется **необразующим** для G, если его можно исключить из любой системы образующих группы G. Иными словами, из того, что $G = \langle X, g\rangle$, вытекает, что $G = \langle X\rangle$.

Теорема. *Подгруппа Фраттини $\Phi(G)$ совпадает с множеством необразующих элементов группы G.*

Доказательство. Докажем вначале, что каждый необразующий элемент g содержится в $\Phi(G)$. Если в G нет максимальных подгрупп, то доказывать нечего. Если же $H \leq G$ — максимальная подгруппа и $x \notin H$, то $\langle H, g\rangle = G$ в силу максимальности H. Но так как g необразующий, это значит, что $H = \langle H\rangle = G$, что невозможно.

Пусть, обратно, $g \in \Phi(G)$, а X — какое-то множество такое, что $\langle X, g\rangle = G$. Если $\langle X\rangle = G$, то по лемме Куратовского—Цорна существует подгруппа $H \leq G$ максимальная по отношению к свойству содержать X и не содержать g. Ясно, что $\langle H, g\rangle \geq \langle X, g\rangle = G$. Так как по самому определению H любая подгруппа, строго содержащая H, содержит g, то H максимальна в G. Тем самым, мы построили максимальную подгруппу в G, не содержащую g, что невозможно.

Примеры подгрупп Фраттини.

- $\Phi(\mathbb{Q}^+) = \mathbb{Q}^+$.
- $\Phi(\mu_{p^\infty}) = \mu_{p^\infty}$.
- $\Phi(\mathbb{Z}) = 0$.
- $\Phi(A_n) = 1$. Для $n \geq 5$ это сразу вытекает из простоты группы A_n.
- $\Phi(S_n) = 1$. Для доказательства этого можно, например, заметить, что для каждого $i = 1, \ldots, n$ его стабилизатор $\mathrm{Stab}_i \cong S_{n-1}$ максимален в S_n, а $\mathrm{Stab}_1 \cap \ldots \cap \mathrm{Stab}_n = 1$.

• $\Phi(U(n,K)) = [U(n,K),U(n,K)]$. Для доказательства этого можно, например, заметить, что подгруппа

$$U^r = \{u = (u_{ij}) \in U(n,K) \mid u_{r,r+1} = 0\}$$

максимальна в $U(n,R)$ (с научной точки зрения это в точности унипотентный радикал *минимальной* параболической подгруппы $P^r = \langle B, X_{r+1,r}\rangle$), а

$$U^1 \cap \ldots \cap U^{n-1} = [U(n,K),U(n,K)].$$

§ 12♢. Циклические группы и их подгруппы

Напомним, что группа G называется **циклической**, если она порождается одним элементом. Иными словами, это означает, что найдется такое $g \in G$, что каждый элемент группы G является степенью g, т. е. $G = \{g^n, n \in \mathbb{Z}\}$. По существу циклические группы изучали де Ферма, Эйлер и Гаусс, в связи с задачами теории чисел. Однако, явным образом класс циклических групп выделил Кэли, который и придумал название `cyclical group`. Но, конечно, *фактически* следующий результат был известен еще Эйлеру.

Теорема 1. *Каждая подгруппа циклической группы $G = \langle g\rangle$ является циклической.*

Доказательство. Пусть $H \leq G$. Если $H = e$, то она циклическая. Пусть поэтому $H \neq e$ и $g^m \in H$ для некоторого $m \neq 0$. Заменяя, если нужно, m на $-m$, можно считать, что $m \in \mathbb{N}$. Пусть $d \in \mathbb{N}$ — наименьшее натуральное число такое, что $g^d \in H$. Покажем, что тогда $H = \langle g^d\rangle$. В самом деле, пусть $g^m \in H$ для какого-то $m \in \mathbb{Z}$. Поделим m с остатком на d: $m = qd + r$, $0 \leq r < d$. Тогда $g^r = g^m(g^{qd})^{-1} \in H$, что противоречит минимальности d, если $r \neq 0$. Значит, $r = 0$ и все элементы H являются степенями g^d.

Отметим следующий важнейший частный случай этой теоремы.

Следствие. *Каждая подгруппа аддитивной группы $\mathbb{Z}$ имеет вид $n\mathbb{Z}$ для некоторого $n \in \mathbb{N}_0$.*

В частности, отсюда сразу вытекает классификация циклических групп.

Теорема 2. *Если циклическая группа G бесконечна, то она изоморфна $\mathbb{Z}$. Конечная циклическая группа G изоморфна $\mathbb{Z}/n\mathbb{Z}$, где $n = |G|$ — порядок G.*

Доказательство. Рассмотрим циклическую группу $G = \langle g \rangle$ и зададим гомоморфизм $\eta : \mathbb{Z} \longrightarrow G$, $m \mapsto g^m$. Так как группа G циклическая, этот гомоморфизм сюръективен. Обозначим через H ядро этого гомоморфизма. Согласно только что доказанному, $H = n\mathbb{Z}$ для однозначно определенного $n \in \mathbb{N}_0$. При $n = 0$ гомоморфизм η является изоморфизмом, так что $G \cong \mathbb{Z}$ и все степени образующей g попарно различны. В случае же $n > 0$ из теоремы о гомоморфизме (см. § 11 главы 4) сразу следует, что $G \cong \mathbb{Z}/\operatorname{Ker}(\eta) = \mathbb{Z}/n\mathbb{Z}$.

Если порядок $G = \langle g \rangle$ равен n, то $g^n = e$. Вообще, пусть $g^k = g^l$ для некоторых $k, l \in \mathbb{Z}$. Тогда $e = g^k(g^l)^{-1} = g^{k-l}$, так что $k - l$ делится на n или, что то же самое, $k \equiv l \pmod{n}$. Это значит, что в этом случае $G = \{e = g^0, g, g^2, \dots, g^{n-1}\}$. Это значит, что **порядок $\mathbf{o}(\mathbf{g})$ элемента** $g \in G$ может быть определен как наименьшее натуральное число такое, что $g^n = e$, или $o(g) = \infty$, если такого натурального числа не существует.

Рассмотрим теперь элемент g^m циклической группы $G = \langle g \rangle$ и выясним, какую подгруппу он порождает. Так как $g^0 = e$, можно считать, что $m \neq 0$. Если $G \cong \mathbb{Z}$ бесконечна, то, очевидно, g^m имеет бесконечный порядок и порождает подгруппу индекса $|m|$. Таким образом, в дальнейшем мы ограничимся случаем конечной циклической группы G порядка n. Этот вопрос уже был нами фактически рассмотрен в § 3 и сейчас мы сформулируем несколько важных результатов непосредственно вытекающих из доказанной там теоремы о порядке элемента g^m и только что доказанных теорем 1 и 2. В частности, так как образующими циклической группы G порядка n являются те и только те элементы, порядок которых равен n, мы сразу получаем такую характеризацию **функции Эйлера** φ.

Следствие 1. *Конечная циклическая группа $G = \langle g \rangle$ порядка n содержит $\varphi(n)$ образующих. Образующими G являются те и только степени g^m элемента g, для которых $\gcd(m, n) = 1$.*

Следствие 2. *Пусть $G = \langle g \rangle$ есть конечная циклическая группа порядка n. Тогда для каждого делителя d числа n в группе G существует единственная подгруппа порядка d.*

Доказательство. Пусть $d \mid n$, тогда $g^{n/d}$ порождает подгруппу порядка d. Обратно, пусть H — произвольная подгруппа порядка d. Для $d = 1$ доказывать нечего, поэтому в дальнейшем мы считаем, что $H \neq e$. Согласно теореме 1 мы уже знаем, что H циклическая, значит, $H = \langle g^m \rangle$ для некоторого m. По теореме порядок подгруппы, порожденной g^m, равен $d = n/\gcd(m, n)$. В частности, $(n/d) \mid m$. Это

значит, что $H = \langle g^m \rangle$ содержится в подгруппе, порожденной $g^{n/d}$, но, так как их порядки совпадают, $H = \langle g^{n/d} \rangle$.

Задача. Докажите, что единственными группами, у которых ровно две подгруппы, являются циклические группы простого порядка p.

Задача. Докажите, что единственными группами, у которых ровно три подгруппы, являются циклические группы порядка p^2, где p простое.

Задача. Докажите, что если $H \trianglelefteq G$ — нормальная циклическая подгруппа, то каждая подгруппа $F \leq H$ нормальна в G.

Комбинируя два предшествующих следствия, мы получаем следующий результат.

Следствие 3. *Пусть d — натуральный делитель порядка n конечной циклической группы $G = \langle g \rangle$. Тогда G содержит ровно $\varphi(d)$ элементов порядка d.*

Доказательство. Элементы порядка d в группе G — это в точности образующие единственной подгруппы порядка d. Как мы знаем из следствия 1, у циклической группы порядка d ровно $\varphi(d)$ образующих.

Заметим, что это следствие дает еще одно доказательство **сумматорной формулы** для функции Эйлера $\sum\limits_{d|n} \varphi(d) = n$. В самом деле, каждый элемент $h \in G$ конечной циклической группы порядка n имеет порядок $d \mid n$, причем число элементов порядка d равно $\varphi(d)$. Используя это наблюдение легко доказать, что в действительности следствие 2 характеризует циклические группы: если G конечная группа порядка n, в которой для каждого делителя d ее порядка существует не более одной подгруппы порядка d, то G циклическая.

Следствие 4. *Число элементов порядка m в любой конечной группе G делится на $\varphi(m)$.*

Доказательство. В самом деле, определим на G отношение эквивалентности, полагая $x \approx y$, если $\langle x \rangle = \langle y \rangle$. Но мы только что доказали, что каждый класс эквивалентности элементов порядка m содержит ровно $\varphi(m)$ элементов.

Следствие 2 можно сформулировать и чуть иначе.

Следствие 5. *Пусть $G = \langle g \rangle$ есть конечная циклическая группа порядка n. Тогда для каждого делителя d порядка n в G существует*

единственная подгруппа H индекса d. Фактор-группа G/H является циклической группой порядка d.

Доказательство. Согласно следствию 2 в группе G существует единственная подгруппа H порядка $(n/d) \mid n$, а именно, подгруппа, порожденная $g^{n/(n/d)} = g^d$. Ясно, что фактор-группа G/H порождена классом gH, причем $g^d \in H$.

§ 13♢. Системы образующих

1. Системы образующих. Пусть $H \leq G$. Любое подмножество $X \subseteq G$ такое, что $\langle X \rangle = H$ называется **системой образующих** alias **системой порождающих** группы H. Одним из наиболее простых и эффективных способов задания группы является задание какой-то ее системы образующих. В связи с этим возникают две противоположные проблемы.

• Найти группу H, зная какую-то систему ее образующих X. Особенно широко такой способ задания групп используется для описания конечных и дискретных групп. В пункте 2 мы приведем простейший пример порождения довольно большой (с обывательской точки зрения) группы двумя совсем простыми перестановками.

• Обратно, зная группу G, найти наиболее простые и/или удобные системы ее образующих. В пунктах 3–6 мы перечислим несколько очевидных (и несколько чуть менее очевидных!) примеров систем образующих известных групп.

2. Тасование Монжа. Следующий замечательный пример взят из [148]. Пусть d — делитель числа 12. Возьмем колоду из d карт, занумерованных $1, \dots, d$, и применим к ней две перестановки:

- **переворачивание**, т. е. отображение $i \mapsto d - i$;
- **тасование Монжа**, т. е. отображение $i \mapsto \min(2i, 2d + 1 - 2i)$.

Гаспар Монж (Gaspard Monge, 10 мая 1746, Beaune — 28 июля 1818, Париж) — французский геометр, основные работы которого относятся к дифференциальной и начертательной геометрии. Интересно, что основная идея начертательной геометрии возникла у него при разработке фортификационных планов еще во время обучения в военной академии. Этот метод был тут же объявлен военной тайной. Монж принимал активное участие во французской революции и в 1892–1893 годах был морским министром. Как друг Наполеона он стал директором Египетского музея и одного из самых престижных учебных заведений (grandes ecoles) во Франции, Ecole Polytechnique. Известие о поражении Наполеона в России вызвало у него инсульт, в 1815 году после реставрации Монж потерял все свои должности, а в 1816 году был исключен из Парижской Академии!

Задача. Докажите (или возьмите карточную колоду и проверьте экспериментально!), что для $d = 1, 2, 3, 4, 6$ порядок подгруппы в S_d, порожденной переворачиванием и тасованием Монжа, равен 1,2,6,12 и 120, соответственно. Отождествите* с точностью до изоморфизма первые четыре из этих групп.

Ответ. Это группы S_1, S_2, S_3 и A_4. При $d = 6$ получается группа, изоморфная $\mathrm{PGL}(2, 5)$, факторгруппе $\mathrm{GL}(2, 5)$ по центру.

Обратите внимание, что мы не предлагали читателю отождествить соответствующую группу для $d = 12$. Дело в том, что получающаяся при этом группа имеет порядок $95040 = 3^6 \cdot 3^3 \cdot 5 \cdot 11$. Это знаменитая **группа Матье** M_{12}, одна из спорадических конечных простых групп.

3. Порождение $\mathbf{S_n}$ и $\mathbf{A_n}$. Следующие 5 результатов доказаны в главе 5.

• Симметрическая группа S_n порождается множеством циклов

$$(i_1 \dots i_r), \qquad i_1 < \dots < i_r.$$

• Симметрическая группа S_n порождается множеством транспозиций (ij), $i < j$.

• Симметрическая группа S_n порождается множеством фундаментальных транспозиций $s_i = (i, i+1)$, $i = 1, \dots, l-1$.

• Знакопеременная группа A_n порождается множеством 3-циклов (ijh), $i < j < h$.

• При $n \geq 5$ знакопеременная группа A_n порождается множеством попарных произведений независимых транспозиций

$$(ij)(hk), \qquad |\{i, j, h, k\}| = 4.$$

4. Порождение линейных групп. Следующие результаты доказаны в главе 7.

• Для поля K группа $\mathrm{SL}(n, K)$ порождается множеством элементарных трансвекций $t_{ij}(1) = e + \xi e_{ij}$, $\xi \in K$, $1 \leq i \neq j \leq n$.

---

*Здесь и далее предложение читателю **отождествить что-то** является переводом с моего внутреннего математического языка команды `identify smth`. Таким образом, пожелание **отождествить что-то**, означает совершенно не то же самое, что приказ **отождествить что-то с чем-то**, в свою очередь, являющийся переводом `identify smth. with smth. else`!! Другие возможные русские переводы: **опознайте**, **распознайте** или, как сказали бы физики, программисты и криминалисты, **идентифицируйте**.

• Для поля K группа $\mathrm{GL}(n, K)$ порождается множеством элементарных преобразований, состоящим из элементарных трансвекций

$$t_{ij}(\xi) = e + \xi e_{ij}, \qquad \xi \in K, \quad 1 \le i \ne j \le n,$$

и элементарных псевдоотражений

$$d_i(\varepsilon) = e + \varepsilon e_{ii}, \qquad \varepsilon \in K^*, \quad 1 \le i \le n.$$

5. Конечно порожденные группы. Группа, для которой существует конечная система образующих, называется **конечно порожденной**. Ясно, что любая конечная группа конечно порождена. Но, как мы уже знаем, даже группа, порожденная одним элементом, может быть бесконечной. С другой стороны, она не может быть *слишком* бесконечной: из конечного (или счетного) числа букв можно образовать лишь счетное количество слов. Поэтому ни одна группа мощности континуум, скажем, $\mathbb{R}$ или $\mathbb{T}$, не может быть конечно порожденной. В действительности, конечно порожденные группы являются естественным обобщением конечных групп и наследуют многие их свойства. Приведем некоторые примеры бесконечных конечно порожденных групп (много дальнейших примеров строится в главе 12).

• Свободная абелева группа $\mathbb{Z}^n$ конечного ранга.

• Группа $\mathrm{SL}(n, \mathbb{Z})$ порождена трансвекциями $t_{ij}(1) = e + e_{ij}$, $1 \le i \ne j \le n$ (это будет доказано в главе 7 как следствие эвклидовости $\mathbb{Z}$).

• Пусть $G = \langle x, y\rangle$ подгруппа в $\mathrm{GL}(n, \mathbb{Z})$, порожденная двумя инволюциями

$$x = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Так как $yx = t_{12}(1)$ — элемент бесконечного порядка, группа G бесконечна. Эта группа обозначается D_∞ и называется **бесконечной диэдральной группой**.

А вот следующие группы не могут быть конечно порожденными:

• свободная абелева группа $\mathbb{Z}^{\aleph_0}$ счетного ранга;

• аддитивная группа $\mathbb{Q}^+$, она порождена $\{1/n, n \in \mathbb{N}\}$;

• мультипликативная группа μ_{p^∞}, она порождается первообразными корнями ζ_{p^n} степеней p^n, $n \in \mathbb{N}$;

• мультипликативная группа $\mathbb{Q}^*$, она порождена -1 и $p \in \mathbb{P}$ (это просто еще одна формулировка основной теоремы арифметики!).

Для каждой из этих групп очевидно, что она не порождается *никаким* конечным числом элементов. В действительности легко видеть, что группы $\mathbb{Q}^+$ и μ_{p^∞}, $p \in \mathbb{P}$, обладают следующим замечательным свойством: любая их конечно порожденная подгруппа циклическая — группы с таким свойством называются **локально циклическими**. Для группы $\mathbb{Q}^+$ этот факт называется `приведением дробей к общему знаменателю`, а в μ_{p^∞} подгруппа, порожденная элементами $\zeta_1, \dots, \zeta_n$, порождается уже тем из них, который имеет наибольший порядок. Что касается группы $\mathbb{Q}^*$, то она изоморфна прямому произведению группы $\{\pm 1\}$ и свободной абелевой группы счетного ранга. Тем самым, любая ее конечно порожденная подгруппа содержится в некоторой подгруппе, порожденной -1 и конечным множеством простых $p_1, \dots, p_n$.

6. Экономичное порождение. В действительности, приведенные в предыдущих пунктах системы образующих весьма далеки от минимальных. На самом деле, обычно достаточно гораздо меньшего числа элементов, элементов меньших порядков, и т. д. В последние годы в связи с компьютерными вычислениями в группах получил громадное развитие поиск более эффективных порождающих множеств — известный как `economic generation`. Например, установлено, что многие достаточно неабелевы группы, включая все конечные простые группы, порождаются двумя элементами. Приведем два примера экономичного порождения.

• Симметрическая группа S_n порождена транспозицией (12) и длинным циклом $(123\dots n)$.

• Группа $\mathrm{SL}(n, \mathbb{Z})$ порождена трансвекцией $t_{12}(1)$ и элементом Коксетера $e_{12} + e_{23} + \dots + e_{n-1,n} + (-1)^n e_{n1}$

§ 14♠. Условия минимальности и максимальности

> A group G **has both chain conditions** if it has both chain conditions!
>
> Joseph Rotman. [**338**]

В 1950-е годы совершенно чудовищно разрослось направление, связанное с **условиями конечности**. Незамысловатая интрига здесь состояла в следующем: наложим на группу G *какое-то* условие, которое заведомо выполнено для конечных групп, и посмотрим, какие из теорем о конечных группах переносятся на этот случай. Однако очень скоро эта деятельность утратила все резидуальные связи с реальностью и полностью превратилась в артефакты для артефактов. По-

разительно, что многие алгебраисты, в первую очередь на Украине, но также и в России, Великобритании, Германии, Италии по инерции и сегодня продолжают заниматься подобного рода вопросами, плодя все новые и новые доморощенные, а часто просто бредовые (= `home-bred`) условия.

Разумеется, среди условий конечности есть и естественные классические условия, возникающие в настоящих вопросах и фигурирующие в настоящих классических теоремах. Некоторые из них нам фактически уже встречались. Так, группа G называется

- **периодической**, если все ее элементы имеют конечный порядок;
- **конечно порожденной**, если $G = \langle x_1, \dots, x_n \rangle$;
- **конечно представимой**, если $G = \langle x_1, \dots, x_n \mid w_1, \dots, w_m \rangle$.

В главе 12 нам встретится следующее усиление периодичности.

• Группа G называется **локально конечной**, если любая ее конечно порожденная подгруппа конечна.

Ясно, что локально конечная группа периодична. Вопрос о том, верно ли обратное, составлял содержание **общей проблемы Бернсайда**. Как мы узнаем в главе 12, эта проблема решается отрицательно. Вот еще одно часто возникающее в приложениях условие конечности.

• Группа G называется **финитно аппроксимируемой**, если для любого $g \in G^\sharp$ существует такой гомоморфизм $\phi : G \longrightarrow H$ на *конечную* группу H, что $\phi(g) \neq 1$.

В настоящем параграфе мы рассмотрим еще две пары *естественных* условий конечности, называемые **условиями обрыва**.

• Группа G удовлетворяет **условию максимальности**, если ней не существует бесконечных строго *возрастающих* цепочек подгрупп

$$H_1 < H_2 < H_3 < \dots$$

• Группа G удовлетворяет **условию минимальности**, если ней не существует бесконечных строго *убывающих* цепочек подгрупп

$$H_1 > H_2 > H_3 > \dots$$

Иными словами, в первом случае утверждается, что любая *возрастающая* цепочка подгрупп обрывается на конечном шаге, это условие называется еще **условием обрыва возрастающих** цепочек или, коротко, **условием ACC** (= `ascending chain condition`). Аналогично, во

втором случае утверждается, что любая *убывающая* цепочка подгрупп обрывается на конечном шаге, это условие называется еще **условием обрыва убывающих** цепочек или, коротко, **условием DCC** (= `descending chain condition`). Чтобы подчеркнуть аналогию с другими алгебраическими теориями, группа G, удовлетворяющая условию максимальности, часто называется **нетеровой**, а условию минимальности — **артиновой**. Конечно, они называются так в честь Эмми Нетер и Эмиля Артина, которые начали систематическое использование аналогичных условий в теории колец и модулей. Специалисты по теории бесконечных групп часто обозначают эти условия `max` и `min`.

Условия `ACC` и `DCC` независимы:

- Группа $\mathbb{Z}$ нетерова, но не артинова,
- Группа μ_{p^∞} артинова, но не нетерова.

В предположении аксиомы выбора условие максимальности можно сформулировать еще и так: любое непустое множество подгрупп в G имеет максимальный элемент. В частности, любая собственная подгруппа $H \neq G$ содержится в максимальной. В свою очередь условие минимальности утверждает, что любое такое множество имеет минимальный элемент. В частности, любая нетривиальная подгруппа $H \neq 1$ содержит минимальную.

Условие максимальности является усилением условия конечной порожденности. Следующий результат доказывается точно так же, как аналогичный результат для идеалов колец в книге III.

Теорема. *Группа G в том и только том случае удовлетворяет условию максимальности, когда все ее подгруппы конечно порождены.*

Доказательство. В самом деле, пусть подгруппа $H \leq G$ не является конечно порожденной. В этом случае в H можно построить бесконечную строго возрастающую цепочку подгрупп. Для начала возьмем любой элемент $g_1 \in H \setminus \{1\}$ и положим $H_1 = \langle g_1 \rangle$. Так как H бесконечно порождена, то $H_1 < H$. Поэтому найдется $g_2 \in H \setminus H_1$, положим $H_2 = \langle g_1, g_2 \rangle$. По-прежнему, так как H бесконечно порождена, то $H_2 < H$. Продолжая действовать таким образом, мы и построим бесконечную цепочку.

Обратно, пусть $H_1 < H_2 < \dots$ — бесконечная возрастающая цепочка. Легко видеть, что объединение $H = \cup H_i$ является подгруппой в G. В самом деле, если $h \in H_i$, $g \in H_j$ для некоторых i, j, то $hg^{-1} \in H_{\max(i,j)}$. Таким образом по условию группа H конечно порождена. Пусть, скажем, $H = \langle g_1, \dots, g_n \rangle$. Тогда $g_i \in H_{j_i}$ для некото-

рых j_i. Полагая $m = \max(j_1, \ldots, j_n)$, мы видим, что $g_1, \ldots, g_n \in H_m$ и, значит, $H_m = H$, так что начиная с m-го шага цепочка перестает быть строго возрастающей, вопреки предположению.

В свою очередь, условие минимальности является усилением периодичности.

Задача. Докажите, что любая группа с условием минимальности периодична.

В дальнейшем условия минимальности и максимальности обычно будут использоваться совместно. Кроме того, в большинстве результатов достаточно требовать лишь обрыва цепочек *нормальных* подгрупп:

• Группа G удовлетворяет **условию максимальности для нормальных подгрупп**, если ней не существует бесконечных строго *возрастающих* цепочек *нормальных* подгрупп

$$H_1 \lhd H_2 \lhd H_3 \lhd \ldots$$

• Группа G удовлетворяет **условию минимальности для нормальных подгрупп**, если ней не существует бесконечных строго *убывающих* цепочек *нормальных* подгрупп

$$H_1 \rhd H_2 \rhd H_3 \rhd \ldots$$

В дальнейшем эти условия будут обычно называться условием `ACC` и условием `DCC` для нормальных подгрупп, соответственно. Подчеркнем, что все подгруппы H_i здесь предполагаются нормальными *во всей группе* G, а не просто в следующей или предыдущей подгруппе! Специалисты по теории бесконечных групп часто обозначают эти условия `max-n` и `min-n`. Условие максимальности для нормальных подгрупп допускает обычную характеризацию, в терминах конечной порожденности. Доказательство следующей теоремы слово в слово повторяет предыдущее.

Теорема bis. *Группа G в том и только том случае удовлетворяет условию максимальности для нормальных подгрупп, когда все ее нормальные подгруппы конечно порождены* (*как нормальные подгруппы*).

На группы, которые одновременно удовлетворяют условиям `ACC` и `DCC` для всех — или даже только для нормальных! — подгрупп, можно перенести многие из общих структурных фактов о конечных группах.

В частности, для них справедливы аналоги основных результатов о единственности композиционных факторов, главных факторов, прямых разложений и т. д., таких как теоремы Жордана—Гельдера и Ремака—Крулля—Шмидта.

Впрочем, в той мере, в которой в доказательстве этих теорем конечность используется *только* в форме обрыва цепей, с содержательной точки зрения абсолютно все равно, доказывать их в такой общности, или же доказывать их только для конечных групп и отмечать, что они продолжают оставаться справедливыми при условии обрыва цепей. С другой стороны, имеется ряд результатов, которые для конечных групп получаются применением простых общих соображений (индукция по порядку, принцип Дирихле, etc.), в то время как их доказательство для артиновых или нетеровых групп требует несколько более тонких рассуждений. В таких случаях мы стараемся проводить доказательства, явным образом ссылающиеся на условия обрыва — даже в тех случаях, когда они заметно длиннее!

Однако, как мы уже упоминали, в 1950-е годы критика и самокритика ослабли и учение об условиях конечности `растеклось белкой по дубу`*. В теории бесконечных групп начали изучать слойно-конечные и сопряженно-конечные группы, группы конечного ранга, условия максимальности и минимальности для абелевых подгрупп, абелевых нормальных подгрупп ... — однако, что касается этих условий, по крайней мере все еще можно понять, что в них говорится. В дальнейшем возникли **многие сотни** — а может и **тысячи**, я не пытался считать — других наводящих тоску условий. Вот диагноз, который поставили этому направлению Александр Юрьевич Ольшанский и Альфред Львович Шмелькин [149]: "Узкие, самоизолированные направления развиваются, если их авторы, не имея конечной цели или игнорируя невозможность ее достижения, вводят все новые условия на группы лишь для того, чтобы опубликовать еще несколько статей; такое явление встречается, впрочем, не только в теории групп". В настоящей книге мы, конечно, не будем интересоваться подобными извращениями.

§ 15♠. Длина и приведенные разложения

1. Длина. Пусть G — произвольная группа, а X — система образующих группы G. Предположим, что $1 \notin X$ и $X^{-1} = X$, таким образом, каждый элемент есть произведение конечного числа элементов из X.

**Серым волком по земли, шизым орлом под облакы.*

Пусть $g \in G$ наименьшее число m такое, что $g = x_1 \dots x_m$, где $x_i \in X$, есть произведение m множителей из X, называется **длиной** элемента g по отношению к системе образующих X и обозначается $l_X(g)$ или, если система X определена из контекста, просто $l(g)$. Обозначение $l(g)$ происходит от слова `длина` = `longueur` = `Länge` = `lunghezza` = `length`. Любое представление g в виде $g = x_1 \dots x_m$, где $x_i \in X$, а $m = l(g)$ называется **приведенным разложением** элемента g.

Ясно, что единственным элементом длины 0 является $1 \in G$. Элементы X и только они имеют длину 1. Попарные произведения xy, где $x, y \in X$, но $xy \notin X \cup \{1\}$ имеют длину 2 и т. д. Если $g = x_1 \dots x_m$ — приведенное разложение элемента g, то $g^{-1} = x_m^{-1} \dots x_1^{-1}$ является приведенным разложением элемента g^{-1}. В частности, $l(w^{-1}) = l(w)$. В действительности, сейчас мы докажем, что $d(g,h) = d_X(g,h) = l(gh^{-1})$ определяет расстояние на группе G. В самом деле, положительность расстояния была только что отмечена, а симметричность вытекает из того, что $l(gh^{-1}) = l(hg^{-1})$. Таким образом, нам остается только доказать неравенство треугольника.

Неравенство треугольника. *Для любых двух $h, g \in G$ выполняются неравенства*

$$|l(g) - l(h)| \le l(gh) \le l(g) + l(h).$$

Доказательство. Докажем вначале правое неравенство. Для этого запишем h и g как произведение образующих, пусть, скажем, $g = x_1 \dots x_m$, $h = y_1 \dots y_n$. Тогда $gh = x_1 \dots x_m y_1 \dots y_n$, так что $l(gh) \le m + n$. С другой стороны,

$$l(g) = l(ghh^{-1}) \le l(gh) + l(h^{-1}) = l(gh) - l(h),$$

так что $l(gh) \ge l(g) - l(h)$. Неравенство $l(gh) \ge l(h) - l(g)$ доказывается аналогично.

Можно заметить, что это расстояние инвариантно относительно правых сдвигов на элементы G, а именно, $d(fg, hg) = d(f,h)$ для любых $f, g, h \in G$.

Задача. Верно ли, что это расстояние инвариантно относительно левых сдвигов? Определите в терминах функции l такое расстояние на G, которое инвариантно относительно левых сдвигов.

В терминах длины элементов определяются два важнейших инварианта группы: ширина и рост.

2. Ширина. Пусть, по-прежнему, X — система образующих группы G. Рассмотрим множество элементов длины, не превосходящей n,

$$B(X,n) = \{g \in G \mid l_X(g) \le n\}.$$

С точки зрения расстояния $d = d_X$ это в точности шар радиуса n с центром в e. Говорят, что **ширина** $w_X(G)$ (`width`) группы G относительно системы образующих X равна n, если $B(X,n) = G$, но $B(X,n-1) \ne G$. Многие сотни публикаций посвящены вычислению ширины $w_X(G)$ различных конкретных групп G относительно различных конкретных систем образующих X: коммутаторов, инволюций, отражений, трансвекций и т. д. Первый вопрос здесь, уже ответ на который может быть в высшей степени нетривиален, таков: верно ли, что группа G имеет **конечную ширину** относительно образующих X? Некоторые результаты в этом направлении для классических групп встретятся нам в книге IIB.

3. Рост. С другой стороны, так как $|B(X,n)| \leq |X|^n$, если группа G бесконечна, а система образующих X конечна, то G заведомо не может иметь конечной ширины в образующих X. В этом случае в качестве характеристики G рассматривается характер роста функции $|B(X,n)|$, когда n стремится к ∞.

На первый взгляд длина $l(g) = l_X(g)$ элемента $g \in G$ — а тем самым и размер шара $B(X,n)$ — зависит от выбора X. Однако на самом деле, *с точностью до константы* длина g от выбора *конечной* системы образующих X не зависит!

Задача. Докажите, что если $X = X^{-1}$ и $Y = Y^{-1}$ — две системы образующих группы G, то найдется такая константа $c \in \mathbb{N}$, что $l_Y(g) \leq cl_X(g)$ и $l_X(g) \leq cl_Y(g)$.

Решение. В самом деле, каждый элемент $y \in Y$ представим как произведение m_y элементов из X. Заменяя в выражении $g \in G$ в образующих Y каждый элемент $y \in Y$ на его выражение через элементы X, мы видим, что $l_Y(g) \leq ml_X(g)$, где $m = \max(m_y)$, $y \in Y$. Точно так же проверяется, что $l_X(g) \leq nl_Y(g)$ для некоторого $n \in \mathbb{N}$. Осталось взять $c = \max(m,n)$.

Следствие. *Для любых двух конечных систем образующих X, Y группы G существует такая константа $c \in \mathbb{N}$, что*

$$|B(X,n)| \leq c|B(Y,cn)|, \qquad |B(Y,n)| \leq c|B(X,cn)|.$$

Две арифметические функции $\phi, \psi : \mathbb{N} \longrightarrow \mathbb{N}$, для которых существует такая константа $c \in \mathbb{N}$, что $\phi(n) \leq c\psi(cn)$ и $\psi(n) \leq c\phi(cn)$ называются **эквивалентными**. Таким образом, *класс эквивалентности* функции $n \mapsto |B(X,n)|$ не зависит от выбора конечной системы образующих X. Этот класс называется **ростом** группы G и обозначается $\mathrm{growth}(G)$.

• Свободная абелева группа $G = \mathbb{Z}^m$ имеет **полиномиальный рост**, т. е. $\mathrm{growth}(\mathbb{Z}^m)$ это класс какой-то функции $n \mapsto n^l$.

• Свободная группа $G = F_m$ имеет **экспоненциальный рост**, т. е. $\mathrm{growth}(F_m)$ это класс какой-то функции $n \mapsto l^n$.

Легко построить *самые разнообразные* примеры групп экспоненциального роста. С другой стороны, групп полиномиального роста совсем немного. А именно, Милнор и Вольф в классе разрешимых групп, а потом Михаил Громов в общем случае (1981) полностью описали такие группы.

Теорема Громова. *Почти нильпотентные группы и только они имеют полиномиальный рост.*

Долгое время оставалась открытой проблема Милнора: существуют ли группы **промежуточного роста**, в которых размер шара $B(X,n)$ растет быстрее, чем любой многочлен, но медленнее, чем любая экспонента от n? Ответ на этот вопрос получил Ростислав Григорчук в 1983 году. Он показал, что существует целая бесконечная иерархия групп промежуточного роста, причем как периодических, так и групп без кручения!

§ 16♢. Смежные классы

В настоящем параграфе мы свяжем с каждой подгруппой $H \leq G$ два отношения эквивалентности на G.

1. Смежные классы. Сейчас мы введем одно из ключевых понятий теории групп, которое первым рассматривал Эварист Галуа.

Определение. Левым смежным классом G *по* H *называется любое множество вида* $Hx = \{hx \mid h \in H\}$, *где* $x \in G$. *При этом* x *называется* **представителем** *класса* Hx. *Аналогично, множество* $xH = \{xh \mid h \in H\}$ *называется* **правым смежным классом** G *по* H *с представителем* x.

Через $H\backslash G = \{Hx \mid x \in G\}$ обозначается множество всех *левых* смежных классов G по H, а через $G/H = \{xH \mid x \in G\}$ — множество всех *правых* смежных классов.

Комментарий 1, типографский. Обратите внимание, что здесь использован знак \, который TEXнически называется `\backslash`. Мало-мальски грамотный человек должен с полувзгляда отличать его от знака \, выражающего теоретико-множественную разность и называемого `\setminus`. Дело в том, что знак \ трактуется как *знак операции* и `отбивает тонкие шпации` после первого и перед вторым операндом, в то время как знак \ этого не делает! Еще раз посмотрите на $H\backslash G$ и $H \setminus G$ и раз и навсегда запомните, *which is which*[♮]. В рукописном тексте знаки `\backslash` и `\setminus` обычно пишутся с разным наклоном, первый из них почти вертикально, а второй — под углом $3\pi/4$.

Комментарий 2, лингвистический. Русский термин `смежный класс` является парафразом немецкого `Nebenklasse`, существующего в двух энантиоморфных формах: `Linksnebenklasse` и `Rechtsnebenklasse` (в совсем старых книгах говорится также `Nebengruppe`). Этот термин в большинстве языков образуется от нового корня и является одним их самых трудных для перевода. Скажем, по-английски смежный класс называется `coset` (сомножество) (этот термин ввел А.Миллер в 1910 году), по-итальянски — `classe laterale` (боковой класс), по-польски — `warstwa` (слой) и т. д.

Комментарий 3, a parte. Во многих книгах левыми смежными классами называется то, что мы называем правыми смежными классами, и наоборот. Наша терминология представляется мне более логичной, так как наши левые смежные классы являются в точности орбитами H в *левом* регулярном представлении. Этой терминологии придерживаются, в частности, Холл [**207**], Фаддеев [**184**] и Шафаревич ?? . В то же время, под влиянием Куроша [**118**] кафедра алгебры Московского университета называет Hx *правым* смежным классом, см., например, учебники Кострикина [**108**], [**109**] и Винберга [**59**].

2. Разбиение на смежные классы. Сейчас мы покажем, что смежные классы по подгруппе H задают разбиение группы G. Напомним (см. аппендикс 1), что **разбиением** множества X называется его представление в виде объединения попарно непересекающихся непустых подмножеств.

[♮]Which is the master, that's the question — Humpty Dumpty.

Теорема. *Группа G является дизъюнктным объединением всех различных левых (или правых) смежных классов по подгруппе H.*

Доказательство. Так как $x \in Hx$, то $G = \bigcup Hx$, где объединение берется по всем $Hx \in H\backslash G$. Таким образом, нужно лишь показать, что это объединение дизъюнктно. В самом деле, пусть Hx и Hy — два смежных класса G по H. Предположим, что $Hx \cap Hy \neq \varnothing$. Это значит, что найдется $z \in Hx \cap Hy$, т. е. найдутся такие $h, g \in H$, что $z = hx = gy$. Тем самым $y = g^{-1}(hx) = (g^{-1}h)x$, так что $y \in Hx$. Поэтому $Hy \subseteq H(Hx) = (HH)x = Hx$. Точно так же проверяется и включение $Hx \subseteq Hy$. Таким образом, окончательно, $Hx = Hy$. Тем самым, никакие два различных левых смежных класса не пересекаются, что и утверждалось. Доказательство для правых классов совершенно аналогично.

Эта теорема означает, что

$$G = \bigsqcup Hx, \qquad Hx \in H\backslash G.$$

Разбиение на левые смежные классы G по H называется **разложением группы G по подгруппе H** (`Nebenklassenzerlegung`, `coset decomposition`). Одним из смежных классов является сама подгруппа $H = H1 = 1H$. Из наличия сокращения в группе сразу следует, что для каждого $x \in G$ отображение $H \longrightarrow Hx$, $h \mapsto hx$, задает биекцию H на смежный класс Hx, так что, в частности, $|Hx| = |H|$. Из только что доказанной теоремы вытекает, что для любого $x \notin H$ класс Hx не пересекается с H и, значит, не является подгруппой.

Задача. Пусть $H \leq G$. Докажите, что если $G \setminus H$ конечно, то либо G конечна, либо $H = G$.

Решение. Пусть G бесконечна, $H \neq G$. Если H конечна, то сравнение мощностей показывает, что $G \setminus H$ бесконечно. С другой стороны, если H бесконечна и $g \notin H$, то $G \setminus H$ содержит бесконечный смежный класс gH и, значит, снова бесконечно.

Задача. Пусть $F, H \leq G$. Докажите, что если $Fx = Hy$, то $F = H$.

Результат этой задачи легко уточнить.

Задача. i) Пусть $F, H \leq G$. Покажите, что пересечение двух смежных классов $Fx \cap Hy$ либо пусто, либо имеет вид $(F \cap H)g$, для подходящего $g \in G$.

ii) Обобщите этот результат на *произвольное* семейство подгрупп.

3. Сравнение по модулю подгруппы. В предыдущем пункте мы построили разбиения G на левые/правые классы смежности по H. Мы

знаем, что с каждым разбиением связано некоторое отношение эквивалентности. Опишем получающиеся отношения эквивалентности явно.

Будем говорить, что x и y **сравнимы по модулю H слева**, и писать $x \,{}_H\!\equiv\, y$, если $Hx = Hy$. Это означает, что найдутся такие $h, g \in H$, что $hx = gy$. Тем самым, $xy^{-1} = h^{-1}g \in H^{-1}H = H$. С подгруппой H связано и второе отношение эквивалентности, **сравнимость по модулю H справа**: $x \equiv_H y$, если $xH = yH$. Легко видеть, что $xH = yH$ эквивалентно включению $x^{-1}y \in H$. Таким образом, мы можем ввести отношение сравнимости по модулю H и не упоминая смежные классы.

Определение. *Говорят, что элементы $x, y \in G$* **сравнимы по модулю H слева** (*соответственно,* **справа**)*, если $xy^{-1} \in H$ (соответственно, $x^{-1}y \in H$).*

Из теоремы предыдущего пункта вытекает, что это действительно отношение эквивалентности, но это легко усмотреть и непосредственно из определения подгруппы. Посмотрим, скажем на сравнимость по модулю H слева. Это отношение *рефлексивно*, так как $xx^{-1} = e \in H$, *симметрично*, так как $yx^{-1} = (xy^{-1})^{-1} \in H^{-1} = H$, и *транзитивно*, так как $xz^{-1} = (xy^{-1})(yz^{-1}) \in HH = H$.

В случае, когда G коммутативна, $Hx = xH$ так что сравнимости по модулю H слева и справа совпадают. В этом случае обычно говорят просто о сравнимости по модулю H, которая обозначается $x \equiv y \pmod{H}$. В общем случае отношения эквивалентности ${}_H\!\equiv$ и $\equiv_H$ различны и сейчас мы постараемся установить связь между ними.

§ 17◇. Индекс, системы представителей

1. Индекс подгруппы. Заметим, прежде всего, что между множеством $H\backslash G$ левых смежных классов и множеством G/H правых смежных классов существует естественная биекция. Наивная попытка установить биекцию посредством $Hx \mapsto xH$ не приводит к желаемому результату, так как это соответствие, вообще говоря, не является корректным определением отображения: из $Hx = Hy$ *не следует*, что $xH = yH$. Поэтому приходится поступать чуточку хитрее. Вспомним, прежде всего, определение обратного по Минковскому к множеству X, а именно, $X^{-1} = \{x^{-1} \mid x \in X\}$. Ясно, что $X = Y \iff X^{-1} = Y^{-1}$. В интересующем нас случае $(Hx)^{-1} = x^{-1}H^{-1} = x^{-1}H$, так что $Hx = Hy \iff x^{-1}H = y^{-1}H$. Это значит, что сопоставление $Hx \mapsto x^{-1}H$ корректно определяет биекцию $H\backslash G$ на G/H.

Определение. *Пусть $H \leq G$. Мощность $|H\backslash G| = |G/H|$ множества смежных классов G по H называется* **индексом** *подгруппы H в группе G и обозначается $|G : H|$.*

Понятие индекса оказывается особенно полезным в случае, когда множество смежных классов конечно. Если $|G : H| < \infty$, то H называется **подгруппой конечного индекса** в G.

Комментарий. Многие авторы обозначают индекс подгруппы через $(G : H)$ или $[G : H]$. Наше обозначение представляется мне более удобным, так как оно подчеркивает аналогию между индексом и порядком группы. В самом деле, если $H = 1$, то $H\backslash G = G/H$ состоит из одноэлементных классов $\{g\}$, $g \in G$, и находится в биективном соответствии с группой G. Тем самым, $|G| = |G : 1|$.

Задача. Покажите, что в аддитивной группе $\mathbb{Q}^+$ нет подгрупп конечного индекса. Есть ли подгруппы конечного индекса в мультипликативной группе $\mathbb{Q}^*$?

2. Система представителей смежных классов. В одной из своих изначальных форм аксиома выбора утверждает, что для каждого отношения эквивалентности существует трансверсаль.

Определение. *Трансверсаль X к отношению сравнимости по модулю H слева/справа называется* **системой представителей левых/правых смежных классов** *G по H или, коротко,* **левой/-правой трансверсалью** *к H в G.*

Терминологический комментарий. В большинстве русских книг традиционно используется калька классических немецких выражений `Linksnebenklassenvertretersystem` и `Rechtsnebenklassenvertretersystem`, однако русский термин не столь **транспарентен**, так как требует для своего выражения пять слов*. Как и в случае **нормальных подгрупп/делителей**, *субстанциально* я пропагандирую современную терминологию **левая/правая трансверсаль**, но *акцидентально* сбиваюсь на привычный — тяжеловесный и менее удобный — традиционный *способ выражаться*.

Иными словами, система представителей левых смежных классов G по H — это такое подмножество $X \subseteq G$, что для любого $z \in G$ найдется $x \in X$ такое, что $Hz = Hz$ и из того, что $Hx = Hy$ для некоторых $x, y \in X$ следует, что $x = y$. С учетом этого определения теорема из

*Впрочем, даже по-немецки многие современные писатели, потерявшие классическое чувство языка и стиля, вместо недвусмысленного и энергичного `Linksnebenklassenvertretersystem` употребляют *обратный перевод с русского* `ein System von Linksnebenklassenvertretern` или, соответственно, `ein System von Rechtsnebenklassenvertretern`.

пункта 2 может быть переписана в виде $G = \bigsqcup Hx$, $x \in X$. Ясно, что $|X| = |G : H|$. Аналогично, если Y — система представителей правых смежных классов, то $G = \bigsqcup yH$, $y \in Y$. Эти понятия особенно полезны для подгрупп конечного индекса. Например, если $X = \{x_1, \dots, x_n\}$ — система представителей левых смежных классов, то группа G представляется в виде дизъюнктного объединения $G = Hx_1 \sqcup \dots \sqcup Hx_n$.

3. Системы общих представителей. Естественно возникает вопрос, верно ли, что можно найти **систему общих представителей** X для левых и правых смежных классов, т.е. такое множество X, которое одновременно является системой представителей как левых, так и правых смежных классов G по H? Многие элементарные учебники по теории групп и комбинаторике ссылаются на этот результат как на теорему Филипа Холла [150]. Например, именно так поступает Маршалл Холл [151][b].

> **Филип Холл** (`Philip Hall`, 11 апреля 1904, Хампстед — 30 декабря 1982, Кембридж) — замечательный английский алгебраист. Холл поступил в Кембридж в 1922 году. Под влиянием книги Бернсайда Холл заинтересовался теорией групп. Уже в 1927 году он открыл свое поразительное усиление теорем Силова для разрешимых групп, известное как теоремы Холла, мы подробно обсуждаем эти теоремы в главе 9. В 1932 году он написал свою знаменитую статью по теории p-групп, в которой ввел коммутаторное исчисление и собирательный процесс, установил связь между p-группами и алгебрами Ли. Во время Второй мировой войны Холл работал в Bletchey Park, где он занимался итальянскими и японскими шифрами, для этой цели ему даже пришлось выучить японский язык! После войны Холл получил много других прекрасных результатов, самым влиятельным из которых была теорема Холла—Хигмена. В нашем курсе встречаются *десятки* введенных им понятий: силовские системы, силовские башни, системные нормализаторы, изоклинизм, собирательный процесс и т. д. Филип Холл является известным контрпримером к утверждению, о том, что математика — это спорт исключительно для молодых. Один из острых пиков его активности пришелся на середину 1960-х годов.

Однако в действительности теорема Холла здесь совершенно ни при чем, так как замечание о существовании системы общих представителей в случае подгрупп конечного порядка абсолютно элементарно и было сделано лет за 25 до Холла [152], [153], притом даже в более общем случае двух разных [154] подгрупп $F, H \leq G$ одного и того же конечного порядка $|F| = |H| < \infty$.

---

[b] Стоит предостеречь, что обращение к первоисточникам в книге Маршалла Холла *весьма* своеобразно, так как теорема Филипа Холла цитируется по оригинальной статье 1935 года, в то время как теорема Кенига — не по оригинальной статье 1916 года, а по вышедшей в 1950 году книге, из-за чего у начинающего может возникнуть впечатление, что она получена позже теоремы Холла. Ну а про теоремы ван дер Вардена и де Брюйна вообще не упоминается!

Маршалл Холл (Marshall Hall, 17 сентября 1910, Сент-Луис, Миссури — 4 июля 1990, Лондон) — замечательный американский алгебраист, самые знаменитые результаты которого относятся к теории групп, теории алгебр Ли, конечным геометриям и комбинаторике. После окончания в 1932 году Йельского университета Холл решил продолжить свое образование в Кембридже, где большое влияние на него оказали Филип Холл, Харди и Давенпорт. После возвращения в США в 1936 году он получил докторат под руководством Оре. В 1941 году он поступил в морскую разведку, где занимался дешифровкой. После войны он стал профессором в Огайо, а в 1959 году переехал в Caltech. Среди самых известных результатов Холла в теории групп можно упомянуть положительное решение проблемы Бернсайда для групп экспоненты 6. Еще одно знаменитое достижение Холла — построение базиса свободной алгебры Ли. Интересно, что здесь, как и еще несколько раз в своей карьере, он шел по следам Филипа Холла, например, описание групп порядка 2^6 получено Ф. Холлом и Синиором, но опубликовано М. Холлом и Синиором! Маршалл Холл написал несколько классических текстов, по которым учились поколения математиков, в том числе *Теорию групп* и *Комбинаторику*.

Задача. Предположим, что подгруппы $F, H \leq G$ конечны, причем $|F| = |H|$. Тогда существует система общих представителей *левых* смежных классов G по F и *правых* смежных классов G по H.

Решение. В силу конечности каждый двойной смежный класс FxH содержит одинаковое количество левых смежных классов по F и правых смежных классов по H. Установим какую-то биекцию между ними. Осталось заметить, что любой левый смежный класс по F пересекается с любым правым смежным классом по H. В самом деле, $Fxh \cap fxH$ содержит fxh.

В частности, такая система представителей всегда существует, если сама группа G конечна. Где ссылка на теорему Холла — или на какую-то предшествующую ей комбинаторную теорему, такую как теоремы Кенига или ван дер Вардена, или последующую ей комбинаторную теорему, такую как теорема де Брюйна — действительно нужна [155], так это случай, когда мы рассматриваем *правые* смежные классы по F и *правые* смежные классы по H.

Система общих представителей существует и при некоторых других предположениях относительно подгруппы H, например, если ее *индекс* конечен **[369]**, p.12, 37. Точнее, имеет место следующий результат [158], теорема 4.3 или [159].

Теорема. *Предположим, что $F, H \leq G$, причем $|G : F| = |G : H| < \infty$. Тогда существует система общих представителей левых смежных классов G по F и правых смежных классов G по H.*

Если и порядок H и индекс H оба бесконечны, то система общих представителей вообще говоря совершенно не обязана существовать, первый контрпример построен ван дер Варденом [160]. Один из самых простых примеров живет внутри $(ax+b)$-группы $G = \mathrm{Aff}(1, \mathbb{Q})$. При этом H — это просто циклическая подгруппа, порожденная одной трансвекцией, а $g \in G$ — псевдоотражение:

$$G = \begin{matrix} \mathbb{Q}^* & \mathbb{Q} \\ 0 & 1 \end{matrix}, \qquad H = \begin{matrix} 1 & \mathbb{Z} \\ 0 & 1 \end{matrix}, \qquad g = \begin{matrix} n & 0 \\ 0 & 1 \end{matrix}$$

Бартель Леендерт ван дер Варден (`Bartel Leendert van der Waerden`, 2 февраля 1903, Амстердам — 12 декабря 1996, Цюрих) — замечательный голландский математик и историк науки. Из-за необычайной популярности его книги *Алгебра* (в младенчестве *Современная алгебра*), выдержавшей множество изданий и несколько десятилетий считавшейся каноническим текстом, многие рассматривают ван дер Вардена в первую очередь как алгебраиста, и ему действительно принадлежат фундаментальные результаты в коммутативной алгебре, теории Галуа, теории линейных групп, комбинаторной теории групп, теории инвариантов и теории групп Ли. Однако на самом деле ван дер Варден был одним из последних подлинно универсальных математиков, работавшим в области квантовой механики, алгебраической геометрии, теории чисел, комбинаторики, геометрии, топологии, анализа, теории вероятностей и математической статистики. Кроме того, он весьма основательно и абсолютно профессионально занимался историей математики и науки вообще, уже в 1950 году вышел первый том его блистательной книги [156], а в 1965 году — второй [157]. С 1919 по 1925 годы он учился в университетах Амстердама, где его руководителем был Гендрик де Фриз, и Геттингена, где он работал с Эмми Нетер. После нескольких лет работы в Гронингене ван дер Варден становится профессором в Лейпциге, где в то время работал Гейзенберг. После войны он некоторое время работал в Амстердаме (не только в университете, но и в компании `Shell`!!), но в 1951 году переезжает в Цюрих, где остается до конца жизни. Кроме уже цитированных книг на русский переведена книга [**47**]. В нашем курсе встречается несколько результатов ван дер Вардена: кроме упомянутых здесь комбинаторных теорем, которые обсуждаются в книге I, это теорема Шрайера—ван дер Вардена, теорема Леви—ван дер Вардена и т. д. Однако, конечно, его влияние на развитие алгебры *гораздо* шире, чем непосредственно принадлежащие ему результаты.

для некоторого $n \in \mathbb{N}$, $n > 1$. Теорема о делении с остатком в $\mathbb{Z}$ утверждает теперь, что левый смежный класс Hg является дизъюнктным объединением n правых смежных классов по H:

$$H\begin{matrix} n & 0 \\ 0 & 1 \end{matrix} = \begin{matrix} n & 0 \\ 0 & 1 \end{matrix} H \sqcup \begin{matrix} n & 1 \\ 0 & 1 \end{matrix} H \sqcup \ldots \sqcup \begin{matrix} n & n-1 \\ 0 & 1 \end{matrix} H.$$

Ясно, что в таких условиях нет никакой возможности выбрать систему общих представителей. Разумеется, здесь $|H|$ и $|G : H|$ оба бесконечны. Этот пример встретится нам по разным поводам еще раза три, первый раз уже в этой главе.

§ 18◇. Теорема Лагранжа

В этом параграфе мы докажем важнейшие равенства, связывающие индексы подгрупп, а в следующем параграфе извлечем из них интересные неравенства.

1. Теорема Лагранжа. Следующий результат, несмотря на свою простоту, исключительно важен.

Джузеппе Лодовико Лагранж (Giuseppe Lodovico Lagrange also known as Joseph-Louis Langrange, 25 января 1736, Турин — 10 апреля 1813, Париж) — наряду с Эйлером величайший математик XVIII века. Часто Лагранжа называют на французский манер **Жозеф-Луи**, но в действительности он был итальянцем, работавшим в Германии и Франции. Уже в 1755 году он стал профессором артиллерийской школы в Турине. Первые работы Лагранжа относятся к вариационному исчислению (уравнение Эйлера—Лагранжа). В 1766 году переехал в Берлин, где по рекомендации Эйлера был избран президентом Берлинской Академии наук. Каждый месяц он публиковал новую статью. Его работы охватывали всю современную ему математику, им получены ключевые результаты в анализе, алгебре, теории чисел, теории дифференциальных уравнений в частных производных. Его работы по механике и астрономии и сыграла ключевую роль в дальнейшем развитии физики и послужили отправной точкой работ Гамильтона и Якоби. В 1787 году перехал в Париж, где в 1788 году опубликовал свой классический труд *Аналитическая механика*. Однако после французской революции Парижская академия перестала платить зарплату своим членам и он вынужден был преподавать в различных учебных заведениях. Как вспоминал Пуассон, студенты с трудом понимали лекции Лагранжа из-за его сильного итальянского акцента. Более того, он чуть не подпал под конфискацию имущества как **подозрительный иностранец**, и только вмешательство влиятельных друзей-республиканцев защитило его. В нашем курсе встречаются несколько теорем Лагранжа, тождество Лагранжа, резольвента Лагранжа, метод Вандермонда—Лагранжа, интерполяционная формула Лагранжа, и т. д. В физике широко используется лагранжиан, в курсе математического анализа — остаточный член ряда Тейлора в форме Лагранжа, и т. д.

Теорема Лагранжа. *Если $H \leq G$, то $|G| = |H||G : H|$.*

Доказательство. Как всегда, правильный способ доказательства равенства двух кардинальных чисел состоит в установлении биекции между некоторыми множествами. В самом деле, пусть X — любая система представителей левых смежных классов. Тогда $|G : H| = |X|$. Мы утверждаем, что отображение $H \times X \longrightarrow G$, $(h, x) \mapsto hx$ представляет собой биекцию. В самом деле, $G = \cup Hx$, $x \in X$, так что это отображение сюръективно. С другой стороны, если для некоторых $h, g \in H$, $x, y \in X$ имеет место равенство $hx = gy$, то $Hx = Hy$, и, значит, по определению трансверсали $x = y$. Сокращая равенство $hx = gx$ на x справа, получаем $h = g$. Но это и значит, что $|G| = |H \times X| = |H||X| = |H||G : H|$.

Этот результат особенно важен для конечных групп, где из него вытекает важнейшее арифметическое ограничение на подгруппы.

Следствие 1. *Пусть G — конечная группа, $H \leq G$. Тогда порядок G делится на порядок H.*

Комментарий. Некоторые авторы называют теоремой Лагранжа именно это следствие, то же утверждение, которое мы называем теоремой Лагранжа, в этом случае называется **теоремой об индексе** (`Indexsatz`). Такая точка зрения имеет основание, так как сам Лагранж, конечно, явно формулировал именно это следствие [161], причем только для $G = S_n$. Для произвольных конечных групп теорему Лагранжа доказал Галуа.

В частности, применяя это следствие к циклическим подгруппам, мы видим, что порядок $o(g)$ любого элемента конечной группы делит порядок $|G|$ этой группы.

Следствие 2 (теорема Ферма). *Пусть G — конечная группа, $g \in G$. Тогда $g^{|G|} = e$.*

Мы будем использовать классический частный случай этой теоремы.

Следствие 3. *Если x и p взаимно просты, то $p|x^{p-1} - 1$.*

2. Контрпример Руффини. Пусть m делитель порядка группы G. Имеет ли место "обращение теоремы Лагранжа", т. е., иными словами, верно ли, что в G существует подгруппа H порядка m? В 1799 году Паоло Руффини перечислил все подгруппы симметрической группы S_5. В частности, он показал, что в ней нет подгрупп порядков 15, 30 и 40. Разумеется, Руффини формулировал этот результат в терминах **индексов** подгрупп, а не их порядков: не существует функций 5 переменных, которые при всевозможных перестановках этих переменных принимали бы ровно 8, 4 или 3 значения.

Паоло Руффини (`Paolo Ruffini`, 23 сентября 1765, Валентано — 10 мая 1822, Модена) — итальянский математик и врач. После окончания университета Модены, где он специализировался в математике и хирургии, Руффини некоторое время преподавал там математический анализ и геометрию. Однако жизнь Руффини пришлась на интересный период европейской истории. После того, как из религиозных соображений он отказался принести присягу Цизальпинской республике, его отстранили от преподавания и он зарабатывал на жизнь как практикующий врач, занимаясь математикой в свободной время. Именно тогда в 1799 году он первым доказал неразрешимость общего алгебраического уравнения степени ≥ 5 в радикалах. Считается, что его доказательство этого факта содержало пробел, который был через 27 лет заполнен Абелем, поэтому утверждение о неразрешимости в радикалах обычно называется теоремой Руффини—Абеля. Интересно, однако, что никто из современников Руффини не заметил этой ошибки. Кроме того, как раз в части, посвященной группам перестановок, доказательство Руффини совершенно безупречно. После падения Наполеона в 1814 году Руффини возвращается к преподаванию — одновременно математики и медицины! — и даже становится ректором университета Модены. Другие его математические работы относятся к теории алгебраических кривых, теории вероятностей и методам вычислений.

Пьер де Ферма (`Pierre de Fermat`, 17 августа 1601, Beaumont de Lomagne — 12 января 1665, Castres) — величайший математик XVII века, основатель теории чисел, алгебраической геометрии, дифференциального исчисления и теории вероятностей. Ферма изучал юриспруденцию и в 1630 году купил себе должность советника парламента Тулузы. Однако все свободное время он занимался математикой и сообщал свои результаты в письмах современникам. Особенно знаменита его переписка с Декартом, в которой он ввел инфинитезимальное исчисление и переписка с Паскалем по поводу оснований теории вероятностей, а также письма Робервалю, Мерсенну и английским коллегам, в которых он формулировал нерешенные задачи теории чисел. В действительности, именно Ферма построил первый вариант дифференциального исчисления, основанный на понятии актуально бесконечно малых первого порядка, и применил его к задачам нахождения экстремумов, касательных и т.д. Кроме того, в связи с задачами механики и оптики он занимался интегральным исчислением. При жизни Ферма почти ничего не опубликовал, все его результаты известны из писем, примечаний на полях книг и рукописей, которые были тщательно собраны и опубликованы его сыном Самюэлем. В нашем курсе встречаются десятки восходящих к нему понятий: декартовы координаты, дифференцирование, простые числа Ферма, теорема Ферма, кольцо двойных чисел, и т. д.

В теории чисел Ферма сформулировал громадное количество предположений, большинство из которых были доказаны математиками XVIII века, однако некоторые остаются открытыми и сегодня. Вероятно, самой знаменитой проблемой математики, супербрендом над супербрендами, shir hash shirim, в течение 300 лет оставалась **большая** aka **последняя** aka **великая теорема Ферма** известная также как **проблема Ферма**. Так называется сформулированная Ферма задача об отсутствии нетривиальных целочисленных решений уравнения $x^n + y^n = z^n$ при $n \geq 3$. На полях своей копии *Арифметики* Диофанта он даже написал, что нашел *поистине замечательное* доказательство этого факта. Однако, за исключением случая $n = 4$, где он действительно дал безукоризненное доказательство основанное на методе математической индукции ("бесконечного спуска"), в его бумагах не было обнаружено никаких следов этого *замечательного доказательства*. Можно с полной уверенностью утверждать, что "доказательство" Ферма было ошибочным. Более того, современные математики знают, в чем именно состояла ошибка Ферма: он считал, что кольца целых круговых полей являются кольцами главных идеалов. На протяжении двух веков это неявное предположение ускользало от внимания даже лучших математиков. Необходимость доказательства этого факта не заметил Эйлер в своем (неполном) доказательстве теоремы Ферма при $n = 3$. Спустя почти два века это же сомнительное предположение было использовано Ламе и Коши в еще одном (ошибочном) доказательстве теоремы Ферма. Вскрытие этой ошибки Дирихле и Куммером привело к созданию алгебраической теории чисел и теории колец. На протяжении примерно 100 лет, после проникновения отрывочных сведений о проблеме Ферма в широкие неумытые массы, эти массы терроризировали математические факультеты и институты своими безграмотными сочинениями на эту тему. К счастью, в 1994 году проблема Ферма была наконец положительно решена Эндрю Уайлсом.

Задача. Докажите, что у группы A_4 нет подгруппы порядка 6.

Решение (T.-L. Shen, [**338**], стр.48). Если $H \leq A_4$ – подгруппа порядка 6, то она имеет индекс 2 в A_4 и, следовательно, $g^2 \in H$ для всех $g \in A_4$. Однако, если g — 3-цикл, то $g = g^4 = (g^2)^2$. Таким образом, H должна содержать по крайней мере 8 элементов.

Задача. Докажите, что A_4 — единственная подгруппа порядка 12 в S_4.

Указание. Мы это уже где-то видели. Пусть $H \leq S_4$, $|H| = 12$. Тогда квадрат любого элемента из S_4 лежит в H.

3. Мультипликативность индекса. Теорема Лагранжа допускает следующее естественное обобщение, называемое **общей теоремой об индексе** (`allgemeiner Indexsatz`).

Теорема. *Если $F \leq H \leq G$, то $|G : F| = |G : H||H : F|$.*

Доказательство. План доказательства этой теоремы точно такой же, как в теореме Лагранжа. А именно, пусть X — система представителей левых смежных классов H по F, а Y — система представителей левых смежных классов G по H. Мы утверждаем, что XY является системой представителей левых смежных классов G F, а отображение $X \times Y \longrightarrow XY$, $(x, y) \mapsto xy$, устанавливает биекцию прямого произведения множеств X и Y с их произведением по Минковскому. Тем самым,

$$|G : F| = |XY| = |X \times Y| = |X||Y| = |H : F||G : H|,$$

что и доказывает теорему.

Проверим теперь высказанные в предыдущем абзаце утверждения. По условию $G = \bigcup Hy$, $y \in Y$, и $H = \bigcup Fx$, $x \in X$. Подставляя выражение для H из второй формулы в первую и пользуясь ассоциативностью, получаем, что $G = \bigcup F(xy)$, $(x, y) \in X \times Y$. Поэтому нам осталось лишь доказать, что если $Fx_1y_1 = Fx_2y_2$ для некоторых $x_1, x_2 \in X$ и $y_1, y_2 \in Y$, то $x_1 = x_2$ и $y_1 = y_2$. В самом деле, пусть $Fx_1y_1 = Fx_2y_2$. Так как $x_1, x_2 \in X \subseteq H$, это означает, что $Hy_1 \cap Hy_2 \neq \varnothing$. По теореме пункта 2 тогда $Hy_1 = Hy_2$, и, значит, $y_1 = y_2 = y$ по определению трансверсали. Сокращая равенство $Fx_1y_1 = Fx_2y_2$ на y справа, получаем $Fx_1 = Fx_2$, так что, снова по определению трансверсали, $x_1 = x_2$, что и требовалось доказать.

Теорема Лагранжа получается как частный случай этой теоремы в случае $F = 1$.

§ 19♡. Теорема Пуанкаре

1. Индекс пересечения. Сейчас мы выведем из мультипликативности индекса важное следствие. Разумеется $|G : F \cap H|$ здесь нужно понимать как $|G : (F \cap H)|$.

Теорема. *Если $F, H \leq G$, то $|G : F \cap H| \leq |G : F| \cdot |G : H|$.*

Это утверждение моментально вытекает из теоремы об индексе и следующей леммы.

Лемма. *Если $F, H \leq G$, то $|F : F \cap H| \leq |G : H|$.*

В самом деле, $|G : F \cap H| = |G : F||F : F \cap H| \leq |G : F||G : H|$. Таким образом, нам остается лишь доказать лемму.

Доказательство леммы. Пусть X — система представителей левых смежных классов F по $F \cap H$. Нам достаточно показать, что для любых $x, y \in X$ из равенства $Hx = Hy$ вытекает $x = y$. В самом деле, пусть $Hx = Hy$. Это означает, что найдутся такие $h, g \in H$, что $hx = gy$, так что $xy^{-1} = h^{-1}g \in H$. Однако по самому определению $x, y \in X \subseteq F$, так что в действительности $xy^{-1} \in F \cap H$, и, окончательно, $x = y$.

Для конечных групп мы будем *десятки раз* пользоваться этой теоремой в следующей форме.

Следствие. *Если подгруппы $F, H \leq G$, таковы, что $|G : F|, |G : H| < \infty$, и $\gcd(|G : F|, |G : H|) = 1$, то*

i) $|G : F \cap H| = |G : F| \cdot |G : H|$,

ii) *если, кроме того, группа G конечна, то $FH = G$.*

Доказательство. По теореме об индексе

$$|G : F \cap H| = |G : H||H : F \cap H| = |G : F||F : F \cap H|,$$

так что $|G : F \cap H|$ делится на $|G : H|$ и $|G : F|$. Но тогда в силу их взаимной простоты $|G : F \cap H|$ делится на их произведение и, значит, по крайней мере, $|G : F \cap H| \geq |G : F| \cdot |G : H|$. Теперь ii) получается с использованием формулы произведения.

2. Теорема Пуанкаре. Сформулируем важнейшее следствие доказанного в предыдущем пункте неравенства, впервые отмеченное в 1887 году Анри Пуанкаре в связи с теорией автоморфных функций.

Теорема Пуанкаре. *Если $H_1, \dots, H_n$ — подгруппы группы G, имеющие в ней конечный индекс, то их пересечение $H_1 \cap \dots \cap H_n$ тоже подгруппа конечного индекса в G.*

Сам Пуанкаре формулировал эту теорему чуть иначе. Две подгруппы F, H группы G называются **соизмеримыми**, если их пересечение имеет в каждой из них конечный индекс $|F : F \cap H|, |H : F \cap H| < \infty$. Теперь мы можем сформулировать теорему Пуанкаре следующим образом.

Следствие 1. *Любые две подгруппы, имеющие конечный индекс в группе G, соизмеримы.*

Отметим еще два полезных следствия теоремы Пуанкаре.

Следствие 2. *Отношение соизмеримости транзитивно.*

Доказательство. Пусть A, B, C — три подгруппы в группе G, причем A соизмерима с B, а B соизмерима с C. В частности, $|B : A \cap B|, |B : B \cap C| < \infty$. Из теоремы Пуанкаре вытекает, что

$$|B : A \cap B \cap C| = |B : (A \cap B) \cap (B \cap C)| < \infty.$$

Тогда тем более

$$|A \cap B : A \cap B \cap C|, |B \cap C : A \cap B \cap C| < \infty.$$

Теперь по теореме об индексе получаем, что

$$|A : A \cap B \cap C| = |A : A \cap B||A \cap B : A \cap B \cap C| < \infty,$$

$$|C : A \cap B \cap C| = |A : A \cap B||A \cap B : A \cap B \cap C| < \infty,$$

так что уже подгруппа $A \cap B \cap C$ имеет конечный индекс как в A, так и в C. Тем более, то же верно для $A \cap C$. Так как рефлексивность и симметричность соизмеримости очевидны, отношение соизмеримости является отношением эквивалентности.

Пусть $F, H \leq G$ — две соизмеримые подгруппы. Положим $|F : H| = |F : F \cap H|/|H : F \cap H|$. По определению $|F : H| \in \mathbb{Q}_+$.

Задача. Докажите, что

- для любой подгруппы $K \leq F \cap H$ такой, что $|F \cap H : K| < \infty$ имеем $|F : H| = |F : K|/|H : K|$;
- для любых трех попарно соизмеримых подгрупп F, H, K имеем $|F : H||H : K| = |F : K|$, в частности, $|F : H||H : F| = 1$;
- для любого $g \in G$ имеем $|F : H| = |gFg^{-1} : gHg^{-1}|$.

Следствие 3. *Любая подгруппа $H \leq G$ конечного индекса содержит нормальный делитель $F \trianglelefteq G$, $F \leq H$, конечного индекса.*

Доказательство. Пусть $|G : H| = n$ и $g_1, \ldots, g_n$ — трансверсаль к H в G. Тогда все подгруппы H^{g_i} имеют индекс n в G. Тем самым, по теореме Пуанкаре подгруппа $F = H^{g_1} \cap \ldots \cap H^{g_n} \trianglelefteq G$ имеет там конечный индекс.

Для решения следующей задачи полезно понимать связь между классом сопряженности элемента и централизатором этого элемента.

Задача. Пусть $H \trianglelefteq G$ — конечная нормальная подгруппа в G. Докажите, что тогда существует нормальная подгруппа $F \trianglelefteq G$ конечного индекса, поэлементно коммутирующая с H.

Решение. Возьмем элемент $h \in H$. Так как его сопряженный класс $h^G \leq H$ конечен, индекс $|G : C_G(h)|$ конечен. По теореме Пуанкаре подгруппа $\bigcap C_G(h)$, где пересечение берется по всем $h \in H$, также имеет конечный индекс в G. Эта подгруппа состоит из элементов, поэлементно коммутирующих с H. По следствию 3 любая подгруппа конечного индекса содержит нормальную подгруппу конечного индекса.

§ 20♠. Виртуальные группы

Во многих вопросах теории вероятностей, теории динамических систем, теории когомологий, теории арифметических групп и т. д. нет различия между самой группой и ее подгруппой конечного индекса. Точка зрения, не отличающая группу от ее подгрупп конечного индекса, называется **виртуальной***.

1. Виртуальные гомоморфизмы. Пусть H и G — две группы. Гомоморфизм $\phi : H' \longrightarrow G$, где $H' \leq H$ — подгруппа конечного индекса, называется **виртуальным гомоморфизмом** H в G и обозначается $\phi : H \dashrightarrow G$. При этом подгруппа H' называется **областью определения** виртуального гомоморфизма ϕ и обозначается через $D(\phi)$, а ее индекс $|H : H'|$ обозначается через $\mathrm{ind}(\phi)$ и называется **индексом** виртуального гомоморфизма ϕ. Если $H = G$, виртуальный гомоморфизм $G \dashrightarrow G$ называется **виртуальным эндоморфизмом**.

В действительности, виртуальные гомоморфизмы обычно рассматриваются не с точностью до равенства отображений, а с точностью до соизмеримости. Пусть $\phi : H \dashrightarrow G$ — виртуальный гомоморфизм, а $F \leq H$ — подгруппа конечного индекса. Тогда **ограничением** ϕ на F называется виртуальный гомоморфизм $\phi|_F : H \dashrightarrow G$ с областью определения $D(\phi) \cap F$. То, что это действительно виртуальный гомоморфизм, вытекает из теоремы Пуанкаре! Два виртуальных гомоморфизма $\phi : H \dashrightarrow G$ и $\psi : H \dashrightarrow G$ называются **соизмеримыми** (`commensurable`) $\phi \approx \psi$, если существует такая подгруппа $F \leq H$ конечного индекса, что $\phi|_F = \psi|_F$.

Для любой подгруппы $H \leq G$ конечного индекса определен тождественный виртуальный эндоморфизм $\mathrm{id}_H : G \dashrightarrow G$ с областью определения H. Пусть теперь

*Во избежание недоразумений стоит уточнить, что слово **виртуальный** здесь используется в своем *исконном* значении, *виртуально* противоположном тому, которое оно в последние годы приобрело в русском языке. **Виртуальный** означает здесь **действительный**, **действующий**, **эффективный**, **фактический**.

$\phi : F \dashrightarrow H$ и $\psi : H \dashrightarrow G$ – два виртуальных гомоморфизма. Их **композицией** называется частичное отображение $\psi \circ \phi : F \dashrightarrow G$, с областью определения $D(\psi \circ \phi) = \{x \in D(\phi) \mid \phi(x) \in D(\psi)\}$. Для любого $x \in D(\psi \circ \phi)$ значение $\psi \circ \phi$ на x можно определить обычным образом, $(\psi \circ \phi)(x) = \psi(\phi(x))$.

Задача. Проверьте, что композиция двух виртуальных гомоморфизмов является виртуальным гомоморфизмом. Что можно сказать об индексе $\mathrm{ind}(\psi \circ \phi)$?

Задача. Проверьте, что отношение соизмеримости $\approx$ является отношением эквивалентности.

Задача. Проверьте, что отношение соизмеримости является конгруэнцией по отношению к композиции. Иными словами, если $\phi_1, \phi_2 : F \dashrightarrow H$ и $\psi_1, \psi_2 : H \dashrightarrow G$, причем $\phi_1 \approx \phi_2$ и $\psi_1 \approx \psi_2$, то $\psi_1 \circ \phi_1 \approx \psi_2 \circ \phi_2$.

Так как композиция частичных отображений ассоциативна, то из этих трех задач вытекает, в частности, что как виртуальные эндоморфизмы $\mathrm{VEnd}(G)$, так и классы соизмеримости виртуальных эндоморфизмов $\mathrm{RVEnd}(G)$ группы G образуют моноиды относительно композиции, единицами которых являются id_G и класс соизмеримости id_G, соответственно.

2. Виртуальные группы. Категория **виртуальных групп** — это категория, объектами которой являются группы, а морфизмами — *классы соизмеримости* виртуальных гомоморфизмов. Все термины, в которые входит эпитет **виртуально**, понимаются по отношению к этой категории. Например, две группы, изоморфные в категории виртуальных групп, называются **виртуально изоморфными**, что обозначается $H \approx G$. Некоторые авторы называют виртуально изоморфные группы H и G **абстрактно соизмеримыми**, виртуальный изоморфизм называется в этом случае (абстрактной) **соизмеримостью** (commensuration).

Задача. Проверьте, что две группы H и G в том и только том случае виртуально изоморфны, когда в них существуют подгруппы конечного индекса $H' \leq H$, $G' \leq G$ изоморфные в обычном смысле:

$$H \approx G \qquad \Longleftrightarrow \qquad H' \cong G'.$$

3. Виртуальные эндоморфизмы $\mathbb{Z}^n$. Рассмотрим ключевой пример, иллюстрирующий введенные в предыдущих пунктах понятия. А именно, вычислим моноид классов виртуальных эндоморфизмов и группу классов виртуальных автоморфизмов группы $G = \mathbb{Z}^n$.

Задача. Докажите, что каждый виртуальный эндоморфизм $\phi : \mathbb{Z}^n \dashrightarrow \mathbb{Z}^n$ продолжается до линейного отображения $\phi \otimes \mathbb{Q} : \mathbb{Q}^n \longrightarrow \mathbb{Q}^n$.

Задача. Докажите, что построенное в предыдущей задаче продолжение $\phi \otimes \mathbb{Q}$ единственно.

Задача. Докажите, что два эндоморфизма $\phi, \psi : \mathbb{Z}^n \dashrightarrow \mathbb{Z}^n$ тогда и только тогда соизмеримы, $\phi \approx \psi$, когда $\phi \otimes \mathbb{Q} = \psi \otimes \mathbb{Q}$.

В частности, это означает, что $\mathrm{RVEnd}(\mathbb{Z}^n) \cong \mathrm{End}(\mathbb{Q}^n) \cong M(n, \mathbb{Q})$, как мультипликативные моноиды, и, тем самым, группа (классов) виртуальных автоморфизмов группы $\mathbb{Z}^n$ изоморфна $\mathrm{GL}(n, \mathbb{Q})$.

§ 21♢. Двойные смежные классы

Two BwB or not two BwB, that's the bottom line.

Frobenius—Chevalley—Tits

Сейчас мы рассмотрим важное обобщение понятие смежного класса, введенное в 1887–1894 годах Георгом Фробениусом [162] и Рихардом Дедекиндом [163]. В современных учебниках это понятие обычно спрятано в действия групп (орбиты подгруппы $F \leq G$ на однородном G-множестве G/H). Однако мне кажется, что начинающему *намного* проще понять доказательства многих классических теорем, если явно артикулировать их в терминах двойных смежных классов, как это, собственно, и делали Фробениус и Бернсайд. Содержание настоящего параграфа — в особенности формула индекса Фробениуса! — абсолютно необходимо для понимания большинства доказательств в главе 9.

1. Двойные смежные классы. Пусть $F, H \leq G$. Произведение вида

$$FgH = \{fgh \mid f \in F, h \in H\}$$

называется **двойным смежным классом** (`double coset`, `Doppelnebenklasse`) группы G по паре подгрупп (F, H). Множество всех двойных смежных классов обозначается через

$$F\backslash G/H = \{FgH \mid g \in G\}.$$

Вся теория алгебраических групп и весь гармонический анализ основаны на изучении этих множеств. Перенесем на них основные факты, относящиеся к обычным смежным классам.

Лемма 1. *Два двойных смежных класса FxH и FyH либо не пересекаются, либо совпадают.*

Доказательство. Пусть $z \in FxH \cap FyH$. Это значит, что z можно представить в виде $z = f_1xh_1 = f_2yh_2$, где $f_i \in F$, $h_i \in H$. Тогда $x = f_1^{-1}f_2yh_2h_1^{-1} \in FyH$, тем самым $FxH \leq FyH$. Доказательство обратного включения совершенно аналогично.

Таким образом, отношение $\sim$ на G, определенное посредством: $x \sim y$ если и только если $FxH = FyH$, является отношением эквивалентности, называемым **сравнимостью по двойному модулю** (F, H). Трансверсаль к этому отношению эквивлентности называется **системой представителей** двойных смежных классов по модулю (F, H).

Например, если $X = \{x_1, \ldots, x_n\}$ — система представителей смежных классов, то

$$G = Fx_1H \sqcup \ldots \sqcup Fx_nH.$$

Это разложение известно как **разложение на двойные смежные классы** по модулю (F, H) или, коротко, `Doppelnebenklassenzerlegung`.

Упражнение. Убедитесь, что в качестве системы представителей двойных смежных классов по модулю (H, F) можно взять

$$X^{-1} = \{x_1^{-1}, \ldots, x_n^{-1}\},$$

иными словами,

$$G = Hx_1^{-1}F \sqcup \ldots \sqcup Hx_n^{-1}F.$$

2. Формула Фробениуса для индекса. Сейчас мы докажем один из самых фундаментальных фактов всей теории групп, столь же элементарный, как теорема Лагранжа, но гораздо более `могущественный`.

Лемма 2. *Двойной смежный класс FxH содержит в точности*

$$|H : H \cap x^{-1}Fx|$$

левых смежных классов по F.

Доказательство. Каждый левый смежный класс по F, содержащийся в FxH имеет вид Fxh для некоторого $h \in H$. Ясно, что для двух $h, g \in H$ равенство $Fxh = Fxg$ означает в точности $hg^{-1} \in x^{-1}Fx$. Но так как изначально, кроме того, $hg^{-1} \in H$, то $hg^{-1} \in H \cap x^{-1}Fx$. Но это как раз и значит, что

$$Fxh = Fxg \quad \Longleftrightarrow \quad (H \cap x^{-1}Fx)h = (H \cap x^{-1}Fx)g,$$

как и утверждалось.

Следствие. *Двойной смежный класс FxH содержит в точности*

$$|F : F \cap xHx^{-1}|$$

правых смежных классов по H.

Доказательство. Лемма утверждает, что двойной класс $Hx^{-1}F$ содержит $|F : F \cap xHx^{-1}|$ левых смежных классов по H. Однако $fxH \mapsto$

$Hx^{-1}f^{-1}$ устанавливает биекцию между правыми смежными классами в FxH и левыми смежными классами в $Hx^{-1}F$.

Мы будем *десятки* раз пользоваться следующим утверждением, классически известным как **формула Фробениуса для индекса** = `Indexformel`, но последнее время все чаще называемым **формулой индекса Фробениуса** = `Frobenius index formula`*.

Indexformel. *Пусть* $G = Fx_1H \sqcup \ldots \sqcup Fx_nH$ — *разложение* G *по двойному модулю* (F, H). *Тогда*

$$|G : F| = |H : H \cap x_1^{-1}Fx_1| + \ldots + |H : H \cap x_n^{-1}Fx_n|.$$

Доказательство. В силу леммы 1 имеем $|G| = |Fx_1H| \sqcup \ldots \sqcup |FX_nH|$, осталось подставить сюда формулу для количества левых смежных классов по F, содержащихся в FxH, установленную в лемме 2.

Теорема Лагранжа является частным случаем этого утверждения, получающимся при $H = 1$.

Следствие. *В условиях теоремы*

$$|G : H| = |F : F \cap x_1Hx_1^{-1}| + \ldots + |F : F \cap x_nHx_n^{-1}|.$$

§ 22♢. Пересечения левых и правых смежных классов

Приведем еще несколько вариаций на тему леммы 2 предыдущего параграфа, с тем, чтобы парафразировать доказательство формулы Фробениуса. Хотя это второе доказательство не содержит ничего нового и даже чуть длиннее, в нем эксплицируется связь с пересечениями односторонних классов, а сама формула индекса принимает более симметричный вид, который, по-видимому, легче запомнить тому, кто видит формулу в первый раз.

Пусть $F, H \leq G$. Что можно сказать о пересечениях *левых* смежных классов Fx и *правых* смежных классов yH? Сейчас мы дадим полный ответ на этот вопрос. Лемма 1 утверждает, что два двойных смежных класса по (F, H) либо не пересекаются, либо совпадают. Это можно сформулировать чуть иначе, а именно: если Fx и Fy — два левых смежных класса по F, то множества правых смежных классов

*В этом месте те из первокурсников, кто еще не слышал о нарушении ассоциативности в языке, обычно спрашивают меня, что такое **индекс Фробениуса**.

zH таких, что $Fx\cap zH\neq\varnothing$ и $Fy\cap zH\neq\varnothing$ либо не пересекаются, либо совпадают. Таким образом, если множество двойных смежных классов $F\backslash G/H$ конечно, то левые смежные классы $F\backslash G$ и правые смежные классы G/H можно разбить на одинаковое количество $n=|F\backslash G/H|$ дизъюнктных блоков $F\backslash G=X_1\sqcup\ldots\sqcup X_n$ и $G/H=Y_1\sqcup\ldots\sqcup Y_n$ так что если $Fx\in X_i$, $yH\in Y_j$ и $Fx\cap yH\neq\varnothing$, то $i=j$. Оказывается, этот результат можно уточнить, а именно, если $Fx\in X_i$ и $yH\in Y_i$, то порядок их пересечения $Fx\cap yH$ зависит не от самих классов Fx и yH, а только от i.

Предложение. *Если $Fx\cap yH, Fx\cap zH\neq\varnothing$, то $|Fx\cap yH|=|Fx\cap zH|$.*

Доказательство. Пусть $u\in Fx\cap yH$, $v\in Fx\cap zH$. Тогда $Fu=Fx=Fv$, $uH=yH$ и $vH=zH$ и, таким образом,

$$Fx\cap yH=Fu\cap uH=u(u^{-1}Fu\cap H),$$

$$Fx\cap zH=Fv\cap vH=v(v^{-1}Fv\cap H).$$

С другой стороны, так как $Fu=Fv$, то $u^{-1}Fu=v^{-1}Fv$ (проверьте!). Это значит, что оба пересечения $Fx\cap yH$ и $Fx\cap zH$ являются смежными классами по одной и той же подгруппе $u^{-1}Fu\cap H$, и, тем самым,

$$|Fx\cap yH|=|u^{-1}Fu\cap H|=|Fx\cap zH|,$$

как и утверждалось.

В частности, отсюда получается такое обобщение формулы произведения: $|F|\cdot|H|=|FgH|\cdot|F\cap gHg^{-1}|$. Сформулируем его чуть иначе.

Allgemeine Produktformel. *Если $F,H\leq G$ подгруппы конечной группы G, $g\in G$, то*

$$|FgH|=\frac{|F|\cdot|H|}{|F\cap gHg^{-1}|}.$$

Обычная формула произведения получается если подставить сюда $g=1$. Теперь у нас все готово, чтобы еще раз доказать формулу Фробениуса. В самом деле, суммируя общую формулу произведения по всем классам $G=Fx_1H\sqcup\ldots\sqcup Fx_nH$, получаем

$$|G|=\sum_{i=1}^{n}\frac{|F||H|}{|F\cap x_iHx_i^{-1}|}.$$

Обе части формулы можно разделить хоть на $|H|$, хоть — воспользовавшись тем, что $|F \cap x_i H x_i^{-1}| = |x_i^{-1} F x_i \cap H|$ — на $|F|$.

Коан. А теперь вернемся к примеру, рассмотренному нами в § 16. Возьмем, как и там,

$$G = \begin{pmatrix} \mathbb{Q}^* & \mathbb{Q} \\ 0 & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}.$$

Тогда класс HgH по двойному модулю (H, H) совпадает с левым классом Hg, но при этом представляется как объединение n правых классов по H:

$$HgH = Hg = g_1 H \sqcup \ldots \sqcup g_n H.$$

Почему это не противоречит результатам настоящего параграфа?

§ 23♠. Алгебра Гекке

В этом параграфе мы введем одну из важнейших общих конструкций теории групп — алгебры Гекке. Алгебры Гекке в полной общности были впервые определены Горо Шимура в начале 1950-х годов, две известные мне трактовки этого сюжета в такой общности на русском языке даны в упражнениях Бурбаки и в книге Шимура. Мое изложение следует [164].

Эрих Гекке (Erich Hecke, 20 сентября 1887, Познань — 13 февраля 1947, Копенгаген) — замечательный немецкий математик, один из классиков теории чисел. Гекке учился во Вроцлаве и Берлине, а потом в Геттингене, под руководством Гильберта. Уже в 1910 году он получил там **докторат**, а в 1912 году — **хабилитацию**. В 1919 году Гекке становится профессором в только что созданном университете Гамбурга. Его самые знаменитые работы относятся к теории модулярных форм и рядов Дирихле. Именно в этом контексте он ввел прославившие его имя операторы Гекке и алгебры Гекке. Кроме того, в нашем курсе встречается конгруэнц-подгруппа Гекке.

1. Пары Гекке. Сейчас мы сведем воедино три обсуждавшиеся только что темы: системы общих представителей, соизмеримость и двойные смежные классы. Говорят, что $H \leq G$ — **подгруппа Гекке** в G, если для любого $g \in G$ подгруппы H и gHg^{-1} соизмеримы. В этом случае говорят также, что (G, H) — **пара Гекке**.

Терминологический комментарий. Некоторые авторы называют такую подгруппу H **почти нормальной** в G, но эта практика порочна, так как выражение **почти нормальная подгруппа** в теории групп имеет другой твердо установленный смысл. Подгруппа $H \leq G$ называется **почти нормальной** в G, если ее нормализатор имеет конечный индекс в G, т. е. $|G : N_G(H)| < \infty$. Иными словами, H имеет в G лишь конечное число сопряженных. Мы же утверждаем нечто совершенно другое. Термин **подгруппа Гекке** тоже не идеален, но никакой подходящей альтернативы мне не известно.

Вот три очевидных примера подгрупп Гекке:

• любой нормальный делитель $H \trianglelefteq G$,

• любая конечная подгруппа $H \leq G$,

• любая подгруппа $H \leq G$ конечного индекса

— где-то мы все это уже видели!!

А вот зачем это вводил Шимура. Из § 21 мы знаем, что двойной смежный класс HgH содержит $|H : H \cap g^{-1}Hg|$ левых смежных классов по H и $|H : H \cap gHg^{-1}|$ правых смежных классов по H. Таким образом, мы получаем следующий результат.

Предложение. *Для подгруппы $H \leq G$ следующие условия эквивалентны:*

• *каждый двойной класс HgH, $g \in H$, содержит конечное число левых смежных классов по H;*

• *каждый двойной класс HgH, $g \in H$, содержит конечное число правых смежных классов по H;*

• *H является подгруппой Гекке в G.*

Сейчас мы свяжем с каждой парой Гекке (G, H) некоторый гомоморфизм $\mathrm{gear}_H : G \longrightarrow \mathbb{Q}_+$, **передаточное число**. Равенство передаточного числа 1 означает, что у подгруппы H найдется система общих представителей.

Задача. См., например, [165]. Докажите, что отображение $\mathrm{gear}_H : G \mapsto \mathbb{Q}_+$, $g \mapsto |gHg^{-1} : H|$, является гомоморфизмом.

Решение. В самом деле,

$$|ghHh^{-1}g^{-1} : H| = |ghHh^{-1}g^{-1} : gHg^{-1}||gHg^{-1} : H| = |hHh^{-1} : H||gHg^{-1} : H|.$$

Вернемся теперь к анализу примера, который встречался нам в § 17 по поводу систем общих представителей и потом еще раз в предыдущем параграфе.

Задача. (Бост и Конн, [166]) Убедитесь, что (G, H) — пара Гекке и

$$\mathrm{gear}_H \begin{matrix} x & y \\ 0 & 1 \end{matrix} = x.$$

Вот теперь мы можем сказать, что полностью понимаем все, что происходило вокруг этого примера!

2. Алгебра двойных смежных классов. Пусть $H \leq G$. Тогда произведение двух двойных смежных классов HxH и HyH снова является объединением двойных смежных классов. Если (G, H) — пара Гекке, то можно сказать гораздо больше!

Задача. Докажите, что если (G, H) — пара Гекке, то:

• $HxH \cdot HyH$ является объединением конечного числа смежных классов;

• количество представлений элемента $g \in HzH$ в виде произведения элемента из HxH и элемента из HyH не зависит от выбора g, а только от самого класса HzH.

Пусть $HyH = w_1H \sqcup \ldots \sqcup w_nH$. Тогда

$$HxH * HyH =$$

$$|H : H \cap xHx^{-1}| \quad \frac{Hxw_1H}{|H : H \cap xw_1Hw_1^{-1}x^{-1}|} + \ldots + \frac{Hxw_nH}{|H : H \cap xw_nHw_n^{-1}x^{-1}|}\Bigg).$$

Глава 3. НОРМАЛЬНЫЕ ПОДГРУППЫ И ФАКТОР-ГРУППЫ

Я не имею права задерживать нормального человека в лечебнице. Тем более, что у меня и мест не хватает. И я вас сию же секунду выпущу, если только вы мне скажете, что вы нормальны. Не докажете, поймите, а только скажете. Итак, вы — нормальны?

Михаил Булгаков. *Великий Канцлер*

Здесь мы обсуждаем три ключевых понятия теории групп: нормальные делители, сопряженность и фактор-группы. Переход от уровня абстракции, который ассоциируется со школьной алгеброй, к тому уровню абстракции, который ассоциируется с алгеброй университетской, связан ровно с одной конструкцией — рассмотрением фактор-объектов. Тот, кто в состоянии понять, что такое фактор-группа, в состоянии полностью овладеть всем содержанием настоящего курса.

§ 1♢. Нормальные подгруппы, простые группы

В этом параграфе мы рассмотрим такие подгруппы $H \leq G$, для которых отношения сравнимости по модулю H слева и справа совпадают.

1. Нормальные подгруппы. Сейчас мы введем *важнейший* класс подгрупп, а именно, нормальные подгруппы, впервые определенные в 1830 году Эваристом Галуа (сам Галуа называл их **инвариантными**). Собственно говоря, с этого момента предсуществование теории групп и переходит в существование. Как выяснится в дальнейшем, нормальные подгруппы — это *в точности* такие подгруппы в G, отношение сравнимости по модулю которых является конгруэнцией на G. Иными словами — это *в точности* такие подгруппы в G, что на множестве G/H смежных классов по H можно *естественным образом* ввести структуру группы!

Определение. *Подгруппа H группы G называется* **нормальной** *в G, если для любого $x \in G$ левый смежный класс элемента x по H совпадает с правым:*

$$Hx = xH.$$

Чтобы обозначить, что H нормальна в G, пишут $H \trianglelefteq G$ или $G \trianglerighteq H$.

Таким образом, подгруппа H в том и только том случае нормальна в G, когда для любых двух элементов $x, y \in G$, включение $xy^{-1} \in H$ эквивалентно включению $x^{-1}y \in H$. В старинных книгах нормальные подгруппы чаще назывались **нормальными делителями** (от немецкого `Normalteiler`) или **инвариантными подгруппами** (от французского `sous-groupe invariant`, `sous-groupe distingué`, также и по-немецки иногда использовалось выражение `invariante Untergruppe` и, совсем редко, `ausgezeichnete Untergruppe`). Мы уже отмечали, что второе из этих названий восходит к самому Галуа, сдругой стороны термин `Normalt[h]eiler` предложил Генрих Вебер в своем классическом учебнике алгебры. Однако в последние 20–30 лет в русском математическом узусе существует устойчивая тенденция к униформизации лексики и вытеснению заимствований немецкого и французского происхождения терминологией, конформной с англоязычной нормой, поэтому в настоящее время выражение *нормальная подгруппа* (`normal subgroup`) превратилось в *единственную* употребительную форму.

Следующая задача дает весьма выразительную переформулировку того, что подгруппа H нормальна в G, и у меня было сильное искушение принять именно этот критерий за *определение* нормальности. Однако после некоторой внутренней борьбы традиция победила.

Задача. Докажите, что подгруппа $H \leq G$ в том и только том случае нормальна в G, когда для любых $x, y \in G$ из $xy \in H$ следует, что $yx \in H$.

2. Очевидные нормальные делители[♮]**.** Во всякой группе есть два **очевидных** нормальных делителя. А именно, **тривиальный** нормальный делитель $1 \trianglelefteq G$ и **несобственный** нормальный делитель $G \trianglelefteq G$. Будем писать $H \triangleleft G$, чтобы подчеркнуть, что H **собственная** нормальная подгруппа.

Основной интерес в теории групп представляют группы, в которых нет никаких неочевидных нормальных делителей. Группа G называется **простой**, если $G \neq 1$ и из того, что $H \trianglelefteq G$ вытекает, что

[♮]Алексей Степанов отметил явное противоречие этой фразы с декларацией, что термин **нормальная подгруппа** превратился сегодня в *единственную* употребительную форму. Тут и комментировать нечего, все ясно: *The well-bred contradict other people. The wise contradict themselves* — Воспитанные люди противоречат другим. Мудрые противоречат себе. Мой собственный слог (с)формировался в то время, когда вся русскоязычная математическая лексика была основана на немецких образцах. Поэтому *субстанциально* пропагандируя термин **нормальная подгруппа**, *акцидентально* я сбиваюсь на термины **нормальное делимое**, **нормальный делитель**, **нормальное частное**.

Генрих Вебер (Heinrich Martin Weber, 5 мая 1842, Гейдельберг — 17 мая 1913, Страсбург) — замечательный немецкий математик, один из величайших классиков алгебры и теории чисел. После обучения в Гейдельберге и Лейпциге он в 1863 году получает докторскую степень, еще через 3 года заканчивает в Кенигсберге работу над **хабилитацией**. В течение следующих 30 лет он преподает в университетах Гейдельберга и Кенигсберга, и в Eidgenossische Technische Hochschule в Цюрихе, а в 1895 году окончательно обосновывается в Страсбурге. Основные работы Вебера относятся к теории алгебраических функций и теории алгебраических чисел.

Сегодня чаще всего вспоминают два его достижения. Прежде всего, это работа Дедекинда и Вебера 1882 года *Theorie der algebraischen Funktionen einer Veränderlichen*, в которой — руководствуясь аналогией с арифметикой числовых полей — чисто алгебраически строится арифметика полей алгебраических функций над произвольным полем констант. Часто цитируется следующая поразительная фраза из этой работы: "Две точки *называются* различными, если существует функция, принимающая в них различные значения." Тем самым Дедекинд и Вебер — подобно Гельфанду, Гротендику и Джету Неструеву, но в противоположность Риману — стартуют непосредственно с *кольца* функций и только потом вводят то пространство, где эти функции определены! Столь же знаменита теорема Кронекера—Вебера, сформулированная Кронекером в 1853 году и доказанная Вебером в 1886 году, которая послужила отправной точкой для теории полей классов.

Еще одним замечательным достижением Вебера, обессмертившим его имя, стал классический двухтомный труд *Lehrbuch der Algebra*. Эта удивительная книга не только значительно полнее, но во многих отношениях гораздо *современнее* большинства учебников алгебры, написанных 50 лет спустя. Ее чтение и сегодня производит *огромное* впечатление. Мои собственные оценки в том, что касается вопросов приоритета в применении к XIX веку, в основном следуют Веберу.

Кроме алгебры, алгебраической геометрии и теории чисел Вебер работал в других областях математики, главным образом анализе и математической физике. Тем не менее, его не следует путать с физиком **Вильгельмом Вебером** (Wilhelm Eduard Weber, 24 октября 1804, Виттенберг — 23 июня 1891 Геттинген), основные работы которого относились к электричеству и магнетизму и в честь которого названы физические единицы **вебер** и **гаусс**.

$H = 1$ или $H = G$. Простые группы являются блоками, из которых собраны все остальные группы и сами не могут быть разобраны на меньшие составные части. При этом, в отличие от (бессмысленной!) задачи классификации всех групп, классификация простых групп различных классов, хотя и очень сложна, но возможна. В частности, центральными достижениями математики XX века были классификация простых алгебраических групп и классификация простых конечных групп. В действительности, в соответствии с нашим сегодняшним уровнем понимания, именно классификация простых групп и изучение их строения является основной

ЗАДАЧЕЙ ТЕОРИИ ГРУПП.

3. Максимальные и минимальные нормальные подгруппы. В доказательстве многих результатов теории (конечных) групп совершенно особую роль играют атомы и коатомы структурной решетки:

• Подгруппа $H \trianglelefteq G$ называется **минимальной нормальной подгруппой**, если она является минимальным элементом в множестве *нетривиальных* нормальных делителей. Иными словами, $H \neq 1$ и не существует такой подгруппы $1 < F < H$, что $F \trianglelefteq G$. В следующей главе мы докажем, что минимальная нормальная подгруппа конечной группы является произведением попарно изоморфных простых групп.

• Подгруппа $H \trianglelefteq G$ называется **максимальной нормальной подгруппой**, если она является максимальным элементом в множестве *собственных* нормальных делителей. Иными словами, $H \neq G$ и не существует такой подгруппы $H < F < G$, что $F \trianglelefteq G$.

Из теоремы о соответствии сразу следует, что максимальные нормальные подгруппы, это в точности такие нормальные подгруппы, что фактор-группа G/H проста. Для минимальных нормальных делителей в главе 4 будет доказан аналогичный, но чуть более сложный результат.

§ 2◇. Первые примеры нормальных подгрупп

Укажем несколько очевидных примеров нормальных делителей. В дальнейшем, когда мы научимся строить нормальные делители из гомоморфизмов и сопряженных классов, возникнет много других, более интересных примеров.

1. Совсем очевидные примеры. Совпадение левого с правым *заведомо* имеет место, если H коммутирует со всем на свете — в действительности, нормальность H как раз и означает, что H коммутирует ПО МОДУЛЮ H со всем на свете.

• **Подгруппы абелевой группы.** В абелевой группе $Hx = xH$ для любой подгруппы H и любого элемента $x \in G$. Тем самым, в абелевой группе *все* подгруппы нормальны.

• **Центральные подгруппы.** Предыдущий пример допускает следующее очевидное обобщение: если $H \leq C(G)$, то $H \trianglelefteq G$.

• **Гамильтоновы группы.** Следующее понятие ввел в 1896 году Рихард Дедекинд [168]. Группа G называется **гамильтоновой**, если все ее подгруппы нормальны — иногда при этом еще требуется, чтобы сама G не была абелевой. Важнейшим примером гамильтоновой

группы является группа Q кватернионных единиц. Мы знаем, что в Q имеется ровно 6 подгрупп, 1, $\{\pm 1\}$, G и три подгруппы вида $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$. Подгруппы 1 и G являются очевидными нормальными делителями, подгруппа $\{\pm 1\}$ совпадает с центром Q и, значит, нормальна, а все остальные подгруппы имеют индекс 2 в Q и, тем самым, как мы убедимся в следующем пункте, тоже нормальны.

Пока же, из чистого любопытства приведем полное описание гамильтоновых подгрупп. Оказывается, группа кватернионов является *по существу* единственным примером неабелевой гамильтоновой группы. Для конечных групп следующий результат был доказан Дедекиндом в цитированной работе, а в общем случае Рейнольдом Бэром в 1933 году [169].

Рейнольд Бэр (Reinhold Baer, 22 июля 1902, Берлин — 22 октября 1979, Цюрих) — замечательный немецкий алгебраист, основные работы которого связаны с теорией бесконечных групп, линейной алгеброй, геометрией, топологией и комбинаторикой. Бэр учился в Ганновере, Фрайбурге и Геттингене, где попал под влияние Эмми Нетер и Хельмута Кнезера. После этого он на год поехал в Киль, где работал с Хассе, Штейницем и Теплицом и в 1925 году защитил диссертацию в Геттингене. В 1928 году он получил постоянную позицию в Халле, но весной 1933 года, когда он был на каникулах в Австрии, ему сообщили, что *в его услугах больше не нуждаются*. Бэр тут же направился в Великобританию, а в 1935 году в США, в Институт высших научных исследований, где два года был ассистентом Германа Вейля (может быть проще перечислять тех немецких алгебраистов, кто *не был* ассистентом Вейля в Принстоне?) В эти годы основные его работы относятся к теории бесконечных абелевых групп, в частности, он вводит ключевое понятие произведения расширений по Бэру, которое послужило одним из важнейших шагов в формировании гомологической алгебры. Кстати, именно Бэр ввел и понятие инъективного модуля, ставшее еще одним из ключевых инструментов гомологической алгебры. В 1938 году Бэр получает профессорскую позицию в Университете Иллинойса Urbana-Champagne, но в 1956 году решает вернуться в Германию и становится профессором во Франкфурте. Начиная с 1950 года он все больше переключается на теорию бесконечных групп (условия конечности, обобщения нильпотентных и разрешимых групп и т. д.) Здесь с его именем связаны десятки понятий и результатов: проблема Бэра, радикал Бэра, группы Бэра и т. д. В книге Куроша цитируются 79 его статей, а его фамилия в тексте упоминается *по крайней мере* 82 раза, т. е. даже чаще, чем самого Куроша.

Не следует путать Рейнольда Бэра ни с французским аналистом **Рене Бэром** (René-Louis Baire, 21 января 1874, Париж — 5 июля 1932, Шамбри), ни с **Хельмутом Бером** (Helmut Behr), которые оба ему даже не однофамильцы! Однако, Хельмут Бер тоже работал в области теории групп и тоже был профессором во Франкфурте!!

Теорема. *Любая (неабелева) гамильтонова группа представлима в виде прямого произведения $Q \times A \times B$, где A абелева группа, все элементы которой имеют*

конечный нечетный порядок, а B — (абелева) группа, все элементы которой имеют период 2.

• **Образ нормальной подгруппы.** Если $H \trianglelefteq G$, а $\varphi \in \mathrm{Aut}(G)$, то $\varphi(H) \trianglelefteq G$.

2. Подгруппы простого индекса. Каждая подгруппа индекса 2 является нормальным делителем. В самом деле, в этом случае $G = H \sqcup (G \setminus H)$ является разбиением G как на левые, так и на правые смежные классы по H. Если $x \in H$, то $Hx = H = xH$. Если же $x \notin H$, то $Hx \neq H$ и $xH \neq H$, и, значит, $Hx = G \setminus H = xH$. Важнейший пример — **знакопеременная группа** A_n, состоящая их всех четных перестановок степени n. Эта подгруппа имеет индекс 2 в симметрической группе S_n и, следовательно, согласно только что сделанному наблюдению, $A_n \trianglelefteq S_n$.

Упражнение. Если $|G : H| = 2$, то для любого $g \in G$ имеем $g^2 \in H$.

Это упражнение легко обобщить. Мичио Судзуки (глава 1, § 4) называет следующее утверждение **теоремой Оре**, но в действительности задачка с такой формулировкой содержится уже в книге Бернсайда, который **аттрибутирует** этот факт Фробениусу. Скорее всего, правы оба, просто первые два доказательства были известны — или, как сформулировал бы эту мысль Шпенглер, должны были быть известны — Фробениусу, а следующие два — Оре.

Теорема. *Пусть p — наименьшее простое, делящее порядок группы G. Тогда любая подгруппа $H \leq G$ индекса p нормальна в G.*

Иными словами, утверждается, что подгруппа индекса 3 в группе *нечетного* порядка нормальна. В следующем параграфе мы увидим, что подгруппа индекса 3 в группе *четного* порядка уже совсем не обязана быть нормальной! По причинам личного свойства я приведу четыре доказательства этой теоремы, еще одно доказательство обсуждается в главе VI.

Доказательство 1. Если $x \in G \setminus H$, то $xH \cap H = \varnothing$, но $xH \cap Hx \neq \varnothing$. Таким образом, число m правых смежных классов Hy, $y \in G$, которые пересекаются с xH, удовлетворяет неравенствам $1 \leq m \leq p-1$. По доказанной в § 21 главы 2 теореме, порядки всех непустых пересечений $xH \cap Hy$ одинаковы, так что m делит $|H|$ и, тем самым, по теореме Лагранжа m делит $|G|$. Так как $m < p-1$, то $m = 1$, но это и значит, что $xH = Hx$.

Соедующее доказательство воспроизводится в [170] со ссылкой на Фробениуса.

Доказательство 2. Пусть $G = Hx_1H \sqcup \ldots \sqcup Hx_mH$ — разложение G на двойные смежные классы по модулю (H, H). Записывая Indexformel Фробениуса

$$p = |G : H| = |H : H \cap x_1Hx_1^{-1}| + \ldots + |H : H \cap x_mHx_m^{-1}|$$

для этого случая, мы видим, что все индексы в правой части делят $|H|$ и, тем самым, $|G|$. Так как H собственная подгруппа, $m \geq 2$. С другой стороны, так как p — наименьшее простое, делящее $|G|$, все эти индексы равны 1 и, значит, $H = x_iHx_i^{-1}$ для всех $i = 1, \ldots, m$, как и утверждалось.

Следующие два решения, которые я впервые прочел в книге Мичио Судзуки, имеют непустое пересечение и я сформулирую его в виде отдельной леммы.

Лемма. *Пусть p — наименьшее простое, делящее порядок группы G, а $H \leq G$ — подгруппа в G индекса p. Если $H \not\trianglelefteq G$, то для любого $x \in G \setminus H$ имеем $|H : H \cap H^x| = p$.*

Доказательство. По теореме Лагранжа H максимальна в G, так что $N_G(H) = H$. Это значит, что для любого $x \in G \setminus H$ имеем $H^x \neq H$ и, значит $H \cap H^x \neq H$. Поэтому $1 \neq |H \cap H^x \neq H| \leq |G : H^x| = |G : H| = p$. Так как p наименьшее простое, делящее порядок G, то $|H \cap H^x \neq H| = p$.

Доказательство 3. Если $H^x \neq H$, то по формуле произведения

$$|HH^x| = |H|^2/|H \cap H^x| = |H||H : H \cap H^x| = |H|p = |G|.$$

Значит $G = HH^x$, что невозможно (см. § 8).

Доказательство 4. Предположим, что (G, H) — контрпример минимального порядка. Так как $|H : H \cap H^x| = |H^x : H \cap H^x| = p$, а $|H| = |H^x| < |G|$, то в силу минимальности $H \cap H^x \trianglelefteq H, H^x$. Тогда $H \cap H^x \trianglelefteq \langle H, H^x\rangle = G$. Но ведь фактор-группа $G/H \cap H^x$ имеет порядок p^2 и, значит, абелева. Тем самым, $H/H \cap H^x \trianglelefteq G/H \cap H^x$ и по теореме о соответствии $H \trianglelefteq G$.

3. Централизатор и нормализатор. Рассмотрим подмножество $X \subseteq G$. В главе 2 мы определили централизатор $C_G(X)$ и нормализатор $N_G(X)$ множества X.

Задача. Докажите, что

$$C_G(gXg^{-1}) = gC_G(X)g^{-1}, \qquad N_G(gXg^{-1}) = gN_G(X)g^{-1}.$$

Задача. Докажите, что $C_G(X) \trianglelefteq N_G(X)$.

Следствие. $N_G(X) \leq N_G(C_G(X))$.

В случае, когда $H \leq G$ есть не просто подмножество, а подгруппа в G, фактор-группа $N_G(H)/C_G(H)$ часто называется **группой Вейля** подгруппы H.

Задача. Докажите, что $N_G(H)/C_G(H) \leq \mathrm{Aut}(H)$.

Это простое утверждение имеет массу важных следствий. Например, в следующей главе мы узнаем, что группа $\mathrm{Aut}(C_n)$ циклической группы абелева.

Следствие. *Группа Вейля $N_G(H)/C_G(H)$ любой циклической подгруппы $H \leq G$ абелева.*

Типичный пример группы Вейля, который, собственно, и дал название общей ситуации — это группа Вейля диагональной группы $D = D(n, K)$ в полной линейной группе $G = \mathrm{GL}(n, K)$.

Задача. Докажите, что $N_G(D)/C_G(D) \cong S_n$.

§ 3◇. Не каждая подгруппа нормальна

> Шигашов и Горбовский вообще прекратили здороваться. Заспорили, кто из них менее нормальный.
>
> "До чего же ты стал нормальный!" — укорял приятеля Шигашов.
>
> "Я-то ненормальный, — защищался Горбовский, — абсолютно ненормальный. У меня есть справка из психоневрологического диспансера ... А вот ты — не знаю. Не знаю ... "
>
> Сергей Довлатов. *Невидимая книга*

Сейчас мы приведем два примера подгрупп, весьма далеких от нормальных.

1. Минимальный контрпример. Все подгруппы абелевой группы нормальны. Самая маленькая неабелева группа — это группа $G = D_3 \cong S_3$ симметрий правильного треугольника. В обозначениях главы 5 эта группа состоит из следующих 6 преобразований:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Рассмотрим следующую подгруппу в G:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Легко видеть, что $H\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \neq \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}H$, так как левый класс содержит $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, а правый – не содержит.

2. Стабилизатор точки в S_n. Укажем следующее обобщение этого примера, которое объясняет, что здесь в действительности происходит. Пусть $G = S_n$ — симметрическая группа степени n, а H — подгруппа в G, состоящая из преобразований, фиксирующих n. Ясно, что $H \cong S_{n-1}$ и, значит, $|G : H| = n$. Рассмотренный выше пример — это в точности частный случай этого при $n = 3$. Две перестановки π, σ в том и только том случае лежат в одном *левом* смежном классе по H, когда $\pi\sigma^{-1} \in H$, т. е. когда $\pi\sigma^{-1}(n) = n$ или, что то же самое, $\pi^{-1}(n) = \sigma^{-1}(n)$. Таким образом, левые смежные классы G по H имеют вид

$$\{\pi \in S_n \mid \pi(i) = n\}, \qquad i = 1, \dots, n.$$

В то же время π, σ в том и только том случае лежат в одном *правом* смежном классе по H, когда $\pi^{-1}\sigma \in H$, т. е. когда $\pi^{-1}\sigma(n) = n$ или, что то же самое, $\pi(n) = \sigma(n)$. Тем самым, правые смежные классы имеют вид

$$\{\pi \in S_n \mid \pi(n) = i\}, \qquad i = 1, \dots, n.$$

Ясно, что условия $\pi(i) = n$ и $\pi(n) = i$ совершенно различны. За исключением, конечно, случая $n = 2$, когда каждый элемент имеет период 2, и, поэтому, равенство $\pi(i) = 2$ равносильно равенству $\pi(2) = i$.

3. Стабилизатор точки в $\mathrm{GL}(n, K)$. Рассмотрим теперь подгруппу $Q \leq \mathrm{GL}(n, K)$, состоящую из всех матриц, первый столбец которых совпадает с первым столбцом единичной матрицы. С геометрической точки зрения Q — это в точности стабилизатор столбца $e_1 \in K^n$. Две матрицы $h, g \in GL(n, K)$ в том и только том случае лежат в одном левом смежном классе по Q, когда $hg^{-1} \in Q$, т. е. когда первые столбцы матриц h^{-1} и g^{-1} совпадают. С другой стороны, h, g в том и только том случае лежат в одном правом смежном классе по Q, когда $h^{-1}g \in Q$, т. е. когда первые столбцы матриц h и g совпадают. Итак, левые смежные классы G по Q имеют вид

$$\{g \in \mathrm{GL}(n, K) \mid g'_{*1} = v\}, \qquad v \in K^n \setminus \{0\},$$

а правые — вид

$$\{g \in \mathrm{GL}(n, K) \mid g_{*1} = v\}, \qquad v \in K^n \setminus \{0\}.$$

В этом случае также ясно, что в общем случае $g'_{*1} = v$ и $g_{*1} = v$ отнюдь не эквивалентны. Достаточно взглянуть на матрицы

$$h = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

первые столбцы которых совпадают, а первые столбцы обратных к ним матриц различаются.

§ 4♢. Классы сопряженных элементов

Сейчас мы введем одно из *важнейших* понятий всей теории групп.

1. Классы сопряженных элементов. Посмотрим, что означает условие $xH = Hx$. Домножая это равенство на x^{-1} справа и пользуясь ассоциативностью, мы видим, что оно эквивалентно равенству $xHx^{-1} = H$. Здесь xHx^{-1} понимается обычным образом, как $\{xhx^{-1} \mid h \in H\}$. Это мотивирует следующее определение.

Определение. *Пусть $x, g \in G$. Элемент ${}^x g = xgx^{-1}$ называется* **сопряженным к* g при помощи x слева**. *Два элемента $h, g \in G$ называются* **сопряженными в G**, *если найдется такое $x \in G$, что $h = xgx^{-1}$. Множество всех элементов, сопряженных с g в группе G, обозначается*[♮]

$$g^G = \{xgx^{-1} \mid x \in G\}$$

и называется **классом сопряженных элементов** *группы G с представителем g.*

В дальнейшем вместо официального выражения `класс сопряженных элементов` мы часто употребляем общепринятые жаргонизмы **класс сопряженности** = `conjugacy class` и даже **сопряженный класс** = `Konjugiertenklass`.

---

*Роберт Шмидт заметил, что по-русски лучше говорить `сопряженный с`. С моей точки зрения, в зависимости от *контекстуальных пресуппозиций* возможны оба варианта. Однако в общем положении я предпочитаю говорить `conjugate to`, а не `conjugate with`. Вероятно, подсознательно это связано с популярной в годы моего детства песенкой `look what you've done to my life` — вариант `with my life` тоже возможен, но указывает на симметрию и длительность процесса. Обратите внимание, что *в любом случае* `conjugate`, а не `conjugated`, как *ошибочно* пишут почти все русские математики.

♮Конечно, рассматривая левое сопряжение было бы логичнее писать ${}^G g$. Однако, через секунду мы увидим, что ${}^G g = g^G$, так что нет никакого смысла вводить нестандартное обозначение.

Чтобы обозначить, что h и g сопряжены в G пишут $h \sim_G g$ или, если группа G зафиксирована контекстом, просто $h \sim g$. Элемент $g^x = x^{-1}gx$ называется **сопряженным к** g **при помощи** x **справа**. Резюмируем важнейшие свойства отображения $(x, g) \mapsto x^g$, которые будут многократно использоваться в дальнейшем.

Задача. Докажите, что

- $x^{hg} = (x^h)^g$,
- $(xy)^g = x^g y^g$,
- $(x^{-1})^g = (x^g)^{-1}$.

Так как $g^x = x^{-1}gx = {}^{x^{-1}}g$, сопряжен к g при помощи x^{-1} слева, то ни понятие сопряженности, ни понятие сопряженного класса не меняются при замене сопряжения слева сопряжением справа. Разные авторы понимают выражение "элемент, сопряженный к g при помощи x" по-разному. Можно привести соображения в пользу и того и другого выбора, но нужно иметь в виду, что сопоставление элементу x **левого** сопряжения I_x при помощи этого элемента является **гомоморфизмом** G в симметрическую группу S_G, в то время, как сопоставление ему **правого** сопряжения $I_{x^{-1}}$ – **антигомоморфизм** (см. главы 4 и 6).

Предложение. *Сопряженность в группе G является отношением эквивалентности.*

Доказательство. Рефлексивность вытекает из того, что $1 \in G$. Симметричность вытекает из существования обратных: $h \sim_G g$ означает по определению, что найдется такое $x \in G$, что $xhx^{-1} = g$. Но тогда, разумеется, $h = x^{-1}gx$. Наконец, транзитивность вытекает из замкнутости G относительно умножения. Если $f \sim_G h$ и $h \sim_G g$, то найдутся такие $x, y \in G$, что $xfx^{-1} = h$ и $yhy^{-1} = g$. Но тогда $(yx)f(yx)^{-1} = y(xfx^{-1})y^{-1} = yhy^{-1} = g$.

Тем самым группа G представляется в виде *дизъюнктного* объединения классов сопряженных элементов. Трансверсаль Z к отношению сопряженности называется **системой представителей** классов сопряженных элементов. По определению каждый элемент группы G сопряжен с каким-то элементом из Z, и никакие два различных элемента Z не сопряжены друг с другом. В главе 5 мы опишем классы сопряженных элементов группы S_n, а одной из больших тем в 3-м семестре будет изучение классов сопряженных элементов в группе $\mathrm{GL}(n, K)$ обратимых матриц над полем и некоторых других "классических группах" — "каноническая форма линейного оператора", "спектральная теория операторов".

Задача. Докажите, что если C — класс сопряженных элементов группы G, то $C^{-1} = \{g^{-1} \mid g \in G\}$ тоже класс сопряженных элементов группы G.

2. Связь с централизаторами. Один из наиболее часто используемых фактов элементарной теории групп состоит в том, что число элементов в G, сопряженных с g, равно $|G : \mathrm{C}_G(g)|$. Точнее, имеет место следующий результат.

Предложение. *Сопоставление $C_G(g)x \mapsto g^x$ определяет биекцию между множеством $C_G(g)\backslash G$ левых смежных классов G по $C_G(g)$ и классом g^G.*

Доказательство. В самом деле, если два элемента x, y группы G лежат в одном и том же левом смежном классе G по $C_G(x)$, то найдется такое $u \in C_G(x)$, что $x = uy$. Тем самым, $g^x = g^{uy} = (g^u)^y = g^y$, так что это сопоставление действительно корректно определяет отображение $C_G(g)\backslash G \longrightarrow g^G$

Это отображение очевидно сюръективно, так как для каждого $x \in G$ его смежный класс $C_G(g)x$ переходит в g^x. С другой стороны, сопрягая равенство $g^x = g^y$, $x, y \in G$, при помощи y^{-1}, мы видим, что $g^{xy^{-1}} = g$ так что $xy^{-1} \in C_G(g)$, но это, как раз ровно и значит, что x и y лежат в одном левом смежном классе по $C_G(g)$.

Следствие. *Для любого $g \in G$ имеет место равенство*

$$|g^G| = |G : C_G(g)|.$$

В дальнейшем мы обобщим это утверждение на количество сопряженных с любым подмножеством $X \subseteq G$. А именно, количество сопряженных с X в G равно $|G : N_G(X)|$, просто для одноэлементного множества его нормализатор совпадает с централизатором.

3. Очевидные примеры описания сопряженных классов. Описание классов сопряженных элементов является одной из основных задач, которые мы должны решить, чтобы понять строение группы G. Вот несколько очевидных примеров.

• Класс элемента $x \in G$ в том и только том случае одноэлементный, когда x централен. В частности, группа G тогда и только тогда абелева, когда все ее сопряженные классы одноэлементны.

• В группе кватернионов Q два центральных класса $\{1\}$, $\{-1\}$, а три других сопряженных класса имеют вид $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$.

• Пусть D_n — диэдральная группа. В этом случае классы сопряженных элементов описываются по разному, в зависимости от четности n. Проще всего убедиться в этом представляя себе D_n как группу симметрий правильного n-угольника. Группа D_n содержит n вращений на углы $2\pi m/n$, $m = 0, \ldots, n-1$, и n отражений. Если n нечетно, то все отражения сопряжены в D_n: это отражения относительно прямых, соединяющих каждую из n вершин со серединой противоположной стороны. С другой стороны, если n четно, то отражения разбиваются на два класса: $n/2$ отражений относительно диагоналей n-угольника и $n/2$ отражений относительно прямых, соединяющих середины противоположных сторон. Вращения на углы $2\pi m/$ и $2\pi(n-m)/n$ и только они сопряжены. Таким образом, при нечетном n вращения разбиваются на $(n+1)/2$ сопряженных класса, а при четном n — на $n/2+1$ класса. А именно, в случае четного n кроме тождественного вращения еще и вращение на угол π центрально, и его сопряженный класс состоит из одного элемента.

4. Дальнейшие примеры. А вот несколько классических примеров, которые обсуждаются далее в нашем курсе.

• Как мы увидим в § 4 главы 5, классы сопряженных элементов в симметрической группе S_n описываются **цикленным типом**.

• Классы сопряженных элементов в $\mathrm{GL}(n, K)$ описываются в третьем семестре. В случае алгебраически замкнутого поля K эти классы описываются **жордановой формой**. В случае произвольного поля — **фробениусовой формой**.

• В том же третьем семестре описаны классы сопряженности в $U(n, \mathbb{R})$ и $O(n, \mathbb{R})$.

§ 5♡. Классы сопряженных элементов в конечных группах

В настоящем параграфе, если противное не оговорено явно, мы предполагаем, что группа G конечна.

1. Порядок класса сопряженных элементов. Класс x^G находится в естественном биективном соответствии с $G/C_G(x)$. В самом деле, $yC_G(x) \mapsto yxy^{-1}$ устанавливает такую биекцию.

Следствие. $|x^G| = |G : C_G(x)|$.

В частности, порядок класса C сопряженных элементов конечной группы G делит порядок этой группы.

Задача. Докажите, что порядок любого класса сопряженных элементов группы G не превосходит индекс ее центра.

Задача. Докажите, что порядок любого класса сопряженных элементов группы G не превосходит порядок ее коммутанта.

Задача. Докажите, что количество классов сопряженных элементов конечной группы G равно $\dfrac{1}{|G|}\sum |C_G(g))|$, $g \in G$.

Задача (fusion). Пусть G — конечная группа, а $H \leq G$ — ее подгруппа индекса 2. Как связаны между собой порядки классов x^G и x^H? Докажите, что для любого $h \in H$ либо $h^G = h^H$, либо h^G предствляется как объединение двух сопряженных классов в H.

Задача. Обобщается ли результат предыдущей задачи на подгруппу $H \leq G$ индекса p?

Повторяю для непонятливых: спрашивается, верно ли, что для любого $h \in G$ либо h^G продолжает оставаться одним сопряженным классом в H, либо представляется в виде объединения p различных сопряженных классов в H?

Задача. Предположим, что порядок $g \in G$ по крайней мере 3. Покажите, что если класс g^G содержит нечетное число элементов, то $g \not\sim g^{-1}$.

2. Группы с двумя классами сопряженных элементов. Во всякой нетривиальной группе по крайней мере два класса сопряженными элементов. Следующая задача показывает, что C_2 является *единственной* конечной группой, в которой *ровно* два класса.

Задача. Доказать, что если G — *конечная* группа, содержащая ≥ 3 элементов, то в ней ≥ 3 сопряженных классов.

Решение. Целое число $n \geq 3$ *редко* делится на $n-1$.

Предостережение. Стоит предупредить читателя, что существуют *бесконечные* группы, в которых ровно **два** класса сопряженных элементов, см. [**341**], Ch.V, § 6. Однако в таких группах порядок всех ненулевых элементов бесконечен.

Задача. Докажите, что если G бесконечная группа с двумя классами сопряженных элементов, то порядок любого $\neq 1$ элемента группы G бесконечен.

Решение. Предположим, что в G существует элемент $g \neq 1$ конечного порядка $o(g)$ и p — какой-то простой делитель $o(g)$. Тогда $o(g^{o(g)/p}) = p$. Так как все $\neq 1$ элементы группы G сопряжены, то все они имеют порядок p. Если $p = 2$, то группа G абелева — противоречие. Пусть поэтому $p > 2$. Тогда $g^2 \neq 1$ и, тем самым, $g^2 = xgx^{-1}$ для какого-то $x \neq 1$. Это значит, что для любого $m \in \mathbb{N}$ имеем $g^{2^m} = x^m g x^{-m}$ и, в частности, $g^{2^p} = g$. Но тогда $g^{2^p-1} = 1$ и $p|2^p - 1$. Однако это утверждение представляется довольно сомнительным, так как по теореме Ферма $p|2^{p-1} - 1$, так что, окончательно, $p|2^{p-1}$ — противоречие.

3. Теоремы Бернсайда. С использованием теории представлений Бернсайд доказал множество удивительных арифметических ограничений на количество сопряженных классов конечной группы и их порядки. Для небольших групп эти арифметические ограничения часто позволяют получить весьма детальную информацию о классах сопряженных элементов вообще без всяких вычислений. К сожалению, доказательства всех этих результатов, не опирающиеся на теорию представлений, настолько трудны, что их вообще невозможно изложить на начальном уровне. В главе 8 мы вернемся к некоторым из этих теорем Бернсайда в связи с критериями разрешимости конечных групп. Пока ограничимся формулировкой двух типичных результатов в таком духе.

Теорема Бернсайда. *Порядок $|C|$ класса сопряженных элементов неабелевой конечной простой группы не может быть примарным числом.*

По поводу следующего результата см. [171].

Теорема Бернсайда. *Пусть G — конечная группа нечетного порядка с s классами сопряженных элементов. Тогда $s \equiv |G| \pmod{16}$.*

§ 6♢. Klassengleichung, ♣ теорема Ландау

1. Классовое уравнение. Пусть теперь $Z = \{x_1, \dots, x_m\}$ — система представителей классов сопряженных элементов группы G, $C_i = x_i^G$ — класс с представителем x_i. Тогда

$$G = C_1 \sqcup \ldots \sqcup C_m.$$

Таким образом, если обозначить через $n_i = |C_i|$ порядок класса C_i, а через $n = |G|$ порядок группы G, то $n = n_1 + \ldots + n_m$. Число m называется **числом классов** (`Klassenzahl`, `class number`) группы G, а равенство

$$|G| = |C_1| + \ldots + |C_m| = |G : C_G(x_1)| + \ldots + |G : C_G(x_1)|$$

— **классовым уравнением** (`Klassengleichung`, `class equation`).

Набор $(n_1, \dots, n_m)$ порядков классов сопряженных элементов является важнейшим арифметическим инвариантом группы G. Если, кроме того, $l_i = |C_G(x_i)|$ — порядок централизатора элемента x_i, то $n = n_i l_i$, а классовое уравнение можно переписать в виде

$$1 = \frac{1}{l_1} + \ldots + \frac{1}{l_m}.$$

Обычно сопряженные классы располагают в порядке возрастания их порядков, так что $n_1 \leq \ldots \leq n_m$, и, тем самым, $l_1 \geq \ldots \geq l_m$. Кроме того, обычно полагают $x_1 = 1$, так что $n_1 = 1$, $l_1 = n$.

Задача. Пусть G — конечная группа. Выберем по одному элементу $g_1, \ldots, g_m$ из каждого класса $C_1, \ldots, C_m$ сопряженных элементов. Докажите, что тогда $G = \langle g_1, \ldots, g_m \rangle$.

2. Теорема Ландау. Сейчас мы взглянем на вопрос о количестве классов сопряженных элементов с другой стороны. Следующий результат, доказанный Эдмундом Ландау в 1903 году, иллюстрирует использование классового уравнения.

Эдмунд Ландау (Edmund Georg Hermann Landau, 14 февраля 1877, Берлин — 19 февраля 1938, ibid.) — замечательный немецкий математик. Ландау учился в Берлинском университете и в 1899 году защитил диссертацию под руководством Фробениуса. После этого он несколько лет преподавал там, а в 1909 году занял кафедру в Геттингене, которую до этого занимал Минковский. Однако в 1933 году **патриотически настроенные** немецкие студенты под предводительством Тейхмюллера организовали бойкот его лекций и с тех пор он преподавал только в Голландии, Англии и Палестине. Несмотря на это Ландау не хотел расставаться со своей собственностью в Германии и отказывался эмигрировать.

Подавляющее большинство из его 254 статей относится к различным аспектам теории чисел: распределение простых, гипотеза Римана, арифметические функции, проблема Варинга и другие аддитивные проблемы теории чисел, теория алгебраических чисел, геометрия чисел. Кроме того он опубликовал несколько статей по комбинаторике и анализу. Широко известны его многотомные классические сочинения *Handbuch der Lehre der Verteilung der Primzahlen*, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen*, *Vorlesungen über Zahlentheorie* и замечательные учебники анализа для начинающих: *Основы анализа*, *Введение в дифференциальное и интегральное исчисление*.

По материнской линии Ландау происходил из богатейшей банкирской семьи Якоби и в математическом фольклоре известны *сотни* шуток, отражающих его высокомерие и своеобразное чувство юмора. Например, когда ему представили Литтлвуда, он заметил: “Так значит Вы действительно существуете! А я думал, что это просто псевдоним, которым Харди подписывает свои неудачные работы”. На вопрос, как найти его дом, он имел обыкновение отвечать: “О, это очень просто, это самый красивый дом в Геттингене”. На предложения начинающих математиков рассказать основную идею работы он отвечал, что не знает, что такое **основная идея** и заставлял рассказывать полные доказательства со всеми леммами.

Теорема Ландау. *Существует лишь конечное число неизоморфных конечных групп с m классами сопряженных элементов.*

Доказательство. Достаточно показать, что для каждого m существует такое наибольшее n_0, что порядок n каждой конечной группы с m классами сопряженных элементов не превосходит n_0.

Если $m = 1$, то группа G состоит лишь из элемента 1 и, как было показано в пункте 1, если $m = 2$, то группа G состоит из двух элементов. Поэтому в дальнейшем мы можем считать, что $m \geq 3$.

Ясно, что

$$1 = \frac{1}{l_1} + \ldots + \frac{1}{l_m} \leq \frac{m}{l_m}$$

или, иными словами, $l_m \leq m$. Аналогично,

$$1 - \frac{1}{l_m} = \frac{1}{l_1} + \ldots + \frac{1}{l_m} \leq \frac{m-1}{l_{m-1}}.$$

Так как $l_m \geq 2$, это неравенство можно переписать в виде $l_{m-1} \leq 2(m-1)$. Ясно, что продолжая этот процесс, мы получим оценку для $l_1 = n$ в терминах m. В самом деле, предположим, что для некоторого $k < m-1$ мы уже получили оценки $l_{m-k} \leq h_m, \ldots, l_k \leq h_k$. Тогда существует лишь конечное число возможных наборов $l_k, \ldots, l_m$, так что в множестве всех выражений вида $1 - \frac{1}{l_{m-k}} - \ldots - \frac{1}{l_m} > 0$ существует наименьшее, и, значит, найдется $q \in \mathbb{N}$ такое, что $\frac{1}{q} \leq \frac{m-k-1}{l_{m-k-1}}$ или, что то же самое, $l_{m-k-1} \leq q(m-k-1)$. Таким образом, доказательство теоремы завершается по индукции.

Сделаем для иллюстрации еще один шаг явно:

$$1 - \frac{1}{l_{m-1}} - \frac{1}{l_m} = \frac{1}{l_1} + \ldots + \frac{1}{l_{m-2}} \leq \frac{m-2}{l_{m-2}}.$$

Так как $m \geq 3$, то $l_{m-1} \geq 3$ (в самом деле, если $l_m = 2$, это так потому, что $1 - \frac{1}{l_m} - \frac{1}{l_{m-1}} > 0$, а если $l_m \geq 3$, то просто потому, что $l_{m-1} \geq l_m$). Это значит, что левая часть последнего равенства $\geq \frac{1}{6}$ и, значит, его можно переписать в виде $l_{m-2} \leq 6(m-2)$. Полагая в последнем неравенстве $m = 3$, мы видим, что $n = l_1 \leq 6$, так что порядок группы с тремя классами сопряженных элементов не превосходит 6. Эта оценка является точной, так как существует группа порядка 6, а именно, $S_3 \cong D_3$, у которой ровно 3 класса сопряженных элементов.

Задача. Докажите, что порядок группы с 4 классами сопряженных элементов не превосходит 24. Существует ли группа порядка 24 с 4 классами сопряженных элементов?

§ 7♠. Алгебра классов

1. Сопряженность и коммутирование. Ясно, что два класса сопряженных элементов C и D, вообще говоря, не обязаны коммутировать поэлементно, тем не менее, они всегда коммутируют как множества.

Упражнение. Доказать, что $CD = DC$.

Решение. Ясно, что $xy = (xyx^{-1})x$.

В действительности, из этой формулы можно сделать более глубокомысленный вывод: $xC = Cx$ для любого $x \in G$ и любого класса сопряженных элементов C. Полностью оценить это наблюдение

читатель сможет когда мы определим групповую алгебру — классы сопряженных элементов порождают центр групповой алгебры!

2. Алгебра классов. Начнем со следующего незамысловатого наблюдения.

Задача. Докажите, что произведение CD двух классов сопряженных элементов $C, D \subseteq G$ является объединением классов сопряженных элементов.

В действительности для *конечной* группы G произведение CD естественно представлять себе как *мультимножество*, т. е. считать, что $g \in G$ входит в CD столько раз, сколькими различными способами его можно представить в виде $g = xy$, $x \in C$, $y \in D$. Иными словами, кратность вхождения g в CD определяется следующей формулой

$$m_{CD}(g) = |\{(x, y) \mid x \in C,\ y \in D,\ xy = g\}|.$$

Задача. Покажите, что если $h \sim g$, то $m_{CD}(h) = m_{CD}(g)$.

Пусть E еще один класс сопряженных элементов. Обозначим общее значение всех $m_{CD}(g)$ через $m_{CD}(E)$. Тогда

$$CD = \sum m_{CD}(E)E,$$

где сумма берется по всем сопряженным классам E группы G. Ясно, что для любых трех классов C, D, E имеем $m_{CD}(E) = m_{DC}(E)$. В книге III мы убедимся, что получающаяся при этом алгебра изоморфна центру групповой алгебры $\mathbb{Z}[G]$, а в книге IIB мы увидим, что эта алгебра играет колоссальную роль в разложении регулярного представления группы G на неприводимые. Ограничимся пока несколькими простейшими примерами.

3. Примеры. Совсем просто описать алгебру классов для небольших групп перестановок. Во всех случаях мы полагаем $C_1 = \{1\}$. Ясно, что $C_1 C_i = C_i$.

• В группе S_3 три класса C_1 и

$C_2 = \{(12), (13), (23)\}$,

$C_3 = \{(123), (132)\}$.

Убедитесь, что $C_2^2 = 3C_1 + 3C_3$, $C_2C_3 = 2C_2$, $C_3^2 = 2C_1 + C_3$.

• В группе S_3 четыре класса C_1 и

$C_2 = \{(12)(34), (13)(24), (14)(23)\}$,

$C_3 = \{(123), (142), (134), (243)\}$,

$C_4 = \{(132), (124), (143), (234)\}$.

Убедитесь, что

$C_2^2 = 3C_1 + 2C_2$, $C_2C_3 = 3C_3$, $C_2C_4 = 3C_4$, $C_3^2 = 4C_4$, $C_3C_4 = 4C_1 + 4C_2$, $C_4^2 = 4C_3$.

• В группе S_4 пять классов C_1 и

$C_2 = \{(12), (13), (14), (23), (24), (34)\}$,

$C_3 = \{(123), (142), (134), (243), (132), (124), (143), (234)\}$,

$C_4 = \{(12)(34), (13)(24), (14)(23)\}$,

$C_5 = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$.

Убедитесь, что

$C_2^2 = 6C_1 + 2C_3 + 3C_4$, $C_2C_3 = 4C_2 + 4\mathrm{C}_5$, $C_2C_4 = \mathrm{C}_2 + 2C_4$, $C_2C_5 = 3C_3 + 4\mathrm{C}_4$, $C_3^2 = 8\mathrm{C}_1 + 4C_3 + 8\mathrm{C}_4$, $C_3C_4 = C_3$, $C_3C_5^2 = 4C_2 + 4\mathrm{C}_5$, $C_4^2 = 3\mathrm{C}_1 + 2\mathrm{C}_4$, $C_4C_5 = 2C_2 + C_5$, $C_5^2 = 6C_1 + 3C_3 + 2C_4$.

Задача. Вычислите таблицу умножения в алгебре классов диэдральной группы D_n.

§ 8♢. Нормальные подгруппы и сопряженность

> "Да, *сопрягать надо, сопрягать надо!*" — с внутренним восторгом повторил себе Пьер, чувствуя, что этими именно, и только этими словами выражается то, что он хочет выразить, и разрешается весь мучащий его вопрос.
> — Да, сопрягать надо, пора сопрягать.
>
> Лев Толстой. *Война и Мір*, т.III, ч. III, IX.

Теперь у нас все готово для того, чтобы описать нормальные подгруппы в терминах сопряженных, а не смежных классов.

1. Сопряженность подмножеств. Как мы уже заметили в начале предыдущего пункта, условие $H \trianglelefteq G$ можно переформулировать следующим образом: для любого $x \in G$ имеет место равенство $xHx^{-1} = H$. Рассмотрим эту характеризацию нормальных подгрупп чуть подробнее.

Пусть вначале $A, B \subseteq G$ — два подмножества в G. Они называются **сопряженными в** G, если найдется такое $x \in G$, что $B = xAx^{-1} = \{xax^{-1} \mid a \in A\}$. Так как отображение $g \mapsto xgx^{-1}$ является автоморфизмом G (см. главу 4), то подмножество, сопряженное к подгруппе, само является подгруппой. В самом деле, если $H \leq G$ и $xhx^{-1}, xgx^{-1} \in xHx^{-1}$, то $(xhx^{-1})(xgx^{-1}) = x(hg)x^{-1} \in xHx^{-1}$ и $(xhx^{-1})^{-1} = xh^{-1}x^{-1} \in xHx^{-1}$.

Упражнение. Убедитесь, что $(AB)^g = A^g B^g$, $(A \cap B)^g = A^g \cap B^g$. Обобщите.

2. Связь с нормализаторами. В § 4 нам уже встречалось утверждение о количестве элементов, сопряженных с данным. Сейчас мы обобщим это утверждение на произвольные подмножества.

Предложение. *Сопоставление $X_G(A)x \mapsto X^x$ определяет биекцию между множеством $C_G(A)\backslash G$ левых смежных классов G по $N_G(A)$ и множеством $\{A^x, x \in G\}$ всех сопряженных с A.*

Доказательство. Слово в слово повторяет доказательство соответствующего результата из § 4. В самом деле, если два элемента x, y группы G лежат в одном и том же левом смежном классе G по $N_G(A)$, то найдется такое $u \in N_G(A)$, что $x = uy$. Тем самым, $A^x = A^{uy} = (A^u)^y = g^y$, так что это сопоставление действительно корректно определяет отображение $N_G(A)\backslash G \longrightarrow g^G$

Это отображение очевидно сюръективно, так как для каждого $x \in G$ его смежный класс $N_G(A)x$ переходит в A^x. С другой стороны, сопрягая равенство $A^x = A^y$, $x, y \in G$, при помощи y^{-1}, мы видим, что $A^{xy^{-1}} = A$ так что $xy^{-1} \in N_G(A)$, но это, как раз ровно и значит, что x и y лежат в одном левом смежном классе по $N_G(A)$.

Следствие. *Для любого $g \in G$ имеет место равенство*

$$|\{A^x, x \in G\}| = |N : C_G(A)|.$$

3. Произведения сопряженных подгрупп. Следующий цикл задач иллюстрирует роль сопряженности для подгрупп.

Задача. Пусть $H \leq G$ — подгруппа *конечной* группы G. Докажите, что объединение всех подгрупп в G, сопряженных с H, не может равняться G.

Иными словами, утверждается, что в G найдется элемент, который не сопряжен ни с одним элементом из H!

Предостережение. Как уже упоминалось, можно построить *бесконечную* группу G, все неединичные элементы которой сопряжены. Такая группа G является объединением нетривиальных циклических подгрупп, которые все в ней сопряжены.

Задача. Пусть $F, H \leq G$, $FH = G$, то для любого $g \in G$ найдется такое $h \in H$, что $F^g = F^h$.

Решение. В самом деле, $g = fh$ для подходящих $f \in F$, $H \in H$. Но тогда $F^g = F^{fh} = (F^f)^h = F^h$.

Задача. Пусть $F, H \leq G$, $FH = G$. Докажите, что для любого $g \in G$ имеем $F^g H = G$.

Решение. Как мы только что видели, $F^g = F^h$ для некоторого $h \in H$. Поэтому

$$F^g H = F^h H^h = (FH)^h = G^h = G.$$

Задача. Если $F, H < G$, $FH = G$, то F и H не могут быть сопряжены в G.

Решение. Если $F^g = H$, то $G = F^g H = HH = H$.

Следствие. *Если $H < G$, а $g \in G$, то $H^g H \subset G$.*

Например, отсюда сразу следует, что группа G порядка p^2 абелева. В самом деле, если в G есть нецентральная подгруппа H порядка p, то $H^g H = G$, что невозможно.

Результаты предыдущих задач можно итерировать, рассматривая сопряженные к обеим подгруппам.

Задача. Докажите, что если $G = FH$, а $x, y \in G$, то $G = F^x H^y$.

Задача. Докажите, что если $G = FH$, то для любых $x, y \in G$, найдется такое $g \in G$, что $F^x = F^g$, $H^y = H^g$.

4. Сопряженность и нормальные подгруппы. Итак, мы можем слегка переформулировать определение нормальной подгруппы.

Определение. *Подгруппа H группы G называется* **нормальной**, *если она совпадает со всеми своими сопряженными, т. е. если для любого $x \in G$ имеет место равенство $xHx^{-1} = H$.*

Это значит, что нормальная подгруппа — это такая подгруппа, которая вместе с каждым элементом g целиком содержит его класс сопряженных элементов g^G. Это можно выразив чуть короче, написав $H^G = H$. Например, теперь мы сразу понимаем, почему подгруппа H из примера, рассмотренного в § 2, не является нормальной: при $n \geq 3$ подгруппа H содержит транспозицию, и значит, чтобы быть нормальной, она должна содержать *все* транспозиции, т. е. совпадать с S_n по теореме § 6 главы 5.

Это определение, хотя и тривиальным образом эквивалентное предыдущему, дает больший простор для обобщений. Например, для *индивидуального* элемента $x \in G$ включение $xHx^{-1} \leq H$ не обязательно влечет равенство $xHx^{-1} = H$. Разумеется, для *конечной* подгруппы H равенство следует из совпадения порядков, $|xHx^{-1}| = |H|$. Тем не менее, если включение $xHx^{-1} \leq H$ имеет место *для всех* элементов группы G, то $H \trianglelefteq G$. В самом деле, $H = x(x^{-1}Hx)x^{-1} \leq xHx^{-1} \leq H$.

Предостережение 1. В общем случае из того, что $H^x \leq H$, не следует, что $x \in N_G(X)$.

Предостережение 2. В общем случае множество $x \in G$ таких, что $H^x \leq H$, не образует подгруппы в G.

Оба высказанных утверждения опровергаются тем же контрпримером, который уже дважды встречался нам в предыдущей главе в связи с пересечениями левых и правых смежных классов.

$$G = \begin{pmatrix} \mathbb{Q}^* & \mathbb{Q} \\ 0 & 1 \end{pmatrix}, \qquad H = \begin{pmatrix} 1 & \mathbb{Z} \\ 0 & 1 \end{pmatrix}, \qquad g = \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}.$$

Тогда

$$gHg^{-1} = \begin{pmatrix} 1 & n\mathbb{Z} \\ 0 & 1 \end{pmatrix} < H, \qquad g^{-1}Hg = \begin{pmatrix} 1 & \mathbb{Z}/n \\ 0 & 1 \end{pmatrix}.$$

Для того, чтобы $g \in N_G(H)$ необходимо и достаточно, чтобы

$$gHg^{-1}, g^{-1}Hg \leq H,$$

а как раз второе из этих утверждений в этом случае не имеет места. Таким образом, множество $\{g \in G \mid gHg^{-1} \leq H\}$ является подмоноидом в G, но, вообще говоря, не подгруппой.

5. Пересечения нормальных подгрупп. Отметим еще два результата, сразу вытекающие из нашего нового определения.

• Если $H_i \trianglelefteq G$, $i \in \Omega$, то $H = \bigcap\limits_{i\in\Omega} H_i \trianglelefteq G$. В самом деле, если $x \in H$, то $x \in H_i$ для всех i и, значит, по условию, $x^G \subseteq H_i$. Но тогда $x^G \subseteq H$. В частности, пересечение всех неединичных нормальных подгрупп группы G является нормальной подгруппой в G, называемой **монолитом** группы G. Группа G называется **монолитической**, если ее монолит $\neq 1$ (в главе 8 мы назовем такие группы подпрямо неразложимыми).

• Если $H \leq G$, то $H_G = \bigcap\limits_{x\in G} xHx^{-1} \trianglelefteq G$. Ясно, что H_G — наибольший нормальный делитель в G, содержащийся в H. Подгруппа H_G называется **нормальной внутренностью** (`normal interior`), или **сердцевиной** (`core`) подгруппы H в группе G.

Задача. Докажите, что если $H \trianglelefteq G$, то $C_G(H) \trianglelefteq G$.

Решение. Конечно, проще всего заметить, что $C_G(H) = \{x \in G \mid [x, H] = 1\}$ и применить к этому равенству внутренний автоморфизм

I_g. Однако это рассуждение легко провести и непосредственно. Пусть, например, $g \in G$, $x \in C_G(H)$. Тогда для любого $x \in H$ имеем

$$({}^g x)h = gx(h^g)g^{-1} = g(h^g)xg^{-1} = h({}^g x).$$

6. Коммутаторы и коммутант. Сейчас мы построим *важнейший* пример нормальной подгруппы, к изучению которого вернемся во втором семестре.

Определение. Коммутатором *двух элементов* $x, y \in G$ *называется элемент*

$$[x, y] = xyx^{-1}y^{-1}.$$

Подгруппа в G*, порожденная всеми коммутаторами, называется* **коммутантом** G *и обозначается* $[G, G]$*:*

$$[G, G] = \langle [x, y], x, y \in G \rangle.$$

В большинстве старых книг коммутант обычно назывался **производной группой** (`derived group`) и обозначался G'. Еще и сегодня **ряд коммутантов**

$$G \geq G' \geq G'' \geq \dots$$

часто называется **производным рядом** (`derived series`).

Ясно, что $[x, y]^{-1} = yxy^{-1}x^{-1} = [y, x]$, так что элемент, обратный к коммутатору, сам является коммутатором. Обычная ошибка начинающих состоит в том, что они считают, что коммутант есть *множество* коммутаторов. Это не так, и в главе 8 мы приведем совсем простой пример группы, в которой *не каждый* элемент коммутанта есть коммутатор. Сейчас мы увидим, что коммутант автоматически является нормальной подгруппой.

Предложение. *Для любой группы* $[G, G] \trianglelefteq G$.

Доказательство. В самом деле, легко видеть, что

$$g[x, y]g^{-1} = [gxg^{-1}, gyg^{-1}],$$

это вытекает из того, что $I_g : x \mapsto gxg^{-1}$ является гомоморфизмом. Тем самым, элемент, сопряженный с коммутатором, сам является коммутатором и, значит, коммутант порождается классами сопряженных элементов.

§ 9♢. Порождение нормальных подгрупп

Слова Россия — родина слонов изобрел в XVIII веке испанский путешественник, рекламировавший таким способом увиденные им в кунсткамере Петербурга *остатки* мамонтов.

Владимир Игоревич Арнольд. *Что такое математика?*

1. Нормальная подгруппа, порожденная подмножеством. Постараемся видоизменить конструкцию из § 4 главы 2, заменив там подгруппы на нормальные подгруппы. Пусть $X \subseteq G$. Существует ли наименьшая *нормальная* подгруппа в G, содержащая X, и как ее описать?

Определение. *Пусть $X \subseteq G$. Наименьшая нормальная подгруппа в G, содержащая X называется* **нормальной подгруппой, порожденной** *X и обозначается $\langle X\rangle^G$.*

Заметим, что некоторые авторы обозначают нормальную подгруппу, порожденную X через $\langle\langle X\rangle\rangle$, однако это обозначение подразумевает, что группа G фиксирована. Наше обозначение представляется мне более удобным, так как, во-первых, оно является комбинацией двух общепринятых обозначений $\langle X\rangle$ и H^G и, во-вторых, в нем явно указана группа G. Точно так же, как и в § 4 главы 2 существование такой подгруппы гарантируется тем, что пересечение *любого* множества нормальных подгрупп снова является нормальной подгруппой. Как и в § 4 главы 2 эта подгруппа допускает вполне конкретное описание, проверку которого (полностью аналогичную доказательству теоремы цитированного параграфа) мы оставляем читателю. В следующей теореме X^G имеет обычный смысл: $X^G = \{gxg^{-1} \mid x \in X, g \in G\}$.

Теорема. *Для любого подмножества $X \subseteq G$*

$$\langle X\rangle^G = \langle X^G\rangle = \{y_1x_1y_1^{-1}\dots y_nx_ny_n^{-1} \mid x_i \in X \cup X^{-1}, y_i \in G, n \in \mathbb{N}_0\}.$$

Мораль этого описания состоит в следующем: нормальные подгруппы — это *в точности* подгруппы, порожденные классами сопряженных элементов. В частности, если X состоит из классов сопряженных элементов, то есть $X^G = X$, то $\langle X\rangle^G = \langle X\rangle$, иными словами, подгруппа, порожденная X, *автоматически* является нормальной. В следующем пункте мы приведем ключевой пример, иллюстрирующий это явление.

Задача. Пусть $x \in G$. Покажите, что x в том и только том случае принадлежит абелевой нормальной подгруппе, когда он коммутирует со всеми своими сопряженными.

2. Лемма Дицмана. Доказательство следующей леммы [172] блестяще иллюстрирует мысль Льва Толстого о том, что **надо сопрягать**.

Лемма Дицмана. *Пусть $X \subseteq G$ конечное подмножество группы G, состоящее из элементов конечного порядка и такое, что $x^y \in X$ для двух любых $x, y \in X$. Тогда группа $\langle X\rangle$ конечна.*

Доказательство. Пусть $|X| = n$, а m — наименьшее общее кратное порядков $o(x)$ элементов $x \in X$. Мы докажем, что $|\langle X\rangle| \leq n^{n(m-1)}$. Для этого заметим, что так как порядки всех элементов множества X конечны, каждый элемент $g \in \langle X\rangle$ можно записать как произведение $g = x_1 \dots x_l$, где $x_i \in X$. Мы покажем, что для любого элемента g существует такое представление, в котором $l \leq n(m-1)$. В самом деле, рассмотрим более длинное слово $g = x_1 \dots x_l$. Так как $l > n(m-1)$, то какой-то элемент $x \in X$ входит в это представление по крайней мере m раз. Пусть x_i — первое вхождение x в g. Переписывая g в виде

$$g = x_1 \dots x_l = x x_1^x \dots x_{i-1}^x x_{i+1} \dots x_l$$

мы получаем новое выражение g в виде слова длины l, где все множители снова принадлежат X (так как $X^X \subseteq X$), но теперь x стоит на первом месте. Поступая точно так же со следующим вхождением x, мы перепишем g как слово длины l, в котором *два* первых множителя равны x. Продолжая действовать таким образом, мы перепишем g в виде $x^m y_1 \dots y_{l-m}$, где $y_i \in X$. Так как $x^m = 1$, это значит, что нам удалось записать $g = y_1 \dots y_{l-m}$ как слово длины $l - m$.

Следствие. *Конечное объединение конечных сопряженных классов элементов конечного порядка содержится в конечной нормальной подгруппе.*

§ 10♡. Субнормальные подгруппы, ♣ теорема Виландта

Верно ли, что отношение нормальности транзитивно? Иными словами, верно ли, что нормальная подгруппа нормальной подгруппы сама нормальна? Легко видеть, что это не так. Пусть, например $G = A_4$ — знакопеременная группа степени 4, $H = V$ — четверная группа, а F — любая подгруппа порядка 2 в V, скажем, $F = \langle (12)(34)\rangle$. Мы уже знаем, что $V \trianglelefteq A_4$, а так как V абелева, то и $F \trianglelefteq V$. В то же время очевидно, что F не может быть нормальным делителем в A_4, в самом деле, например, $[(12)(34), (123)] = (13)(24)$. Таким образом, $F \trianglelefteq H \trianglelefteq G$, но $F \not\trianglelefteq G$.

1. Субнормальные подгруппы. Вышесказанное оправдывает введение следующего класса подгрупп [173].

Определение. *Говорят, что подгруппа $F \trianglelefteq G$* **субнормальна** *в G и пишут $F \trianglelefteq\trianglelefteq G$, если существует ряд подгрупп*

$$F = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \dots \trianglelefteq G_d = G$$

в котором каждая подгруппа нормальна в следующей. Наименьшее такое d называется **глубиной** *субнормальной подгруппы.*

Таким образом,

• субнормальная подгруппа глубины 1 — это в точности нормальная подгруппа;

• субнормальная подгруппа глубины 2 — это подгруппа, для которой существует H, $F \trianglelefteq H \trianglelefteq G$;

и т. д. Ясно, что отношение субнормальности уже транзитивно: если $F \trianglelefteq\trianglelefteq H \trianglelefteq\trianglelefteq G$, то $F \trianglelefteq\trianglelefteq G$.

Упражнение. Убедитесь, что если $H \trianglelefteq\trianglelefteq G$ и $F \leq G$, то $H \cap F \trianglelefteq\trianglelefteq F$.

Упражнение. Убедитесь, что если $H \trianglelefteq\trianglelefteq G$ и $H \leq F \leq G$, то $H \trianglelefteq\trianglelefteq F$.

В частности, если $H \trianglelefteq\trianglelefteq G$ и $H \leq F \leq G$, то $H \trianglelefteq\trianglelefteq F$. Естественно спросить, верно ли, что если $F \trianglelefteq\trianglelefteq G$ и $H \trianglelefteq\trianglelefteq G$, то $F \cap H \trianglelefteq\trianglelefteq G$ и $\langle F, H\rangle \trianglelefteq\trianglelefteq G$? Для пересечения это действительно всегда так, для порождения ситуация значительно сложнее.

Задача (Виландт) Докажите, что пересечение двух субнормальных подгрупп $F, H \trianglelefteq\trianglelefteq G$ является субнормальной подгруппой. При этом глубина подгруппы $F \cap H$ не превосходит сумму глубины F и глубины H.

Решение. Пусть глубина F равна r,

$$F = F_0 \trianglelefteq F_1 \trianglelefteq F_2 \trianglelefteq \ldots \trianglelefteq F_r = G,$$

а глубина H равна s,

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_s = G.$$

Тогда

$$F \cap H = F \cap H_0 \trianglelefteq F \cap H_1 \trianglelefteq F \cap H_2 \trianglelefteq \ldots \trianglelefteq F \cap H_r = F$$

показывает, что $F \cap H$ является субнормальной подгруппой в F, глубина которой не превосходит s.

2. Теорема Виландта. В следующем доказательстве конечность группы G используется самым существенным образом.

Теорема Виландта. *Пусть G конечная группа, $F, H \trianglelefteq\trianglelefteq G$. Тогда $\langle F, H\rangle \trianglelefteq\trianglelefteq G$.*

Доказательство. Проведем совместную индукцию по *паре* индексов $|G : F|$ и $|G : H|$, считая, что для всех меньших в лексикографическом порядке пар теорема уже доказана. Зафиксируем какой-то субнормальный ряд

$$F \triangleleft G_n \triangleleft G_{n-1} \triangleleft \ldots \triangleleft G_1 \triangleleft G_0 = G.$$

Предположим, вопреки ожиданиям, что $\langle F, H\rangle$ не является субнормальной в G и в этом предположении докажем, прежде всего, что $\langle G_n, H\rangle = G$. В самом деле, так как $G_n \trianglelefteq\trianglelefteq G$ и $G_n \neq H$, то по индукционному предположению $\langle G_n, H\rangle \trianglelefteq\trianglelefteq G$. Так как $F, H \trianglelefteq \langle G_n, H\rangle$, то если $\langle G_n, H\rangle \neq G$, то, снова по индукционному предположению, $\langle F, H\rangle \trianglelefteq\trianglelefteq \langle G_n, H\rangle$. Но тогда в силу транзитивности субнормальности $\langle F, H\rangle \trianglelefteq\trianglelefteq G$, противоречие.

Докажем теперь, что H нормализует F. В самом деле, предположим, что $F^h \neq F$ для некоторого $h \in H$. Так как $F \leq G_1 \triangleleft G$, то $F^h \leq G_1$ — и даже $F^h \trianglelefteq\trianglelefteq G_1$. Так как $G_1 \neq G$, то мы можем применить индукционное предположение и заключить, что $\langle F, F^h\rangle \trianglelefteq\trianglelefteq G_1$. Но тогда так как $\langle F, F^h\rangle > F$, то по индукционному предположению

$$\langle F, H\rangle = \langle F, F^h, H\rangle = \langle\langle F, F^h\rangle, H\rangle \trianglelefteq\trianglelefteq G,$$

противоречие. Таким образом, $F^h = F$ для всез $h \in H$.

Сопоставляя два только что доказанных утверждения, мы видим, что $G = \langle G_n, H\rangle \leq N_G(F)$, так что $F \trianglelefteq G$. В силу симметрии мы точно так же докажем, что $H \trianglelefteq G$. Но тогда, конечно, $\langle F, H\rangle \trianglelefteq G$, противоречие.

В этом рассуждении, взятом из **[342]**, мы самым существенным образом использовали то, что F и H — подгруппы *конечного индекса*. Кстати, почему мы не могли здесь проводить индукцию по *глубине* подгрупп F и H? Ведь если считать, что F и H соединены с G композиционными рядами (каждая подгруппа G_i не просто нормальна в предыдущей, но и *максимальна* в ней), то индекс можно с успехом заменить на длину такого ряда.

Дело в том, что в бесконечной группе утверждение теоремы, вообще говоря, неверно. Первый такой пример был приведен Цассенхаузом, а более простой пример — Дереком Робинсоном [174].

§ 11◇. Фактор-группы

Теперь мы в состоянии определить, когда на множестве G/H смежных классов G по H можно естественным образом ввести структуру группы.

1. Умножение смежных классов по нормальной подгруппе. Для нормальной подгруппы $H \trianglelefteq G$ отношения сравнимости слева и справа совпадают, тем самым вместо левых и правых смежных классов можно говорить просто о смежных классах G по H.

Лемма. *Отношение сравнимости $\equiv$ alias $\equiv_H$ по нормальной подгруппе H является конгруэнцией в G. Иными словами,*

- *если $x \equiv y$ и $u \equiv v$, то $xu \equiv yv$;*
- *если $x \equiv y$, то $x^{-1} \equiv y^{-1}$.*

Доказательство. По условию, $xH = yH$ и $uH = vH$. Нам нужно показать, что $xuH = yvH$. В самом деле,

$$xuH = (xu)(HH) = x(uH)H = x(Hu)H = (xH)(uH) = \\ = (yH)(vH) = y(Hv)H = y(vH)H = (yv)(HH) = yvH.$$

Кроме ассоциативности и определения подгруппы мы здесь воспользовались тем, что $uH = Hu$ и $Hv = vH$, т. е. тем, что H нормальна. Второе утверждение леммы вытекает из первого (и поэтому обычно не включается в определение конгруэнции). Перемножая сравнения $x^{-1} \equiv x^{-1}$, $x \equiv y$, $y^{-1} \equiv y^{-1}$, по только что доказанному получаем $y^{-1} = x^{-1}xy^{-1} \equiv x^{-1}yy^{-1} = x^{-1}$.

Утверждение леммы можно сформулировать и чуть иначе. А именно, мы доказали два следующих утверждения. Если $H \trianglelefteq G$, то:

- результат произведения по Минковскому двух смежных классов снова является смежным классом,
- обратный по Минковскому к смежному классу является смежным классом.

Первое из этих утверждений неверно, если H не является нормальной подгруппой. Что касается второго, то, как мы уже знаем, $(xH)^{-1} = Hx^{-1}$, но для нормальной подгруппы $Hx^{-1} = x^{-1}H$.

2. Фактор-группа. Как мы только что показали, если $H \trianglelefteq G$, то на множестве смежных классов G/H можно корректно определить умножение. Впервые эту конструкцию начали систематически рассматривать Жордан и Гельдер, причем сам термин `Faktorgruppe` впервые использовал Отто Гельдер в 1889 году.

Определение. *Пусть $H \trianglelefteq G$. Тогда множество смежных классов G по H с умножением $xH \cdot yH = xyH$ называется* **фактор-группой** *G по H и обозначается G/H.*

Используемое здесь написание находится на полпути между английским `factor group` и немецким `Faktorgruppe` (изредка употребляются также термины `Restklassengruppe` и, иногда, `Quotientengruppe`).

Камиль Жордан (Marie Ennemond Camille Jordan, 5 января 1838, Лион — 20 января 1922, Милан) — один из величайших математиков XIX века, внесший фундаментальный вклад в развитие алгебры, анализа, топологии, теории дифференциальных уравнений, арифметической теории квадратичных форм. После учебы в Париже Жордан некоторое время работал горным инженером, но позже полностью сосредоточился на математике и в 1876 году стал профессором Ecole Polytechnique. Вероятно, самые глубокие результаты Жордана относятся к теории групп и многомерной геометрии. Опубликованная в 1870 году совершенно изумительная по глубине и насыщенности конкретными результатами книга Жордана *Traité des substitutions et des équations algébriques* стала одним из поворотных пунктов в истории нашей науки. От этой книги берут начало современная теория групп перестановок, теория линейных групп и теория абстрактных групп. Среди прочего эта книга сыграла громадную роль в пропаганде теории Галуа. В нашем курсе упоминаются несколько теорем Жордана, относящихся к теории групп, теорема Жордана—Гельдера и т. д. Кроме того, Жордан написал замечательный классический *Cours d'analyse*. В учебниках анализа и топологии встречаются мера Жордана, разложение Жордана функции ограниченной вариации, кривая Жордана, теорема Жордана о кривой, лемма Жордана в теории функций комплексного переменного, признак Жордана сходимости рядов Фурье, и т. д. В подтверждение принципа Арнольда стоит упомянуть, что изучаемые в курсе линейной алгебры жорданова форма, жордановы клетки, жорданова матрица, жорданов базис, мультипликативное разложение Жордана, аддитивное разложение Жордана и т. д. были открыты Вейерштрассом. У Жордана было восемь детей: две дочери и шесть сыновей, трое из которых погибли в 1914–1916 годах.

Следует предупредить, что не все понятия, в названии которых по-английски фигурирует Jordan, связаны с именем **Жордана**. В действительности, многие из них (такие как Jordan Algebras — **йордановы алгебры**) связаны либо с **Паскуалем Йорданом**, либо с **Вильгельмом Йорданом**.

Обратите внимание, что в большинстве старых учебников используется *бескомпромиссное* немецкое написание **факторгруппа**, но тогда было бы логично писать **факторалгебра**, **факторпространство**, **фактормногообразие**, etc.

По только что доказанной лемме умножение, которое мы определили на G/H, действительно **корректно**. Иными словами, результат *не зависит* от выбора представителей $u \in xH$ и $v \in yH$. Корректность вытекает также из того, что определенное выше умножение классов совпадает с умножением по Минковскому:

$$(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH = xH \cdot yH.$$

Убедимся в том, что оно действительно определяет на G/H структуру группы.

Теорема. *Пусть $H \trianglelefteq G$. Тогда множество G/H относительно операции умножения классов образует группу.*

Отто Людвиг Гельдер (Otto Ludwig Hölder, 22 декабря 1859, Штуттгарт — 29 августа 1937, Лейпциг), называемый в дальнейшем **Гельдер ст.**, — замечательный немецкий математик, один из классиков алгебры XIX века, основные работы которого относятся к теории групп, теории чисел, теории функций и гармоническому анализу. Гельдер учился в Штуттгарте и Берлине, где его учителями были Кронекер, Вейерштрасс и Куммер. После защиты диссертации по теории аналитических функций в Тюбингене в 1882 году, под руководством дю Буа-Раймона, он провел несколько лет в Лейпциге и Геттингене. Именно в это время он доказал свое знаменитое неравенство и под влиянием Клейна и фон Дика заинтересовался теорией групп. В 1889 году он получает постоянную позицию в Тюбингене. Именно в это время его работа по теории Галуа привела его к изучению композиционных рядов в группах. Понятие фактор-группы впервые явно появляется в его статье 1889 года, за этой статьей следует целый ряд принципиально важных работ, где он изучает автоморфизмы групп, группы небольших порядков, доказывает многие важные факты о конечных группах. С 1899 года он становится профессором в Лейпциге, но в это время его интересы смещаются в сторону геометрии и философии. В нашем курсе встречается десяток теорем Гельдера — описание автоморфизмов S_n, классификация групп порядков p^3, p^2q, pqr, p^4, разрешимость групп бесквадратных порядков и т. д., теорема Жордана—Гельдера, неравенство Гельдера и т. д.

Крупные специалисты по истории математики обычно путают Гельдера ст. с его сыном **Эрнстом Отто Гельдером** (Ernst Otto Hoelder, 2 апреля 1901, Лейпциг —), тоже выдающимся математиком. Однако Гельдер мл. не продолжал алгебраические исследования своего отца, а воспринял чисто аналитическое направление своего учителя Леона Лихтенштейна, который тоже в то время был профессором в Лейпциге. Основные работы Гельдера мл. относятся к области математической физики, вариационного исчисления и интегральных уравнений. Но знаменитое неравенство Гельдера все же доказал в 1889 году Гельдер ст.!

Доказательство. Так как умножение классов определяется в терминах умножения представителей, то ассоциативность вытекает из ассоциативности умножения в G. Нейтральным элементом в G/H является $H = e_{G/H}$. Наконец, классом, обратным к классу xH, является $x^{-1}H$.

По самому определению умножения классов отображение $\pi : G \longrightarrow G/H$, $x \mapsto xH$, сопоставляющее каждому элементу его класс, является гомоморфизмом G на G/H:

$$\pi(xy) = xyH = xHyH = \pi(x)\pi(y).$$

Это этображение π называется **канонической проекцией** G на G/H.

§ 12♢. Первые примеры фактор-групп

1. Первые примеры фактор-групп. Приведем несколько очевидных примеров.

• **Группа классов вычетов.** Пусть $G = \mathbb{Z}$, $H = m\mathbb{Z}$. Тогда $G/H = \mathbb{Z}/m\mathbb{Z}$ есть уже знакомая нам аддитивная группа классов вычетов по модулю m.

• **Фактор-группы группы $\mathbb{R}^*$.** Пусть $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ — мультипликативная группа ненулевых вещественных чисел, а $H = \mathbb{R}_+ = \{\lambda \in \mathbb{R} \mid \lambda > 0\}$ — подгруппа положительных вещественных чисел. Тогда $G/H = \{\mathbb{R}_+, -\mathbb{R}_+\} \cong \{\pm 1\}$. С другой стороны, если $H = \{\pm 1\}$, то $G/H = \{\{\pm\lambda\}, \lambda \in \mathbb{R}_+\} \cong \mathbb{R}_+$. Конечно, это связано с тем, что $\mathbb{R}^* = \mathbb{R}_+ \times \{\pm 1\}$.

• **Группа дробных частей.** Пусть $G = \mathbb{R}^+$ — аддитивная группа вещественных чисел, $H = \mathbb{Z}$. Тогда $G/H = \{\lambda + \mathbb{Z}, \lambda \in [0, 1)\}$ состоит из дробных частей вещественных чисел, при этом сумма двух дробных частей $x, y \in [0, 1)$ — это их обычная сумма $x + y$, как вещественных чисел, если $x + y < 1$ и $x + y - 1$, если $x + y \geq 1$. Легко видеть, что $x \mapsto \cos(2\pi x) + i \sin(2\pi x)$ определяет изоморфизм G/H на мультипликативную группу $\mathbb{T}$ комплексных чисел по модулю равных 1.

• **Фактор-группы $\mathbb{C}^*$.** Пусть $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ — мультипликативная группа ненулевых вещественных чисел, а $H = \mathbb{R}_{>0}$ — подгруппа положительных вещественных чисел. Тогда $G/H = \{\{\varphi\mathbb{R}_{>0}\}, \varphi \in \mathbb{T}\} \cong \mathbb{T}$. С другой стороны, если $H = \mathbb{T}$, то $G/H = \{\{\lambda\mathbb{T}\}, \lambda \in \mathbb{R}_{>0}\} \cong \mathbb{R}_{>0}$. В действительности, это связано с тем, что $\mathbb{C}^* = \mathbb{R}_{>0} \times \mathbb{T}$.

• **Перестановки по модулю четных перестановок.** Пусть $G = S_n$ — симметрическая группа, а $H = A_n$ — знакопеременная группа степени n. Тогда $G/H \cong \{\pm 1\}$. Этот пример (знак перестановки) будет подробно рассмотрен в главе 5.

• Группа $S_3 \cong S_4/V$ является фактор-группой S_4 по модулю четверной группы V.

2. Фактор-группа по центру. Пусть G — произвольная группа, $C(G)$ — ее центр. Тогда фактор-группа $G/C(G) \cong \mathrm{Inn}(G)$ изоморфна группе внутренних автоморфизмов G. Сейчас мы покажем, что если группа $\mathrm{Inn}(G)$ циклическая, то она тривиальна.

Задача. Покажите, что фактор-группа неабелевой группы по центру не может быть циклической.

Решение. Предположим, что $G/C(G)$ циклическая. Это значит, что найдется класс $xC(G)$, $x \in G$, который порождает $G/C(G)$. Тем самым, любой класс G по $C(G)$ имеет вид $x^nC(G)$. Иными словами,

любой элемент $g \in G$ в виде $x^m a$, для некоторых $m \in \mathbb{Z}$, $a \in C(G)$. Ясно, что два любых элемента такого вида коммутируют: $(x^m a)(x^n b) = x^{m+n}ab = (x^n b)(x^m a)$.

Следующее класс групп играет основную роль в классификации конечных простых групп. Группа G называется **квазипростой**, если она совершенна, т. е. $[G, G] = G$, и фактор-группа $G/C(G)$ проста. В этом случае G называется **накрывающей группой** для $G/C(G)$. Дело в том, что обычно гораздо проще построить не саму простую группу, а какую-то ее накрывающую. Например, в § 18 мы выясним, что $I^\star$ является накрывающей для A_5. Исайа Шур [175] обнаружил, что существуют накрытия групп A_6 и A_7 с центром порядка 6, в то время как ни одна из групп A_n, $n \geq 8$, не допускает никаких нетривиальных накрытий.

§ 13◇. Теоремы о соответствии

Пусть $H \trianglelefteq G$. Сейчас мы построим изоморфизм между решетками $L(G, H)$ и $L(G/H) = L(1, G/H)$.

Теорема. *Пусть $H \trianglelefteq G$ и $\pi : G \longrightarrow G/H$. Тогда сопоставление $\varphi : F \mapsto \pi(F) = F/H$ устанавливает биекцию между множеством всех подгрупп в G, содержащих H, и множеством всех подгрупп в G/H. Эта биекция сохраняет включения, пересечения и порождения, а также свойство нормальности. Иными словами, для любых $H \leq F, K \leq G$ имеем:*

i) $F \leq K \iff F/H \leq K/H$;

ii) $\varphi(F \cap K) = \varphi(F) \cap \varphi(K)$;

iii) $\varphi(\langle F, K\rangle) = \langle \varphi(F), \varphi(K)\rangle$;

iv) $F \trianglelefteq G \iff F/H \trianglelefteq G/H$.

Доказательство. Так как $H \leq F \leq G$, $H \trianglelefteq G$ влечет $H \trianglelefteq F$, мы можем рассматривать F/H как подгруппу в G/H. Предположим, что $H \leq F, K \leq G$ — две подгруппы в G такие, что $F/H = K/H$. Тогда для любого $f \in F$ найдется такое $k \in K$, что $fH = kH$ и, тем самым, $f \in KH = K$. Обратное включение проверяется аналогично. Тем самым, $\varphi : L(G, H) \longrightarrow L(G/H, 1)$ инъективно. С другой стороны, если $L \leq G/H$ — подгруппа в G/H, то $F = \pi^{-1}(L) \geq H$ и, так как π сюръекция, то $\pi(F) = \pi(\pi^{-1}(L)) = L$. Тем самым, φ сюръекктивно, как и утверждалось. Проверка свойств i–iv совершенно элементарна и оставляется читателю в качестве упражнения.

В частности, для структурных решеток отсюда вытекает, что

$$\Theta(H,G) \cong \Theta(G/H) = \Theta(1,G/H).$$

Задача. Пусть $H \leq G$. Предположим, что $|H| = 5$ и $G/H \cong S_3$. Покажите, что тогда в G есть нормальная подгруппа порядка 15 и 3 сопряженных подгруппы порядка 10.

Задача. Докажите, что если $F, H \trianglelefteq G$, то существует мономорфизм

$$G/F \cap H \longrightarrow G/F \times G/H.$$

При решении следующей задачи полезно понимать, что **нормальная максимальная подгруппа** — это совсем не то же самое, что *максимальная нормальная подгруппа*. Нормальная максимальная подгруппа максимальна среди *всех* подгрупп, в то время как максимальная нормальная — только среди *нормальных*.

Задача. Пусть $H \trianglelefteq G$ — нормальная максимальная подгруппа. Тогда индекс $|G:H|$ конечен и является простым числом.

Пусть $H \leq G$ — произвольная подгруппа группы G, а $F \trianglelefteq H$ — ее нормальный делитель. Тогда фактор-группа H/F называется **секцией** группы G. Все секции — а не только фактор-группы — вплетены в структуру подгрупп группы G.

Задача. Пусть $F \trianglelefteq H \leq G$. Докажите, что решетка $L(F,G)$ содержит подрешетку изоморфную $L(H/F)$.

§ 14♠. Counting argument

Сейчас мы покажем, что уже простейшее соображение, что для любой нормальной подгруппы $H \trianglelefteq G$ существует гомоморфизм на фактор-группу, позволяет доказывать отсутствие нормальных подгрупп различных индексов [176]. Мы предполагаем, что читатель уже знаком с теоремой Коши, по которой в группе порядка 30 существуют элементы порядков 3 и 5.

Задача. Пусть G — конечная группа, $H \trianglelefteq G$, а $x \in G$ — элемент порядок которого $o(x)$ взаимно прост с индексом $|G:H|$. Докажите, что тогда $x \in H$.

Решение. Порядок xH в фактор-группе G/H делит как $o(x)$, так и $|G:H|$, а значит равен 1. Эта задача обобщается следующим образом.

Следствие. *Пусть G — конечная группа, $H \trianglelefteq G$, а $F \leq G$ — подгруппа, порядок которой $|F|$ взаимно прост с индексом $|G:H|$. Тогда $F \leq H$.*

Задача. Докажите, что группа $A_5 \cong \mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$ проста.

Решение. По теореме Лагранжа порядок нетривиальной нормальной подгруппы $H \trianglelefteq G$ может принимать следующие значения: 2, 3, 4, 5, 6, 12, 15, 20 или 30. В

группе A_5 имеется 24 элемента порядка 3. Таким образом, каждая нормальная подгруппа порядка 3, 6, 12 или 15 должна содержать все эти элементы, что невозможно. С другой стороны, в группе A_5 имеется 20 элементов порядка 5. Значит, каждая нормальная подгруппа порядка 5, 10 или 20 должна содержать все эти элементы, что также невозможно. Если $|H| = 30$, то она должна содержать как все 24 элемента порядка 3, так и все 20 элементов порядка 5. Наконец, в группе A_5 имеется 15 элементов порядка 2, и группа порядка 4 обязана содержать их все.

Таким образом, нам остается только доказать, что в группе A_5 нет нормальной подгруппы порядка 2. Это совершенно ясно, так как единственными элементами порядка 2 в A_5 являются произведения двух транспозиций и, если $(ij)(hk) \in H$, то

$$(ik)(jh) = (ijk)^{-1}(ij)(hk)(ijk) \in H,$$

что невозможно. Для чистоты эксперимента можно рассуждать и следующим образом. Точно так же, как выше, можно показать, что группа A_5/H порядка 30 содержит нормальную подгруппу F/H порядка 3 или 5. Но тогда прообраз F такой подгруппы в A_5 тоже нормален, а мы только что показали, что нормальных подгрупп порядков 6 и 10 в A_5 нет.

Задача. Докажите в том же духе, что группа $\mathrm{PSL}(2,7)$ порядка 168 проста.

Задача. Попробуйте доказать в том же духе, что группа $A_6 \cong \mathrm{PSL}(2,9)$ проста. Какие порядки Вам не удается сразу элиминировать?

Указание. Группа A_6 содержит 45 элементов порядка 2, 40+40 элементов порядка 3, 90 элементов порядка 4 и 144 элемента порядка 5.

§ 15♡. Примеры нормальных подгрупп и фактор-групп в линейных группах

1. Очевидные примеры. В следующих примерах нормальность проверяется совсем легко.

• **Обратимые матрицы по модулю матриц с определителем 1.** Пусть R — коммутативное кольцо с 1, $G = \mathrm{GL}(n,R)$ – группа всех обратимых матриц степени n, а $H = \mathrm{SL}(n,R)$ – подгруппа матриц с определителем 1. Тогда $G/H \cong R^*$. Этот пример (определитель) подробно рассмотрен в книге IV.

• **Треугольные матрицы по модулю унитреугольных.** Группа $U = U(n,K)$ верхних унитреугольных матриц является нормальным делителем в группе $B = B(n,K)$ верхних треугольных матриц, причем фактор-группа B/U изоморфна группе $D = D(n,K)$ диагональных матриц.

• **Мономиальные матрицы по модулю диагональных.** Группа $D = D(n,K)$ диагональных матриц является нормальным делителем в группе $N = N(n,K)$, причем фактор-группа N/D изоморфна S_n.

• **Аффинные преобразования по модулю трансляций.** Векторная группа K^n является нормальным делителем аффинной группы $\mathrm{Aff}(n,K)$, причем фактор-группа $\mathrm{Aff}(n,K)/K^n$ изоморфна полной линейной группе $\mathrm{GL}(n,K)$.

2. Главная конгруэнц-подгруппа. Следующий классический пример играет ключевую роль в аналитической теории чисел и теории модулярных функций и модулярных форм (в классическом случае $n=2$). Пусть $m\in\mathbb{Z}$, обозначим через $\Gamma_m=\mathrm{SL}(n,\mathbb{Z},m\mathbb{Z})$ подгруппу в специальной линейной группе $\mathrm{SL}(n,\mathbb{Z})$, состоящую из всех матриц, сравнимых с e по модулю m. Иными словами, $x=(x_{ij})$ в том и только том случае принадлежит Γ_m, когда $x_{ij}\equiv\delta_{ij}$. Группа Γ_m называется **главной конгруэнц-подгруппой** уровня m. Проверьте, что $\Gamma_m=\mathrm{SL}(n,\mathbb{Z},m\mathbb{Z})$ является нормальной подгруппой в $\mathrm{SL}(n,\mathbb{Z})$, причем

$$\mathrm{SL}(n,\mathbb{Z})/\mathrm{SL}(n,\mathbb{Z},m\mathbb{Z})\cong\mathrm{SL}(n,\mathbb{Z}/m\mathbb{Z}).$$

3. Проективные линейные группы. Сейчас мы построим еще два важнейших примера фактор-групп. Пусть $\mathrm{GL}(n,R)$ – полная линейная группа степени n над полем K. Назовем **проективной полной линейной группой** $\mathrm{PGL}(n,K)$ фактор-группу $\mathrm{GL}(n,K)$ по ее центру, состоящему из скалярных матриц λe, $\lambda\in K^*$. Таким образом, элементы $\mathrm{PGL}(n,K)$ представляются матрицами над K, причем класс матрицы $x\in\mathrm{GL}(n,K)$ в проективной группе $\mathrm{PGL}(n,K)$ обычно обозначается $[x]$. В частности, в группе $\mathrm{PGL}(2,K)$ для любого $\lambda\in K^*$ имеем

$$\begin{bmatrix}a&b\\c&d\end{bmatrix}=\begin{bmatrix}\lambda a&\lambda b\\\lambda c&\lambda d\end{bmatrix}.$$

В качестве примера отметим, что преобразование Мебиуса $z\mapsto\dfrac{az+b}{cz+d}$ зависит не от самой матрицы $\begin{pmatrix}a&b\\c&d\end{pmatrix}$, а лишь от ее класса $\begin{bmatrix}a&b\\c&d\end{bmatrix}$. Таким образом, группа Мебиуса изоморфна $\mathrm{PGL}(2,\mathbb{C})$. Еще одна серия примеров, которая будет играть для нас совершенно особую роль, это группы $\mathrm{PGL}(n,\mathbb{F}_q)$ над конечным полем $\mathbb{F}_q$. Обычно обозначение $\mathrm{PGL}(n,\mathbb{F}_q)$ сокращается до $\mathrm{PGL}(n,q)$.

Отступление. Строго говоря, с точки зрения теории алгебраических групп приведенное выше определение является *неправильным*, но для случая поля оно *совпадает* с правильным. Во многих книгах проективная линейная группа $\mathrm{PGL}(n,R)$ и для коммутативного кольца R **ошибочно** определяется как $\mathrm{GL}(n,R)/R^*$. Это грубейшее заблуждение! В действительности, элементы $\mathrm{PGL}(n,R)$ тоже представляются как классы матриц, но, вообще говоря, не над самим кольцом R, а над

некоторым его расширением. Причины, по которым для поля $\mathrm{PGL}(n,K)$ совпадает с $\mathrm{GL}(n,K)/K^*$, *слишком* глубоки, чтобы обсуждать их здесь.

В свою очередь, **проективная специальная линейная группа** $\mathrm{PSL}(n,K)$ это фактор-группа специальной линейной группы $\mathrm{SL}(n,K)$ по ее центру, состоящему из тех скалярных матриц λe, $\lambda \in \mu_n(K)$, для которых λ является корнем n-й степени из 1 в поле K. Большинство алгебраистов сокращают $\mathrm{PSL}(n,\mathbb{F}_q)$ до $\mathrm{PSL}(n,q)$, а специалисты по конечным группам используют стенографическую запись $A_n(q)$ или $L_n(q)$. Группы $\mathrm{PSL}(n,q)$ замечательны тем, они образуют серию конечных простых групп. Одна из самых знаменитых классических теорем алгебры, теорема Жордана—Диксона, утверждает, что все группы $\mathrm{PSL}(n,q)$ просты, кроме ровно двух исключений $\mathrm{PSL}(2,2) \cong S_3$ и $\mathrm{PSL}(2,3) \cong A_4$.

Леонард Юджин Диксон (Leonard Eugene Dickson, 22 января 1874, Индепенденс, Айова — 17 января 1954, Харлинген, Техас) — замечательный американский математик, один из величайших классиков алгебры и теории чисел начала XX века. Диксон начал обучение в Техасе, но в 1894 году поступил в аспирантуру в Чикаго, где его руководителем стал Элиаким Мур. После защиты диссертации в 1896 году он поехал в Европу, где провел некоторое время в Лейпциге у Ли и в Париже у Жордана. После возвращения в США он скитался по разным университетам, пока в 1900 году Университет Чикаго не предложил ему постоянную позицию, которую он немедленно принял, и где он оставался профессором до 1939 года.

В эти годы он получил несколько совершенно замечательных результатов в области теории алгебр, аналитической теории чисел, теории квадратичных форм и, в первую очередь, теории линейных групп, классических групп и исключительных групп. В 1901 году появился его классический труд *Linear groups with an exposition of the Galois field theory*, с которого, собственно, и начинается существование теории линейных групп как самостоятельной науки [177]. Всего Диксон опубликовал 18 книг, в том числе знаменитую трехтомную *Историю теории чисел*.

С моей точки зрения вклад Диксона в алгебру незаслужено малоизвестен и зачастую недооценивается. Например, в годы моего ученичества один из наших выдающихся числовиков называл Диксона "писателем в области теории чисел". Именно Диксон — а не Веддербарн, как это принято считать — дал первое правильное доказательство малой теоремы Веддербарна [178]. Он доказал теоремы Витта в год рождения Витта, а в 1905 году, за 50 лет до Шевалле он построил группы Шевалле типов E_6 и G_2 над произвольным полем. Однако, когда в тридцатые годы XX века в математике началось триумфальное шествие абстракционизма, *конкретные* работы Диксона были не поняты и забыты.

Задача. Докажите, что $\mathrm{PGL}(2,\mathbb{C}) \cong \mathrm{PSL}(2,\mathbb{C})$. Верно ли, что и $\mathrm{PGL}(2,\mathbb{R}) \cong \mathrm{PSL}(2,\mathbb{R})$?

4. Клейновы и фуксовы группы. Любая дискретная подгруппа в $\mathrm{PSL}(2,\mathbb{R})$ называется **фуксовой группой**, а дискретная подгруппа в $\mathrm{PSL}(2,\mathbb{C})$ — **клейновой группой**. Классическим примером фуксовой группы является классическая **модулярная группа** $\mathrm{PSL}(2,\mathbb{Z})$. Аналогично, примером клейновой группы является **группа Пикара** $\mathrm{PSL}(2,\mathbb{Z}[i])$. Вообще, группа $\mathrm{PSL}(2,\mathcal{O}_d)$, где $\mathcal{O}_d)$ — кольцо целых мнимого квадратичного поля $\mathbb{Q}[\sqrt{-d}]$ называется **группой Бьянки**.

Предостережение. Употребление термина группа Пикара в совершенно другом смысле уже было описано в главе 1.

§ 16♠. Бинарные группы многогранников, 1st instalment: группа $T^\star$

В этом и двух следующих параграфах мы построим и отождествим некоторые замечательные подгруппы в мультипликативной группе классических кватернионов [**264**], § 20, которые вскользь упоминались в главе 1. Прежде всего, напомним, что $\mathbb{Z}$-линейная оболочка группы $Q = \{\pm 1, \pm i, \pm, j, \pm, k\}$ кватернионных единиц называется кольцом **целых липшицевых кватернионов** [179]:

$$\mathrm{Lip} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{Z}\}.$$

Однако в действительности интересующие нас группы будут группами единиц чуть больших колец [180], самым известным из которых является кольцо Hurw **целых гурвицевых кватернионов** [181]:

$$\mathrm{Hurw} = \mathrm{Lip} \coprod \tfrac{1}{2}(1 + i + j + k) + \mathrm{Lip},$$

состоящее из кватернионов, все координаты которых либо одновременно целые, либо одновременно полуцелые.

> **Адольф Гурвиц** (`Adolf Hurwitz`, 26 марта 1859, Хильдесхайм 18 ноября 1919, Цюрих) — замечательный немецкий математик, основные работы которого относятся к алгебре, теории чисел, алгебраической геометрии, теории римановых поверхностей и комплексному анализу. Гурвиц учился в Берлине у Куммера, Вейерштрасса и Кронекера, и в 1881 году защитил диссертацию в Лейпциге под руководством Клейна. Уже в 1884 году он стал профессором в Кенигсберге, где его студентами — а потом и ближайшими друзьями — стали Гильберт и Минковский. В 1892 году Фробениус возвращается в Берлин, и Гурвиц занимает освободившуюся кафедру в Цюрихе, где и остается до конца жизни. Кроме целых гурвицевых кватернионов в нашем курсе встречаются гурвицевы группы и теорема Гурвица о суммах квадратов.

Для решения следующих задач полезно ввести элемент $\omega = \frac{1}{2}(-1 + i + j + k)$. Вместе с $1, i, j, k$ этот элемент порождает Hurw над $\mathbb{Z}$. Непонятно, с какой стати он обозначается тем же символом ω, которым мы всегда обозначали $\frac{1}{2} + i\frac{\sqrt{3}}{2}$! **Или**?

Задача. Найдите порядок ω.

Ответ. Легко видеть, что $\omega^2 = \overline{\omega}$ и, значит, $\omega^3 = e$.

Задача. Докажите, что следующие 24 кватерниона

$$T^\star = \{\pm 1,\ \pm i,\ \pm j,\ \pm k,\ \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}$$

образуют группу. Эта группа называется **бинарной группой тетраэдра**.

Решение. Полезно заметить, что все перечисленные элементы имеют вид ± 1, $\pm i$, $\pm j$, $\pm k$, $\pm\omega$, $\pm\omega^i$, $\pm\omega^j$, $\pm\omega^k$, $\pm\overline{\omega}$, $\pm\overline{\omega}^i$, $\pm\overline{\omega}^j$, $\pm\overline{\omega}^k$.

$$\omega^i = i^{-1}\omega i = j\omega = \omega k = \overline{\omega} + i = \frac{1}{2}(-1 + i - j - k),$$

$$\omega^j = j^{-1}\omega j = k\omega = \omega i = \overline{\omega} + j = \frac{1}{2}(-1 - i + j - k),$$

$$\omega^k = k^{-1}\omega k = i\omega = \omega j = \overline{\omega} + k = \frac{1}{2}(-1 - i - j + k),$$

$$\overline{\omega}^i = i^{-1}\overline{\omega} i = -k\overline{\omega} = -\overline{\omega} j = \omega - i = \frac{1}{2}(-1 - i + j + k),$$

$$\overline{\omega}^j = j^{-1}\overline{\omega} j = -i\overline{\omega} = -\overline{\omega} k = \omega - j = \frac{1}{2}(-1 + i - j + k),$$

$$\overline{\omega}^k = k^{-1}\overline{\omega} k = -j\overline{\omega} = -\overline{\omega} i = \omega - k = \frac{1}{2}(-1 + i + j - k),$$

Задача. Докажите, что $T^\star = \langle i, \omega \rangle$.

Предостережение. В следующей задаче, как и в соответствующих местах двух ближайших параграфов, чтобы легче установить соответствия с другими работами, где рассматриваются бинарные группы многогранников, мы считаем, что перестановки умножаются **слева направо**. Обычно в настоящей книге — например, в главе 5 — используется противоположное соглашение. А именно, обычно мы умножаем перестановки *как отображения*, т. е. справа налево. Перейти от изоморфизма в используемой здесь записи к изоморфизму в обычной записи совсем просто. Можно, например, заменить все перестановки на обратные.

Задача. Докажите, что фактор-группа $T^\star$ по ± 1 изоморфна A_4.

Ответ. Приведем явный вид этого изоморфизма. Прежде всего вспомним, что $Q/\{\pm 1\} \cong V$:

$$e \mapsto \mathrm{id}, \quad i \mapsto (12)(34), \quad j \mapsto (13)(24), \quad k \mapsto (14)(23).$$

Остальные 8 классов переходят в 3-циклы. Задание образа одного из них, скажем ω, сразу фиксирует образы всех остальных, если вспомнить, что $\omega^2 = \overline{\omega}$, а все остальные сопряжены с образом ω или $\overline{\omega}$ под действием V:

$$\omega \mapsto (234), \quad \omega^i \mapsto (143), \quad \omega^j \mapsto (124), \quad \omega^k \mapsto (132),$$

$$\overline{\omega} \mapsto (243), \quad \overline{\omega}^i \mapsto (134), \quad \overline{\omega}^j \mapsto (142), \quad \overline{\omega}^k \mapsto (123).$$

В действительности можно доказать значительно более точное утверждение.

Задача. Докажите, что $T^\star \cong \mathrm{SL}(2,3)$.

Решение. (Ноам Элкис [182]) Так как для двух любых кватернионов $w, z \in T^\star$ выполняется неравенство $|w - z| \leq 2$, то для любого нечетного простого $p \in \mathbb{P}$ ограничение проекции $\pi : \mathrm{Hurw} \longrightarrow \mathrm{Hurw}\,/p\,\mathrm{Hurw}$ на группу $T^\star$ инъективно. Но по малой теореме Веддербарна $\mathrm{Hurw}\,/p\,\mathrm{Hurw}$ изоморфна алгебре матриц $M(2,\mathbb{F}_p)$, причем кватернионная норма соответствует определителю. Таким образом, группа $T^\star$ *вкладывается* в $\mathrm{SL}(2,p)$. Но ведь группа $\mathrm{SL}(2,3)$ содержит ровно 24 элемента!

§ 17♠. Бинарные группы многогранников, 2nd instalment: группа $O^\star$

Продолжим **глумиться*** над кватернионами. Для этого введем элемент $\theta = (1+i)/\sqrt{2}$. Этот элемент замечателен тем, что вместе с Hurw порождает еще одно эвклидово подкольцо [183] в теле $\mathbb{H}$.

Задача. Найдите порядок θ и порядок подгруппы $\langle i, \theta\rangle$.

Решение. Ясно, что $i = \theta^2$ так что $\langle i, \theta\rangle = \langle\theta\rangle \cong C_8$.

Задача. Докажите, что следующие 48 кватернионов

$$O^\star = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k),$$
$$\frac{1}{\sqrt{2}}(\pm 1 \pm i), \frac{1}{\sqrt{2}}(\pm 1 \pm j), \frac{1}{\sqrt{2}}(\pm 1 \pm k), \frac{1}{\sqrt{2}}(\pm i \pm j), \frac{1}{\sqrt{2}}(\pm i \pm k), \frac{1}{\sqrt{2}}(\pm j \pm k)\}$$

образуют группу. Эта группа называется **бинарной группой октаэдра**.

Указание. Можно, например, заметить, что

$$\theta = \frac{1}{\sqrt{2}}(1+i),\ \overline{\theta} = \frac{1}{\sqrt{2}}(1-i),\ \omega^2\theta\omega = \frac{1}{\sqrt{2}}(1+j),$$
$$\omega^2\overline{\theta}\omega = \frac{1}{\sqrt{2}}(1-j),\ \omega\theta\omega^2 = \frac{1}{\sqrt{2}}(1+k),\ \omega\overline{\theta}\omega^2 = \frac{1}{\sqrt{2}}(1-k).$$

и, by the same token,

$$-\omega^2\theta = \frac{1}{\sqrt{2}}(i+j),\ k\omega^2\theta = \frac{1}{\sqrt{2}}(i-j),\ -\theta\omega^2 = \frac{1}{\sqrt{2}}(i+k),$$
$$-j\theta\omega^2 = \frac{1}{\sqrt{2}}(i-k),\ -\omega\theta\omega = \frac{1}{\sqrt{2}}(j+k),\ i\omega\theta\omega = \frac{1}{\sqrt{2}}(j-k).$$

После этого легко составить такую же таблицу умножения, как в предыдущем параграфе. Однако гораздо проще вспомнить, что $\theta^2 \in T^\star$ и воспользоваться следующей задачей.

---

*Андрей Семенов выразил сомнение, что это слово будет правильно истолковано современным читателем. Действительно, **глумиться** употреблено здесь в своем исконном значении: рассуждать или размышлять о чем-то, забавляться, упражняться (*в этом лесу леший глумится*).

Задача. Убедитесь, что $O^\star = T^\star \coprod T^\star\theta = T^\star \coprod \theta T^\star$.

Задача. Найдите порядки подгрупп $\langle j, \theta\rangle$, $\langle k, \theta\rangle$.

Решение. Ясно, что $j^{-1}\theta j = k^{-1}\theta k = \theta^{-1}$ и $k = \theta j \theta^{-1}$, так что $\langle j, \theta\rangle = \langle k, \theta\rangle \cong D_8$.

Задача. Докажите, что $O^\star = \langle \omega, \theta\rangle$.

Решение. Так как $i = \theta^2$, то группа $\langle \omega, \theta\rangle$ содержит $\langle i, \omega\rangle$, а как мы знаем из предыдущего параграфа, эта группа совпадает с $T^\star$. Но ведь, $\theta \notin T^\star$, а никаких собственных подгрупп в $O^\star$, содержащих $T^\star$, нет.

Задача. Докажите, что фактор-группа $O^\star$ по ± 1 изоморфна S_4.

Решение. Построим изоморфизм, продолжающий построенный в предыдущем параграфе изоморфизм $T^\star/\{\pm 1\} \cong A_4$. Чего уж там, образы элементов $\frac{1}{\sqrt{2}}(\pm 1 \pm i)$, $\frac{1}{\sqrt{2}}(\pm 1 \pm j)$, $\frac{1}{\sqrt{2}}(\pm 1 \pm k)$, в фактор-группе по $\{\pm 1\}$ должны иметь порядок 4, а образы элементов $\frac{1}{\sqrt{2}}(\pm i \pm j)$, $\frac{1}{\sqrt{2}}(\pm i \pm k)$, $\frac{1}{\sqrt{2}}(\pm j \pm k)$ — порядок 2. Таким образом, первые 12 элементов должны переходить в 4-циклы, а остальные 12 — в транспозиции. Так как

$$\frac{1}{\sqrt{2}}(i+j)\frac{1}{\sqrt{2}}(i-j) = \pm k, \quad \frac{1}{\sqrt{2}}(i+k)\frac{1}{\sqrt{2}}(i-k) = \pm j, \quad \frac{1}{\sqrt{2}}(j+k)\frac{1}{\sqrt{2}}(j-k) = \pm i,$$

то можно взять, например,

$$\frac{1}{\sqrt{2}}(i+j) \mapsto (14), \quad \frac{1}{\sqrt{2}}(i+k) \mapsto (13), \quad \frac{1}{\sqrt{2}}(j+k) \mapsto (12),$$
$$\frac{1}{\sqrt{2}}(i-j) \mapsto (23), \quad \frac{1}{\sqrt{2}}(i-k) \mapsto (24), \quad \frac{1}{\sqrt{2}}(j-k) \mapsto (34).$$

Умножая эти равенства на i, j, k, получаем

$$\frac{1}{\sqrt{2}}(1+i) \mapsto (1423), \quad \frac{1}{\sqrt{2}}(1+j) \mapsto (1234), \quad \frac{1}{\sqrt{2}}(1+k) \mapsto (1342),$$
$$\frac{1}{\sqrt{2}}(1-i) \mapsto (1324), \quad \frac{1}{\sqrt{2}}(1-j) \mapsto (1432), \quad \frac{1}{\sqrt{2}}(1-k) \mapsto (1243).$$

§ 18♠. Бинарные группы многогранников, 3rd instalment: группа $I^\star$

Теперь нам осталось только схватить главаря. Вернемся к рассмотрению поля золотого сечения $\mathbb{Q}(\sqrt{5})$, которое уже встречалось нам в § 11 главы 1. Вспомним, что $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\sigma) = \mathbb{Q}(\tau)$, где $\sigma = \frac{1}{2}(1-\sqrt{5})$, а $\tau = \frac{1}{2}(1+\sqrt{5})$, причем $\sigma = \tau^{-1}$.

Задача. Докажите, что следующие 120 кватернионов:

• уже встречавшиеся нам 24 кватерниона $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$, образующие группу $T^\star$,

• 96 кватернионов, получающихся из $\frac{1}{2}(\pm i\pm\sigma j\pm\tau k)$ **четными** перестановками $1, i, j, k$,

образуют группу. Эта группа называется **бинарной группой икосаэдра** и обозначается $I^\star$. Иногда, следуя Гамильтону, эту группу называют еще **группой икосианов**. Совершенно особую роль в построении спорадических групп играет **кольцо икосианов** $\mathrm{Icos} = \mathbb{Z}I^\star$, состоящее из всевозможных целочисленных линейных комбинаций элементов группы $I^\star$.

Указание. Можете поупражняться в умножении кватернионов или воспользоватеься приведенными в следующем параграфе командами пакета `Mathematica`. Однако гораздо проще ввести в рассмотрение элемент $\zeta = \frac{1}{2}(\sigma + i + \tau j)$, заметить, что $\zeta^5 \in T^\star$, и воспользоваться следующей задачей.

Задача. Убедитесь, что

$$I^\star = T^\star \coprod T^\star\zeta \coprod T^\star\zeta^2 \coprod T^\star\zeta^3 \coprod T^\star\zeta^4 = T^\star \coprod \zeta T^\star \coprod \zeta^2 T^\star \coprod \zeta^3 T^\star \coprod \zeta^4 T^\star.$$

Если Вы овладели идеей, Вам ничего не стоит решить следующую задачу.

Задача. Докажите, что следующие 120 кватернионов:

• уже встречавшиеся нам 24 кватерниона $\pm1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm1 \pm i \pm j \pm k)$, образующие группу $T^\star$,

• 96 кватернионов, получающихся из $\frac{1}{2}(\pm i \pm \sigma j \pm \tau k)$ **нечетными** перестановками $1, i, j, k$,

образуют группу.

Решение. Достаточно повторить то же рассуждение с заменой ζ на $\xi = \frac{1}{2}(\sigma + \tau i + j)$. Разумеется, получающаяся группа будет снова изоморфна $I^\star$.

Следующий замечательный факт был обнаружен в 1856 году самим Гамильтоном.

Задача. Докажите, что фактор-группа $I^\star$ по ±1 изоморфна A_5.

Решение. Сейчас мы явным образом построим изоморфизм, продолжающий построенный в § 16 изоморфизм $T^\star/\{\pm1\} \cong A_4$. Единственное отличие приводимых нами формул от формул из статьи Роберта Уилсона [184] состоит в том, что для наглядности мы переставили 1 и 5. Ясно, что достаточно задать образ одного из элементов x или $-x$. Среди элементов $I^\star \setminus T^\star$ имеется — с точностью до знака — по 12 таких, у которых коэффициент при 1 равен 0, $\frac{1}{2}$ $\frac{\sigma}{2}$ и $\frac{\tau}{2}$. Те, у которых коэффициент при 1 равен 0, имеют порядок 2 и, следовательно, переходят в произведение двух транспозиций. Так как произведения, не затрагивающие 5, уже

заняты, у нас остается ровно 12 таких произведений, как и ожидалось:

$$\frac{1}{2}(i+\sigma j+\tau k)\mapsto(14)(35),\quad \frac{1}{2}(\tau i+j+\sigma k)\mapsto(13)(45),\quad \frac{1}{2}(\sigma i+\tau j+k)\mapsto(15)(34),$$
$$\frac{1}{2}(i-\sigma j-\tau k)\mapsto(14)(25),\quad \frac{1}{2}(-\tau i+j+\sigma k)\mapsto(15)(24),\quad \frac{1}{2}(-\sigma i+\tau j+k)\mapsto(12)(45),$$
$$\frac{1}{2}(i-\sigma j+\tau k)\mapsto(15)(23),\quad \frac{1}{2}(-\tau i+j-\sigma k)\mapsto(13)(25),\quad \frac{1}{2}(\sigma i-\tau j+k)\mapsto(12)(45),$$
$$\frac{1}{2}(i+\sigma j-\tau k)\mapsto(23)(45),\quad \frac{1}{2}(\tau i+j-\sigma k)\mapsto(24)(35),\quad \frac{1}{2}(-\sigma i-\tau j+k)\mapsto(25)(34).\blacksquare$$

Общее количество 3-циклов в группе A_5 равно $2C_5^3=20$. Из них восемь 3-циклов, не затрагивающих 5, уже истрачены, так что у нас снова остается ровно 12 **штук*** 3-циклов, которые и будут образами тех 12 элементов $I^\star\setminus T^\star$, у которых коэффициент при 1 равен $\dfrac{1}{2}$, Вычисление образов облегчается тем, что сопряженные кватернионы переходят во взаимно обратные циклы. Окончательно,

$$\frac{1}{2}(-1+\tau j+\sigma k)\mapsto(154),\quad \frac{1}{2}(-1+\sigma i+\tau k)\mapsto(135),\quad \frac{1}{2}(-1+\tau i+\sigma j)\mapsto(345),$$
$$\frac{1}{2}(-1-\tau j-\sigma k)\mapsto(145),\quad \frac{1}{2}(-1-\sigma i-\tau k)\mapsto(153),\quad \frac{1}{2}(-1-\tau i-\sigma j)\mapsto(354),$$
$$\frac{1}{2}(-1+\tau j-\sigma k)\mapsto(235),\quad \frac{1}{2}(-1-\sigma i+\tau k)\mapsto(245),\quad \frac{1}{2}(-1+\tau i-\sigma j)\mapsto(152),$$
$$\frac{1}{2}(-1-\tau j+\sigma k)\mapsto(253),\quad \frac{1}{2}(-1+\sigma i-\tau k)\mapsto(254),\quad \frac{1}{2}(-1-\tau i+\sigma j)\mapsto(125),$$

Теперь в нашем распоряжении остаются, с точностью до знака, 12 икосианов у которых коэффициент при 1 равен $\dfrac{\sigma}{2}$ и 12 икосианов, у которых этот коэффициент равен $\dfrac{\tau}{2}$. Эти икосианы могут переходить только в 5-циклы и у нас на самом деле имеется $4!=24$ штук 5-циклов в A_5. Снова вычисление облегчается тем, что сопряженные кватернионы переходят во взаимно обратные циклы. Называем третью букву имени:

$$\frac{1}{2}(-\sigma+j+\tau k)\mapsto(13524),\quad \frac{1}{2}(-\sigma+\tau i+k)\mapsto(13452),\quad \frac{1}{2}(-\sigma+i+\tau j)\mapsto(15234),$$
$$\frac{1}{2}(-\sigma-j-\tau k)\mapsto(14253),\quad \frac{1}{2}(-\sigma-\tau i-k)\mapsto(12543),\quad \frac{1}{2}(-\sigma-i-\tau j)\mapsto(14325),$$
$$\frac{1}{2}(-\sigma+j-\tau k)\mapsto(15423),\quad \frac{1}{2}(-\sigma-\tau i+k)\mapsto(12435),\quad \frac{1}{2}(-\sigma+i-\tau j)\mapsto(14532),$$
$$\frac{1}{2}(-\sigma-j+\tau k)\mapsto(13245),\quad \frac{1}{2}(-\sigma+\tau i-k)\mapsto(15342),\quad \frac{1}{2}(-\sigma-i+\tau j)\mapsto(12354).\blacksquare$$

*Штука — диалектное счетное слово, перевод китайского gê.

А вот и последняя буква имени:

$$\frac{1}{2}(-\tau+\sigma j+k)\mapsto(12534),\quad \frac{1}{2}(-\tau+i+\sigma k)\mapsto(13254),\quad \frac{1}{2}(-\tau+\sigma i+j)\mapsto(13425),$$
$$\frac{1}{2}(-\tau-\sigma j-k)\mapsto(14352),\quad \frac{1}{2}(-\tau-i-\sigma k)\mapsto(14523),\quad \frac{1}{2}(-\tau-\sigma i-j)\mapsto(15243),$$
$$\frac{1}{2}(-\tau+\sigma j-k)\mapsto(12345),\quad \frac{1}{2}(-\tau-i+\sigma k)\mapsto(15324),\quad \frac{1}{2}(-\tau+\sigma i-j)\mapsto(13542),$$
$$\frac{1}{2}(-\tau-\sigma j+k)\mapsto(15432),\quad \frac{1}{2}(-\tau+i-\sigma k)\mapsto(14235),\quad \frac{1}{2}(-\tau-\sigma i+j)\mapsto(12453).$$ ∎

§ 19♠. Вычисления с кватернионами

Для домашних умельцев укажем, как *на самом деле* проводились вычисления, результаты которых были предложены в качестве задач в трех предыдущих параграфах. Основным атрибутом алгебраиста является склонность — я бы даже сказал, **предиспозиция** — любой ценой избегать вычислений. Поэтому вместо того, чтобы 10 секунд искать порядок ω мануально, я уполномочил `Среднего Брата` сделать это за меня. Так как имплементация функции `NonCommutativeMultiply` в `Mathematica` крайне неудачна, вычисления с кватернионами проще проводить не при помощи пакета `Quaternions`, а непосредственно в матричном представлении. Ниже мы описываем эти вычисления в четырехмерном вещественном представлении. При желании можно пользоваться и двумерным комплексным представлением, но поскольку для того, чтобы распознать равенство двух комплексных матриц при этом нужно применять `ComplexExpand`, никакой реальной экономии времени это не дает. Следующие четыре матрицы описывают внутреннее представление кватернионных единиц как объектов `Mathematica`:

```
e={{1,0,0,0},{0,1,0,0},{0,0,1,0},{0,0,0,1}};
i={{0,1,0,0},{-1,0,0,0},{0,0,0,-1},{0,0,1,0}};
j={{0,0,1,0},{0,0,0,1},{-1,0,0,0},{0,-1,0,0}};
k={{0,0,0,1},{0,0,-1,0},{0,1,0,0},{-1,0,0,0}};
```

А вот обычная запись e,i,j,k как вещественных матриц:

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\ \begin{pmatrix}0&1&0&0\\-1&0&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix},\ \begin{pmatrix}0&0&1&0\\0&0&0&1\\-1&0&0&0\\0&-1&0&0\end{pmatrix},\ \begin{pmatrix}0&0&0&1\\0&0&-1&0\\0&1&0&0\\-1&0&0&0\end{pmatrix}$$

Определения следующих двух функций представляют собой типичный образец дуболомного программирования, свойственного профессиональным математикам. Однако, поскольку для большинства рекреативных задач время необходимое для написания *настоящей* программы и исправление ошибок в ней в сотни раз больше, чем время вычисления, подобная прямолинейность вполне оправдана. Дело в том, что написание программы в таком стиле занимает 2–3 минуты, а возможность совершить ошибку при этом минимальна. А поскольку для матриц степени ≤ 10 и для групп порядка нескольких сотен элементов вычисление при помощи этих функций занимает несколько секунд, борьба за снижение времени с $O(n^3)$

до $O(n^e)$ is not worth the candle. Если же Вам действительно нужно считать в группах порядка нескольких миллионов или миллиардов, то это нужно делать на других машинах и уж, конечно, совсем другими программными средствами. А для того, чтобы считать в группах порядка 10^{54}, недостаточно просто уметь программировать. Для этого неплохо, кроме того, *реально* понимать, что Вы делаете, т. е. иметь непосредственный контакт с миром идей. Следующая функция определяет произведение по Минковскому двух подмножеств x и y в $M(n,K)$:

```
mink[x_,y_]:=Union[Flatten[Table[Simplify[x[[i]].y[[j]]],
                          {i,1,Length[x]},{j,1,Length[y]}],1]]
```

Субстанциально здесь происходит следующее: поочередно выбирается каждый элемент `x[[i]]` множества x и поочередно умножается на каждый элемент `y[[j]]` множества y. Смысл остальных команд следующий: `Simplify` нужно, чтобы произвести сокращения в произведениях x_iy_j, без которых `Mathematica` может ненароком не обратить внимания на равенство двух матриц и принять их за различные[♮]; `Flatten[blabla,1]` делает из получающегося двумерного списка матриц x_iy_j одномерный и, наконец, `Union` устраняет повторения в возникающем списке. Теперь чтобы определить подгруппу (в действительности, подполугруппу, но для *конечных* подгрупп в $\mathrm{GL}(n,K)$ это одно и то же!) в $\mathrm{GL}(n,K)$, порожденную множеством x, мы организуем незатейливый цикл:

```
span[x_]:=Block[{y,z},y=Union[{e},x];z=Union[y,mink[y,x]];
                      While[z!=y,y=z;z=Union[y,mink[y,x]]];Return[y]]
```

После этого совсем легко определить, какую группу определяют какое-то множество кватернионов. Для этого положим

```
sigma=(1-Sqrt[5])/2;          tau=(1+Sqrt[5])/2;
```

и определим следующие кватернионы[♭]:

```
omega=(-e+i+j+k)/2;           theta=(e+i)/Sqrt[2];
xi=(sigma*e+i+tau*j)/2;       zeta=(sigma*e+tau*i+j)/2;
```

Теперь, спрашивая `Length[span[k,zeta]]`, мы узнаем, что порядок группы $\langle k,\zeta\rangle$ равен 20, а спрашивая `Length[span[omega,theta]]`, — что порядок группы $\langle\omega,\theta\rangle$ равен 48. Вот фрагмент из фактической беседы со **Средним Братом** в процессе проверки результатов предыдущего параграфа:

```
Timing[Length[span[j,zeta]]]  {0.481 Second, 120}
Timing[Length[span[omega,zeta]]]{0.671 Second, 120}
```

[♮]Более того, в комплексной форме это *систематически* происходит *после* применения `Simplify` и даже — что уж совсем одиозно — `FullSimplify`!!! В результате этого я с некоторым удивлением обнаружил подгруппы порядков 31 и 32 в группе порядка 120. Из-за плохой работы команды `Simplify` для комплексных матриц нужны более драстичные средства типа принудительного раскрытия всех скобок, овеществления и т. д. Начинающему, который не готов к такого рода **брутальностям**, проще с самого начала работать только с вещественными матрицами.

[♭]Возможно Вы захотите выбрать другое имя для кватерниона `zeta`, иначе при первой эвалюации Вам доведется увидеть сообщение: `General::"spell1": Possible spelling error: new symbol name "zeta" is similar to existing symbol "Zeta".`

```
Timing[Length[span[omega,xi]]]{0.681 Second, 120}
```

Таким образом, даже при помощи приведенных выше крайне примитивных команд порождение всех 120 элементов групп $\langle j, \zeta\rangle$, $\langle \omega, \zeta\rangle$ и $\langle \omega, \xi\rangle$ — вместе с собственно проверкой того, что это действительно группы — занимает менее 0,7 секунды работы `CPU`.

§ 20♡. Группы гомологий дифференциальных групп

Дифференциальной группой называется пара (A, ∂), где A — абелева группа, а $\partial \in \mathrm{End}(A)$ — эндоморфизм группы A такой, что $\partial^2 = 0$. Эндоморфизм ∂ обычно называется **дифференциалом**. Подгруппа $Z(A) = \mathrm{Ker}(\partial)$ называется **группой циклов** дифференциальной группы A, а ее элементы — **циклами** (отсюда обозначение `Z` — `Zyklus`). Подгруппа $B(A) = \mathrm{Im}(\partial)$ называется **группой границ** дифференциальной группы A, а ее элементы — **границами** (отсюда обозначение `B` — `boundary`). Так как $\partial^2 = 0$, то $B(A) \le Z(A)$.

Фактор-группа $H(A) = Z(A)/B(A)$ называется **группой гомологий** дифференциальной группы A. Элементы $H(A)$ называются **классами гомологий**. Циклы $x, y \in Z(A)$ называются **гомологичными**, если $x - y \in B(A)$.

Если (A, ∂_A) и (B, ∂_B) — две дифференциальные группы, то **гомоморфизмом дифференциальных групп** называется такой гомоморфизм абелевых групп $\varphi : A \longrightarrow B$, который коммутирует с дифференциалом в том смысле, что квадрат

$$\begin{array}{ccc} A & \xrightarrow{\varphi} & B \\ {\scriptstyle\partial_A}\downarrow & & \downarrow{\scriptstyle\partial_B} \\ A & \xrightarrow[\varphi]{} & B \end{array}$$

коммутативен, т. е., иными словами, $\varphi \circ \partial_A = \partial_B \circ \varphi$. Обычно дифференциал во всех дифференциальных группах обозначается просто через ∂, так что это равенство записывается как $\varphi \circ \partial = \partial \circ \varphi$.

Ясно, что гомоморфизм $\varphi : A \longrightarrow B$ дифференциальных групп переводит циклы в циклы и границы в границы: $\varphi(Z(A)) \le Z(B)$, $\varphi(B(A)) \le B(B)$ (проверьте!). Тем самым φ индукцирует гомоморфизм групп гомологий

$$\varphi_* : H(A) \longrightarrow H(B), \quad x + B(A) \mapsto \varphi(x) + B(B).$$

Глава 4. ГОМОМОРФИЗМЫ ГРУПП

La Nature est un temple où de vivant piliers
Laissent parfois sortir de confuses paroles;
L'homme y passe à travers des forêts de symboles
Qui l'observent avec des regards familiers.

Comme de longs échos qui de loin se confondent
Dans une ténébreuse et profonde unité,
Vaste comme la nuit et comme la clarté,
Les parfums, les couleurs et les sons se répondent.

Charles Baudelaire. *Correspondances*

Вместе с каждым классом объектов естественно рассматривать допустимый класс преобразований этих объектов, согласованный с их структурой. В случае групп и других алгебраических систем такие преобразования обычно называются гомоморфизмами. Первым стал сознательно использовать гомоморфизмы групп Джон Непер в самом начале XVII века. Вот, примерно, что говорится в его сочинении 1614 года *Mirifici logarithmorum canonis descriptio*: "Ввиду того, что в математике нет ничего более трудного и приводящего к большему количеству ошибок, чем умножение, деление и извлечение квадратных и кубических корней, нет и ничего более полезного, чем замена чисел, над которыми производятся эти операции, на другие, для которых эти операции превращаются в сложение, вычитание и деление на 2 или 3". Конечно, термин `гомоморфизм` появился гораздо позже.

§ 1◇. Гомоморфизмы

1. Гомоморфизмы. Отображения, сохраняющие структуру группы, называются морфизмами в категории групп или гомоморфизмами.

Определение. *Пусть G и H — две группы. Отображение $f : G \longrightarrow H$ называется* **гомоморфизмом**, *если для любых $x, y \in G$ выполнено равенство $f(xy) = f(x)f(y)$.*

/ При этом мы предполагаем, что обе группы записаны мультипликативно. Если G и H — аддитивные группы, равенство, определяющее гомоморфизм, приняло бы форму $f(x + y) = f(x) + f(y)$, а если, например, G мультипликативна, а H аддитивна, то форму $f(xy) = f(x) + f(y)$. Словом, в каждом случае образ результата применения операции к двум элементам первой группы должен совпадать с результатом применения операции во второй группе к их образам.

Джон Непер (John Napier, 1550, Edinburgh — 4 апреля 1617, ibid.) — шотландский барон, выдающийся политический деятель, протестантский теолог и математик-любитель. Непер начал свое образование в 1563 году в университете St. Andrews, и в 1566–1571 годах продолжил его на континенте в Нидерландах и Франции. Чтобы представить, чему *примерно* он мог там научиться в области математики, полезно сопоставить годы его жизни с годами жизни двух ведущих математиков того времени, Франсуа Виета (1540–1603) и Симона Стевина (1548–1620).

Свободное от политических, религиозных и семейных (у него было 12 детей) забот время Непер посвящал вычислениям. Самым знаменитым вкладом Непера в науку является, конечно, введение им логарифмов. Кроме этого он много занимался сферической тригонометрией и механическими средствами вычислений. Именно он ввел современные обозначения для десятичных дробей.

В качестве лингвистического курьеза отметим, что, как замечают О'Коннор и Робертсон, шотландские современники Непера писали его фамилию как Napeir, Nepair, Nepeir, Napare, Naper, Naipper и чаще всего Neper, и *никогда* не пользовались современной английской орфографией Napier.

В качестве хронологического курьеза отметим, что теологические сочинения Непера чрезвычайно близки по стилистике и типу используемой аргументации историческим трудам школы Фоменко. Например, в них на основе статистических данных производятся абсолютно точные вычисления даты Судного Дня. Скорее всего, более точный анализ текстов позволит установить, что в действительности Непер и Носовский — это один и тот же исторический персонаж.

Понятие гомоморфизма было явным образом введено Капелли под названием **обобщенный изоморфизм**, сам термин **гомоморфизм** предложен Клейном.

Отметим несколько специальных случаев гомоморфизмов, которые имеют отдельное название (впрочем, не обязательно запоминать их все сразу). Гомоморфизм f называется:

• **мономорфизмом**, если f инъективен, (первая часть этого слова нам уже знакома, это '$\mu\grave{o}\nu o\varsigma$' — **единственный**); /

• **эпиморфизмом**, если f сюръективен, (от греческого '$\grave{\varepsilon}\pi\grave{\imath}$' — **на**); /

• **изоморфизмом**, если f биективен, /

• **эндоморфизмом**, если $G = H$, (от греческого '$\grave{\varepsilon}\nu\delta o\nu$' — **внутрь**); /

• **автоморфизмом**, если $G = H$, а f биективен (от греческого '$\alpha\grave{\upsilon}\tau\grave{o}\varsigma$' — **сам**, в том же значении, что немецкое selbst: **сам по себе**, **для себя самого**, etc.). /

Таким образом, изоморфизм — это такой гомоморфизм, который является одновременно мономорфизмом и эпиморфизмом; эндоморфизм

— это гомоморфизм группы в себя, а автоморфизм – это изоморфизм группы на себя.

Множество всех гомоморфизмов из группы G в группу H обозначается через $\mathrm{Hom}(G,H)$ или, реже, через $\mathrm{Mor}(G,H)$. Таким образом, запись $f \in \mathrm{Hom}(G,H)$ означает, что f — гомоморфизм из G в H. Множество всех изоморфизмов из G в H будет обозначаться через $\mathrm{Iso}(G,H)$. Через $\mathrm{End}(G)$ обозначается множество всех эндоморфизмов группы G в себя, а через $\mathrm{Aut}(G)$ — множество всех автоморфизмов G на себя. Композиция отображений превращает $\mathrm{End}(G)$ в моноид, а $\mathrm{Aut}(G)$ в группу и в дальнейшем мы изучим эти структуры и их связь со строением группы G.

Комментарий (исторический). Тех, кто хочет ознакомиться с работами классиков, стоит предостеречь, что следуя Жордану в XIX веке изоморфизмами называли *эпиморфизмы*. См., например, [92], с.9–10 (оригинал опубликован в 1882 году). То, что мы называем просто **изоморфизмом**, при этом называлось **голоэдрическим изоморфизмом** (isomorphisme holoédrique, einstufiger Isomorphismus, holohedral isomorphism). С другой стороны, **эпиморфизмы**, не являющиеся изоморфизмами, назывались **мероэдрическими* изоморфизмами** (isomorphisme meriédrique, mehrstufiger Isomorphismus, merohedral isomorphism). В 1896 году Бернсайд говорит о **простых изоморфизмах** (simple isomorphisms) и **кратных изоморфизмах** (multiple isomorphisms). Однако уже в 1904 году де Сегье пользовался современной терминологией **[344]**.

Мы потребовали, чтобы f сохранял произведение, но на самом деле тогда он сохраняет всю структуру группы. В следующей лемме мы обозначаем единичные элементы в обеих группах через e, вместо педантичных e_G и e_H.

Лемма. *Пусть $f : G \longrightarrow H$ — гомоморфизм групп. Тогда $f(e) = e$ и для любого $x \in G$ имеем $f(x^{-1}) = f(x)^{-1}$.*

Доказательство. В самом деле, $f(e)^2 = f(e^2) = f(e) = f(e)e$. Сокращая это равенство на $f(e)$, получаем первое утверждение леммы. Пусть теперь $x \in G$. По определению гомоморфизма и уже доказанному $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e$, что и завершает доказательство.

В действительности гомоморфизм можно определять и как отображение, сохраняющее операцию правого деления, т. е. посредством тождества $f(xy^{-1}) = f(x)f(y)^{-1}$.

2. Изоморфность. Группы H и G называются **изоморфными**, если между ними можно установить изоморфизм, в этом случае пишут $H \cong G$. С точки зрения алгебры изоморфные объекты устроены одинаково и на определенном этапе своего развития алгебра как

*Вариант: **мериэдрическими**.

раз и понималась как изучение алгебраических систем **с точностью до изоморфизма***. Вот несколько очевидных изоморфизмов, которые подробнее обсуждаются в следующем параграфе: $\mathbb{R}_{>0} \cong \mathbb{R}^+$, $\mathbb{C}^+ \cong (\mathbb{R}^+)^2$, $\mathbb{C}^* \cong \mathbb{T} \times \mathbb{R}_{>0}$, $\mathbb{Z}/m\mathbb{Z} \cong \mu_n$. Однако в действительности понятие изоморфности является *чрезвычайно* тонким. Так, например, можно показать (это будет сделано в книге IV), что $\mathbb{C}^* \cong \mathbb{T}$, хотя этот изоморфизм отнюдь не очевиден.

В своей книге Бернсайд приводит 8 примеров групп, которые на первый взгляд задаются совершенно различным образом, но при этом все изоморфны S_3. Вот его примеры III, IV и V (§ 17, pp.17–19).

Задача. Убедитесь, что в каждом из приведенных трех случаев перечисленные замены переменных образуют группу относительно композиции. Проверьте, что все эти группы изоморфны S_3.

• 6 рациональных замен одной переменной:

$$x \mapsto x,\ x \mapsto \frac{1}{x},\ x \mapsto 1-x,\ x \mapsto \frac{x}{x-1},\ x \mapsto \frac{x-1}{x},\ x \mapsto \frac{1}{1-x};$$

• 6 полиномиальных замен двух переменных:

$$(x,y) \mapsto (x,y),\ (x,y) \mapsto (y,x),\ (x,y) \mapsto (\omega x, \omega^2 y),$$
$$(x,y) \mapsto (\omega^2 x, \omega y),\ (x,y) \mapsto (\omega y, \omega^2 x),\ (x,y) \mapsto (\omega y, \omega^2 x);$$

• 6 полиномиальных замен одной переменной по модулю 3:

$$x \mapsto x,\ x \mapsto -x,\ x \mapsto x+1,\ x \mapsto x-1,\ x \mapsto -x+1,\ x \mapsto -x-1.$$

Приведенный только что пример — типичная ситуация того, как конечные группы проникают в геометрию, комплексный анализ, алгебраическую геометрию, теорию дифференциальных уравнений и т. д. Вот еще два примера. В Главе 1 мы уже упоминали, что имеется ровно 2 неизоморфных неабелевых группы порядка 8, а именно, D_4 и Q.

---

*В этом месте Роберт Шмидт обычно спрашивает: с точностью до *какого* изоморфизма. Он настаивает на конструкции **с точностью до изоморфности**. Я может и постарался бы **сгруппироваться** и выговорить нескладное слово **изоморфность**, но по-английски говорится `up to an isomorphism`, по-немецки `bis auf einem Isomorphismus`, по-французски `à un isomorphisme près`, по-итальянски `a meno di un isomorfismo`, по-испански `a menos de un isomorfismo`, по-японски ... — или пока достаточно?

Задача. Пусть z комплексная переменная. Докажите, что следующие 8 замен переменных образуют группу:

$$z \mapsto \pm z,\ z \mapsto \pm\frac{1}{z},\ z \mapsto \pm\overline{z},\ x \mapsto \pm\frac{1}{\overline{z}}.$$

Что это за группа?

Задача. Рассмотрим кривую рода 2, заданную уравнением $y^2 = x^5 - x$. Докажите, что следующие 8 бирациональных преобразований образуют группу:

$$(x,y) \mapsto (x, \pm y),\ (x,y) \mapsto (-x, \pm iy),$$
$$(x,y) \mapsto (-\frac{1}{x}, \pm\frac{y}{x^3}),\ (x,y) \mapsto (\frac{1}{x}, \pm\frac{iy}{x^3}).$$

Что это за группа?

Задача. Докажите, что $\mathbb{Q}^*_{>0} \cong \mathbb{Z}[x]^+$.

Упражнение. Убедитесь, что Вы только что доказали основную теорему арифметики целых чисел.

Задача. Докажите, что $\mathbb{Q}^*_{>0} \ncong \mathbb{Q}^+$.

Решение. В $\mathbb{Q}^+$ есть квадратные корни, а в $\mathbb{Q}^*_{>0}$ нет $\sqrt{2}$.

Следующий пример возникает в школьной тригонометрии. Рассмотрим группу, порожденную трансляциями и сменой знака аргумента. Нас интересует действие этой группы на пространстве функций с периодом 2π. Ясно, что трансляция $x \mapsto x + 2\pi$ задает на этом пространстве *тождественный* сдвиг. Сейчас мы рассмотрим подгруппу, переставляющую функции $\pm\cos$, $\pm\sin$.

Задача. Убедитесь, что относительно композиции преобразования функций с периодом 2π, задаваемые на аргументах посредством $x \mapsto \pi/2 \pm x$, $x \mapsto \pi \pm x$, $x \mapsto 3\pi/2 \pm x$, $x \mapsto 2\pi \pm x$, образуют группу. Что это за группа?

Задача. Пусть $H, G \leq \mathbb{Q}$, а $\varphi : H \longrightarrow G$ — изоморфизм. Тогда найдется $a \in \mathbb{Q}$ такое, что $\varphi(h) = ah$ для всех $h \in H$.

3. Классы сопряженных гомоморфизмов. В теории представлений, а также в некоторых разделах алгебраической топологии и комбинаторики в качестве морфизмов в категории групп рассматриваются не сами гомоморфизмы, а *классы* сопряженных гоморфизмов. А именно, если $\varphi : H \longrightarrow G$ — гомоморфизм, то гомоморфизмом, **сопряженным к φ при помощи** $g \in G$ называется гомоморфизм ${}^g\varphi = g\varphi g^{-1}$ определяемый как ${}^g\varphi(x) = g\varphi(x)g^{-1}$. Мы говорим, что два гомоморфизма $\varphi, \psi : H \longrightarrow G$ **сопряжены** и пишем $\varphi \sim \psi$, если найдется такое $g \in G$, что $\psi = {}^g\psi$.

Упражнение. Как вы думаете, почему в этом определении фигурирует только сопряжение в G, но не сопряжение в H?

Упражнение. Убедитесь, что если $\varphi_1 \sim \varphi_2$, $\psi_1 \sim \psi_2$, то $\varphi_1 \circ \psi_1 \sim \varphi_2 \circ \psi_2$.

§ 2♢. Первые примеры гомоморфизмов

Приведем несколько очевидных примеров гомоморфизмов.

• **Экспонента и логарифм.** Совершенно удивительное свойство вещественных чисел состоит в том, что относительно сложения и умножения они устроены почти совершенно одинаково. Точнее, экспонента и логарифм задают взаимно обратные изоморфизмы между аддитивной группой $\mathbb{R}^+$ и мультипликативной группой $\mathbb{R}^*$ положительных вещественных чисел. В самом деле, пусть exp и log обозначают экспоненту и натуральный логарифм:

$$\begin{aligned} &\exp : \mathbb{R}^+ \longrightarrow \mathbb{R}_{>0}, \qquad && x \mapsto e^x, \\ &\log : \mathbb{R}_{>0} \longrightarrow \mathbb{R}^+, \qquad && x \mapsto \log_e(x). \end{aligned}$$

Тогда, как хорошо известно, $\exp(x+y) = \exp(x)\exp(y)$, так что экспонента является гомоморфизмом аддитивной структуры в мультипликативную, и $\log(xy) = \log(x) + \log(y)$, так что и log является гомоморфизмом, на сей раз мультипликативной структуры в аддитивную. При этом $\exp(\log(x)) = x$ и $\log(\exp(x)) = x$, так что exp и log взаимно обратны. Так как складывать числа обычно гораздо легче, чем умножать, в докомпьютерную эру эти изоморфизмы широко использовались для практических приближенных вычислений физиками и инженерами ("таблицы логарифмов", "логарифмические линейки"). Заметим, что вообще, для любого $a > 0$ имеет место равенство $a^{x+y} = a^x a^y$, а если, кроме того, $a \neq 1$, то $\log_a(x+y) = \log_a(x) + \log_a(y)$. Таким образом, $\mathbb{R}^+ \longrightarrow \mathbb{R}^*$, $x \mapsto a^x$, и $\mathbb{R}_{>0} \longrightarrow \mathbb{R}^+$, $x \mapsto \log_a(x)$, являются гомоморфизмами между аддитивной и мультипликативной структурами $\mathbb{R}$. Как мы вскоре увидим, никаких других таких *непрерывных* гомоморфизмов нет.

• **Знак и абсолютная величина.** Отображение $|\ | : \mathbb{R}^* \longrightarrow \mathbb{R}_{>0}$, $x \mapsto |x|$, сопоставляющее вещественному числу его абсолютную величину, является эпиморфизмом мультипликативной группы ненулевых вещественных чисел на группу положительных вещественных чисел. Отображение $\operatorname{sign} : \mathbb{R}^* \longrightarrow \{\pm 1\}$, сопоставляющее вещественному числу его знак, $\operatorname{sign}(x)$ является эпиморфизмом $\mathbb{R}^*$ на группу $\{\pm 1\}$. В самом деле, эти отображение сюръективны, $|xy| = |x||y|$ и $\operatorname{sign}(xy) = \operatorname{sign}(x)\operatorname{sign}(y)$.

• **Модуль и аргумент.** То же самое можно сказать вообще про модуль и аргумент комплексного числа: $|\ |:\mathbb{C}^*\longrightarrow\mathbb{R}_{>0}$ и $\arg:\mathbb{C}^*\longrightarrow\mathbb{T}$. При этом снова $|zw|=|z||w|$ и $\arg(zw)=\arg(z)+\arg(w)$.

• **Знак перестановки.** Следующий пример подробно рассматривается в главе 5. Каждой перестановке π сопоставляется знак $\operatorname{sgn}(\pi)$, задающий гомоморфизм $\operatorname{sgn}:S_n\longrightarrow\{\pm1\}$. Иными словами знак произведения равен произведению знаков: $\operatorname{sgn}(\sigma\pi)=\operatorname{sgn}(\sigma)\operatorname{sgn}(\pi)$.

• **Определитель.** В книге IV построен гомоморфизм

$$\det:\mathrm{GL}(n,R)\longrightarrow R^*$$

из группы квадратных обратимых матриц $\mathrm{GL}(n,R)$ степени n над **коммутативным** кольцом R в группу R^* обратимых элементов кольца R, сопоставляющий матрице x ее определитель $\det(x)$. Ключевое свойство, которое, собственно, и оправдывает введение этого понятия, состоит в том, что определитель произведения равен произведению определителей: $\det(xy)=\det(x)\det(y)$.

• **p-адический показатель.** Пусть $G=\mathbb{Q}^*$ – мультипликативная группа рациональных чисел. Зафиксируем простое число $p\in\mathbb{P}$ и зададим отображение v_p группы $\mathbb{Q}^*$ в аддитивную группу $\mathbb{Z}^+$ целых чисел (в дальнейшем обозначаемую просто через $\mathbb{Z}$) следующим образом. Заметим, что каждое рациональное число $x\in\mathbb{Q}^*$ единственным образом представляется в виде $x=p^am/n$, где $a\in\mathbb{Z}$, а m и n взаимно просты с p, и положим $v_p(x)=a$. Так построенное отображение $v_p:\mathbb{Q}^*\longrightarrow\mathbb{Z}$ называется **p-адическим показателем**. Легко видеть, что v_p обладает свойством логарифма, т. е. является гомоморфизмом мультипликативной структуры $\mathbb{Q}^*$ в аддитивную структуру $\mathbb{Z}$, а именно, $v_p(xy)=v_p(x)+v_p(y)$.

• **p-адическое нормирование.** Скомпоновав p-адический показатель с каким-либо гомоморфизмом, переводящим аддитивную структуру в мультипликативную, например, с обычной экспонентой с рациональным основанием из $\mathbb{Q}_+$, мы получим гомоморфизм мультипликативных групп. Обычно в качестве основания здесь выбирают $1/p$, так что $|x|_p=p^{-v_p(x)}$. Так построенное отображение $|\ |_p:\mathbb{Q}^*\longrightarrow\mathbb{Q}_+^*$ называется **p-адическим нормированием**. Ясно, что $|xy|_p=|x|_p|y|_p$.

Отступление. Легко проверить, что p-адическое нормирование обладает всеми обычными свойствами абсолютной величины (например, оно удовлетворяет **неравенству треугольника** $|x+y|_p\le|x|_p+|y|_p$ — а, в действительности, гораздо более замечательному **ультраметрическому неравенству** $|x+y|_p\le\max(|x|_p,|y|_p)$). Таким образом,

$|\ |_p$ задает на $\mathbb{Q}$ метрику $d_p(x,y) = |x-y|_p$, называемую **p-адической метрикой**. Допределим $|\ |_p$ до гомоморфизма мультипликативных **моноидов** $\mathbb{Q} \longrightarrow \mathbb{Q}_+$ полагая $|0|_p = 0$). Пополнив $\mathbb{Q}$ относительно этой метрики, мы получаем поле $\mathbb{Q}_p$, называемое **полем p-адических чисел**, в котором можно развить аналог обычного вещественного анализа, называемый **p-адическим анализом**, играющий основную роль во многих разделах математики, особенно в теории чисел и алгебраической геометрии. В последнее время она все чаще используется в функциональном анализе и математической физике.

§ 3♢. Гомоморфизмы, связанные со структурой группы

Сейчас мы приведем несколько примеров гомоморфизмов, естественно возникающих в любой группе.

1. Гомоморфизмы, имеющиеся в абелевой группе. В следующих примерах существенно, что группа G абелева.

• **Обращение в абелевой группе.** Пусть G аддитивно записанная абелева группа. Отображение $\mathrm{inv} : G \longrightarrow G$, переводящее элемент g в противоположный, является автоморфизмом этой группы. В общем случае это будет изоморфизм группы G на **противоположную группу** G^o.

• **Возведение в степень в абелевой группе.** Зафиксируем $n \in \mathbb{Z}$ и рассмотрим отображение $\mathrm{pow}_n : G \longrightarrow G$, $g \mapsto g^n$. В случае, когда группа G абелева, это отображение является гомоморфизмом, т. е. $(hg)^n = h^n g^n$. В общем случае это, конечно, не обязательно так. Заметим, что если абелева группа G *конечна*, а n взаимно просто с $|G|$, то гомоморфизм $g \mapsto g^n$ является даже автоморфизмом (почему?).

Задача. Обратно, покажите, что если pow_2 гомоморфизм, то группа G абелева. Верно ли то же самое для pow_n, $n \geq 3$?

Следующая задача разбирается в [185] в качестве первого шага при вычислении количества **кольцевых** гомоморфизмов $\mathbb{Z}/m\mathbb{Z}$ в $\mathbb{Z}/n\mathbb{Z}$, где ответ уже не столь очевиден.

Задача. Докажите, что количество групповых гомоморфизмов C_m в C_n равно $\gcd(m,n)$.

Предположение следующей задачи автоматически выполнено для всех $n \in \mathbb{Z}$ в случае, когда G абелева группа.

Задача (Цассенхауз). Предположим, что G — группа такая, что для некоторого $n \in \mathbb{N}$ и всех $x, y \in G$ имеет место равенство $(xy)^n = x^n y^n$. Обозначим через $G^n = \{x^n \mid x \in G\}$ подмножество всех n-х степеней в

G, а через $G_n = \{x \in G \mid x^n = 1\}$ — множество всех элементов из G, порядок которых делит n. Показать, что $G^n, G_n \trianglelefteq G$ и $|G^n| = |G : G_n|$.

Решение. В предположениях теоремы pow_n эндоморфизм группы G, $G^n = \mathrm{Im}(\mathrm{pow}_n)$, $G_n = \mathrm{Ker}(\mathrm{pow}_n)$, так что $G^n, G_n \leq G$, причем G_n нормальна. Так как pow_n коммутирует с внутренними автоморфизмами I_g, $g \in G$, $gx^ng^{-1} = (gxg^{-1})^n$, то G^n тоже нормальна. Утверждение об индексе — это частный случай теоремы о гомоморфизме $G^n \cong G/G_n$.

2. Гомоморфизмы в абелеву группу. Предположим, что группа H абелева и рассмотрим гомоморфизмы $\varphi, \psi \in \mathrm{Hom}(G, H)$. Определим $\varphi\psi \in \mathrm{Hom}(G, H)$ обычной формулой $(\varphi\psi)(x) = \varphi(x)\psi(x)$. Убедитесь, что эта операция превращает $\mathrm{Hom}(G, H)$ в абелеву группу. В случае, когда H записывается аддитивно, операция в $\mathrm{Hom}(G, H)$ тоже записывается аддитивно, т.к. $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$.

3. Антигомоморфизмы. Пусть G — группа, а $\mathrm{inv} : G \longrightarrow G$ — отображение, переводящее каждый элемент $g \in G$ в обратный ему g^{-1}, т. е. $\mathrm{inv}(g) = g^{-1}$. Тогда inv является **антиавтоморфизмом** группы G, т. е. изоморфизмом G на противоположную группу G^o, называемым **обращением**. Так как для абелевой группы $G^o = G$, то **в абелевом случае** $\mathrm{inv} = \mathrm{pow}_{-1}$ является автоморфизмом. Вообще, отображение $f : G \longrightarrow H$ одной группы в другую называется **антигомоморфизмом**, если для любых $x, y \in G$ выполняется $f(xy) = f(y)f(x)$. Иными словами, f — гомоморфизм G в группу, противоположную H. Композиция двух антигомоморфизмов является антигомоморфизмом. В частности, композиция двух антиавтоморфизмов является антиавтоморфизмом.

Пусть, например, $G = \mathrm{GL}(n, R)$ — полная линейная группа над коммутативным кольцом R. Тогда, как хорошо известно, **транспонирование** $x \mapsto x^t$, сопоставляющее каждой матрице $x \in G$ транспонированную к ней является антиавтоморфзмом группы G, т. е. $(xy)^t = y^t x^t$ (то, что кольцо R коммутативно здесь существенно!). Таким образом, композиция обращения и транспонирования является автоморфизмом группы $G = \mathrm{GL}(n, R)$, называемым **контраградиентом**: $x \mapsto x^* = (x^t)^{-1}$. В самом деле, легко видеть, что $(xy)^* = x^*y^*$.

4. Гомоморфизмы, возникающие в произвольной группе. Следующие два примера наличествуют в произвольных группах, но второй из них интересен только только если групп а неабелева.

• Пусть H, G — две любые группы. Тогда отображение $1 : H \longrightarrow G$, переводящее все элементы группы H в единицу группы G является гомоморфизмом, который называется **тривиальным**.

Задача. Покажите, что если H и G конечные группы взаимно простых порядков, то $\mathrm{Hom}(H,G)=\{1\}$.

• Пусть G — любая группа. Тогда $\mathrm{id}: G\longrightarrow G$ является автоморфизмом группы G, называется **тождественным**.

• **Степени элемента.** / Легко видеть, что при фиксированном g отображение $\mathbb{Z}\longrightarrow G$, $n\mapsto g^n$, задает гомоморфизм аддитивной группы $\mathbb{Z}$ в G, иными словами, $g^{m+n}=g^mg^n$. Это значит, что для любого $g\in G$ существует единственный гомоморфизм $\mathbb{Z}\longrightarrow G$ такой, что $\varphi(1)=g$. Иными словами, $G\longleftrightarrow\mathrm{Hom}(\mathbb{Z},G)$.

• **Внутренние автоморфизмы.** / Пусть G — любая группа и $g\in G$. Зададим для всех $x\in G$ их образ под действием отображения $I_g: G\longrightarrow G$ равенством $I_g(x)=gxg^{-1}$ (элемент gxg^{-1} часто обозначается также ${}^gx$ и называется сопряженным к x под действием g). Из ассоциативности умножения и свойств обратного элемента сразу вытекает, что I_g — гомоморфизм. В самом деле, для любых $x,y\in G$ имеем $I_g(xy)=g(xy)g^{-1}=(gxg^{-1})(gyg^{-1})=I_g(x)I_g(y)$. Теперь из возможности сокращения в группе вытекает, что в действительности I_g является автоморфизмом. Автоморфизмы вида I_g называются **внутренними автоморфизмами** группы G. Обозначение I_g как раз и связано со словом `inner` — **`внутренний`**.

Задача. Пусть $h,g\in G$. Определим отображение $I_{g+h}: G\longrightarrow G$, полагая

$$I_{h+g}(x)={}^{h+g}x={}^h({}^gx)=hxh^{-1}gxg^{-1}.$$

При каком условии это отображение будет эндоморфизмом группы G? Автоморфизмом этой группы?

Задача. Верно ли, что $I_{h+g}=I_{g+h}$?

Задача. Докажите, что $I_{f(g+h)}=I_{fg+fh}$ и $I_{(f+g)h}=I_{fh+gh}$.

• **Автоморфизмы индуцированные на нормальной подгруппе.** Пусть G — любая группа, а $H\leq G$ — ее нормальная подгруппа. Тогда сопряжение при помощи любого $g\in N_G(H)$ оставляет H на месте и, следовательно, индуцирует автоморфизм $I_g|_H$ группы H. Важно обратить внимание, что с точки зрения самой группы H этот автоморфизм уже совсем не обязан быть внутренним! Особенно важен случай, когда $H\trianglelefteq G$, так что вообще любой элемент группы G индуцирует некоторый автоморфизм группы H.

В действительности, в главе 6 мы убедимся, что любую группу H можно вложить в группу $\mathrm{Hol}(H)$, называемую **голоморфом** группы

H таким образом, что $H \trianglelefteq \mathrm{Hol}(H)$ и **все** автоморфизмы группы H становятся в $\mathrm{Hol}(H)$ внутренними.

Задача. При каком условии любой автоморфизм $I_g|_H$, $g \in N_G(H)$, является внутренним автоморфизмом группы H?

Ответ. Для этого необходимо и достаточно, чтобы имело место равенство $N_G(H) = HC_G(H)$.

5. Группы с одним или двумя автоморфизмами. Следующая задача предполагает знакомство с векторными пространствами (а при чем здесь векторные пространства?). Она замечательно иллюстрирует принцип **кумуляции*** трудностей. В ее решении использованы три идеи, каждая из которых в отдельности абсолютно тривиальна. Однако собранные вместе и вырванные из контекста они могли бы стать почти непреодолимым препятствием для начинающего.

Задача. Доказать, что любая группа, содержащая по крайней мере 3 элемента, имеет нетривиальные автоморфизмы.

Решение. Вот эти три идеи.

• Если G неабелева, то у нее есть нетривиальный внутренний автоморфизм.

• Если G абелева, то inv является автоморфизмом, который нетривиален в том и только том случае, когда найдется элемент g такой, что $2g \neq 0$.

• Таким образом, мы можем считать, что группа G обладает свойством $2g = 0$ для всех $g \in G$ и, значит, является векторным пространством над полем $\mathbb{F}_2$ из двух элементов. В векторном пространстве можно выбрать базис X (аксиома выбора!), а так как $|G| \geq 3$, то $|X| \geq 2$ и, значит X допускает нетривиальные биекции на себя. Любая такая биекция однозначно продолжается по линейности до автоморфизма G.

Задача. Доказать, что единственными группами, у которых ровно два автоморфизма, являются циклические группы порядков 3,4 и 6.

§ 4♢. Образ и ядро гомоморфизма

*Кумуляция — концентрация огромной энергии в небольшом объеме за счет синхронного действия нескольких факторов. Совсем не то же самое, что **аккумуляция**, которая не предполагает одновременности. Кумулятивный эффект нескольких незначительных причин может ужасающим образом отличаться от их совокупного (аккумулятивного) эффекта.

В настоящем параграфе мы построим две важнейшие подгруппы, связанные с гомоморфизмом.

1. Образ гомоморфизма. Пусть $\varphi : H \longrightarrow G$ — гомоморфизм групп. Тогда **образ** φ — это обычный образ φ как отображения. Тем самым,

$$\mathrm{Im}(\varphi) = \{y \in G \mid \exists x \in H, \varphi(x) = y\}.$$

Легко видеть, что $\varphi(H)$ — подгруппа в G. В самом деле, $1 = \varphi(1) \in \mathrm{Im}(\varphi)$. Если $y, z \in \mathrm{Im}(\varphi)$, то существуют $x, u \in H$ такие, что $\varphi(x) = y$, $\varphi(u) = z$. Тогда $\varphi(xu) = \varphi(x)\varphi(u) = yz$, так что $yz \in \mathrm{Im}(\varphi)$. Аналогично, $\varphi(x^{-1}) = \varphi(x)^{-1} = y^{-1}$, так что $y^{-1} \in \mathrm{Im}(\varphi)$. Ясно однако, что ядро не обязано быть нормальной подгруппой. В самом деле, рассмотрим *произвольную* подгруппу H группы G. Тогда H является образом канонического вложения $H \hookrightarrow G$.

2. Ядро гомоморфизма. Свяжем теперь с гомоморфизмом φ некоторую подгруппу в H.

Определение. Ядром *гомоморфизма φ называется полный прообраз* 1 *при этом гомоморфизме:*

$$\mathrm{Ker}(\varphi) = \{x \in H \mid \varphi(x) = 1\}.$$

Сейчас мы покажем, что в отличие от образа, ядро всегда является *нормальной* подгруппой в H.

Предложение. *Для любого гомоморфизма $\varphi : H \longrightarrow G$ имеем*

$$\mathrm{Ker}(\varphi) \trianglelefteq H.$$

Доказательство. Докажем вначале, что G является подгруппой. В самом деле, $\varphi(1) = 1$, так что $1 \in \mathrm{Ker}(\varphi)$. Если $x, y \in \mathrm{Ker}(\varphi)$, то $\varphi(xy) = \varphi(x)\varphi(y) = 1 \cdot 1 = 1$, так что $xy \in \mathrm{Ker}(\varphi)$. Наконец, если $x \in \mathrm{Ker}(\varphi)$, то $\varphi(x^{-1}) = \varphi(x)^{-1} = 1^{-1} = 1$, так что $x^{-1} \in \mathrm{Ker}(\varphi)$. Это и значит, что $\mathrm{Ker}(\varphi) \leq H$.

С другой стороны, если $x \in \mathrm{Ker}(\varphi)$, а $y \in H$, то

$$\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y^{-1}) = \varphi(y)\varphi(y)^{-1} = 1.$$

Это и значит, что $\mathrm{Ker}(\varphi) \trianglelefteq H$.

Легко видеть, что верно и обратное: любая нормальная подгруппа является ядром некоторого гомоморфизма. А именно, с каждым нормальным делителем $H \trianglelefteq G$ связана каноническая проекция $\pi_H : G \longrightarrow$

G/H, $g \mapsto gH$. Ясно, что $H = \mathrm{Ker}(\pi_H)$. Таким образом, класс ядер гомоморфизмов совпадает с классом нормальных подгрупп.

Напомним, что **уравнителем** (эквалайзером) двух отображений $f, g : X \longrightarrow Y$ называется множество $\mathrm{Eq}(f,g) = \{x \in X \mid f(x) = g(x)\}$. По определению $\mathrm{Ker}(f) = \mathrm{Eq}(f, 1)$.

Задача. Рассмотрим гомоморфизм $f : H \longrightarrow G$.

• Докажите, что $f^{-1}(f(F)) = F\,\mathrm{Ker}(f)$ для любой подгруппы $F \leq H$;

• Докажите, что $f(f^{-1}(K)) = K \cap \mathrm{Im}(f)$ для любой подгруппы $K \leq G$.

Задача. Верно ли, что уравнитель $\mathrm{Eq}(f,g)$ двух любых гомоморфизмов $f, g : H \longrightarrow G$ всегда является подгруппой в G?

Значительно труднее доказать, что любая подгруппа является уравнителем. Доказательство этого факта опирается на существование амальгамированного произведения и мы сможем провести его только в главе 11.

3. Примеры ядер. Укажем ядра нескольких важнейших гомоморфизмов.

• Пусть $\mathrm{pow}_n : G \longrightarrow G$, $x \mapsto x^n$, — возведение в n-ю степень. Тогда $\mathrm{Ker}(\mathrm{pow}_n) = G_n$ — множество элементов в G периода n.

• Пусть $I : G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto I_g$, гомоморфизм, сопоставляющий каждому элементу $g \in G$ соответствующий внутренний автоморфизм I_g. Тогда $\mathrm{Ker}(I) = C(G)$ — центр группы G.

• Пусть $\mathrm{sgn} : S_n \longrightarrow S_n$ — знак перестановки, тогда $\mathrm{Ker}(\mathrm{sgn}) = A_n$ — знакопеременная группа.

• Пусть $\det : \mathrm{GL}(n,K) \longrightarrow K^*$ — определитель, тогда

$$\mathrm{Ker}(\det) = \mathrm{SL}(n,K)$$

— специальная линейная группа.

§ 5♢. Теорема о гомоморфизме

Сейчас мы покажем, что факторизация отображений замечательным образом согласована со структурой группы. Следующая теорема является одним из наиболее типичных и характерных результатов общей алгебры. В полной общности она была впервые сформулирована Эмми Нетер.

Теорема о гомоморфизме. *Пусть* $\varphi : H \longrightarrow G$ — *гомоморфизм групп. Тогда*

$$\operatorname{Im}(\varphi) \cong H/\operatorname{Ker}(\varphi).$$

Напоминание. Вспомним, что с *каждым* отображением $\varphi : H \longrightarrow G$ связано **ядро** $N(\varphi)$ отображения φ, т. е. разбиение H на слои отображения φ. Эти слои являются классами эквивалентности $\sim$ alias $\sim_\varphi$ определяемой условием

$$x \sim y \qquad \Longleftrightarrow \qquad \varphi(x) = \varphi(y).$$

Покажем, прежде всего, что в случае, когда φ является гомоморфизмом, слои являются в точности смежными классами по $\operatorname{Ker}(\varphi)$. Кстати, это объясняет, почему мы называем ядром гомоморфизма слой содержащий 1: в отличие от произвольных отображений для гомоморфизмов задание одного слоя однозначно определяет **все** остальные классы. В самом деле, если $\varphi(x) = \varphi(y)$, то $\varphi(xy^{-1}) = \varphi(x)\varphi(y)^{-1} = 1$ так что $xy^{-1} \in \operatorname{Ker}(\varphi)$. Но это и значит, что $x\operatorname{Ker}(\varphi) = y\operatorname{Ker}(\varphi)$ (вспомним, что ядро является нормальным делителем, так что безразлично, говорить о левых смежных классах или о правых). Обратно, если $x\operatorname{Ker}(\varphi) = y\operatorname{Ker}(\varphi)$, то $y = xh$ для некоторого $h \in \operatorname{Ker}(\varphi)$, так что $\varphi(y) = \varphi(xh) = \varphi(x)\varphi(h) = \varphi(x)$.

Доказательство. Мы можем применить к этой ситуации описанное выше соображение и заключить, что сопоставление

$$\overline{x} = x + \operatorname{Ker}(\varphi) \mapsto \varphi(x)$$

корректно определяет инъективное отображение $\overline{\varphi} : H/\operatorname{Ker}(\varphi) \longrightarrow G$, образ которого совпадает с $\operatorname{Im}(\varphi)$. Для завершения доказательства теоремы нам остается лишь проверить, что $\overline{\varphi}$ гомоморфизм. В самом деле, пользуясь определением произведения классов, определением $\overline{\varphi}$ и тем, что φ — гомоморфизм, получаем

$$\overline{\varphi}(\overline{x} \cdot \overline{y}) = \overline{\varphi}(\overline{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \overline{\varphi}(\overline{x})\overline{\varphi}(\overline{y}),$$

что и завершает доказательство.

Следствие. *Если* $\varphi : H \longrightarrow G$ *эпиморфизм, то* $G \cong H/\operatorname{Ker}(\varphi)$.

Теорема. *Пусть $f : G \longrightarrow G'$ — гомоморфизм групп, а нормальные подгруппы $H \trianglelefteq G$, $H' \trianglelefteq G'$ таковы, что $f(H) \leq H'$. Тогда f индуцирует гомоморфизм $\overline{f} : G/H \longrightarrow G'/H'$, $\overline{f}(xH) = f(x)H'$.*

Доказательство. Прежде всего, необходимо проверить корректность этого определения. Для этого заметим, что если $xH = yH$, то по условию на f имеем $f(x)^{-1}f(y) = f(x^{-1}y) \in H'$, так что $f(x)H' = f(y)H'$. Осталось убедиться в том, что $\overline{f}$ гомоморфизм. В самом деле,

$$\overline{f}(xH \cdot yH) = \overline{f}(xyH) = f(xy)H' = f(x)f(y)H' = (f(x)H')(f(y)H') = \overline{f}(xH)\overline{f}(yH).$$

Следствие. *Если в условиях теоремы $H = f^{-1}(H')$, то гомоморфизм $\overline{f} : G/H \longrightarrow G'/H'$ инъективен. Если, кроме того, f сюръективен, то $\overline{f}$ изоморфизм.*

Фактически некоторые примеры применения этой теоремы содержались в § 3, когда мы обсуждали примеры фактор-групп. Вот еще один типичный пример: $\mathrm{Inn}(G) = G/C(G)$.

§ 6♢. Теоремы об изоморфизме

> Митчерлих в 1819 году установил, что кристаллы четырех разных веществ: KH_2PO_4, KH_2AsO_4, $(NH_4)H_2PO_4$ и $(NH_4)H_2AsO_4$ имеют одну и ту же внешнюю форму и почти одинаковые углы между аналогичными гранями. Явление наличия у различных соединений одинакового внешнего огранения (габитуса) было названо им *изоморфизмом*. Геометрически нельзя отличить изоморфные кристаллы разных веществ, обладающие изогонизмом и отличающиеся лишь физическими свойствми. Изоморфизм широко распространен, как среди минералов, так и среди искусственно полученных химических соединений.
>
> Тадеуш Пенкаля. **[148]**, с. 248–249

В этом параграфе мы докажем несколько важнейших следствий теоремы о гомоморфизме, иллюстрирующих ее использование.

1. Noetherscher Isomorphiesatz. Сейчас мы докажем важнейший результат, обычно называемый в учебной литературе **первой теоремой об изоморфизме**. Впрочем, поскольку никто не может запомнить, которая из теорем об изоморфизме первая, а которая вторая, профессионалы чаще ссылаются на него как **теорему Нетер об изоморфизме**. В общем виде, для произвольных групп с операторами

этот результат был сформулирован в работе Эмми Нетер 1929 года. Впрочем, стоит отметить, что для конечных групп этот результат содержится уже в работе Гельдера 1889 года, а для абелевых групп — в приложении Дедекинда к изданию 1894 года лекций Дирихле по теории чисел. Но название `теорема Гельдера--Дедекинда--Нетер` для такого результата было бы слишком длинным и слишком помпезным.

Прежде всего заметим, что произведение по Минковскому FH произвольной подгруппы $F \leq G$ на нормальную подгруппу $H \trianglelefteq G$ является подгруппой в G. Этот факт уже обсуждался в § 2.8, но мы приведем другое доказательство. Пусть $\pi : G \longrightarrow G/H$ — каноническая проекция. Тогда $FH = \pi^{-1}(\pi(F)) = \cup fH$, $f \in F$. Как образ, так и прообраз подгруппы при гомоморфизме являются подгруппами.

Теорема (Noetherscher Isomorphiesatz). *Пусть $H \trianglelefteq G$ — нормальная подгруппа в группе G, а $F \leq G$ — произвольная подгруппа. Тогда $H \cap F \trianglelefteq F$ и имеет место изоморфизм*

$$F/F \cap H = FH/H.$$

Доказательство. Рассмотрим гомоморфизм

$$\varphi : F \longrightarrow FH \longrightarrow FH/H, \qquad f \mapsto fH,$$

являющийся композицией вложения и канонической проекции. Так как любой правый смежный класс FH по H представляется в виде $(fh)H = fH$ для некоторых $f \in F$, $h \in H$, гомоморфизм φ сюръективен. Ясно, что $f \in F$ в том и только том случае лежит в $\operatorname{Ker}(\varphi)$, когда $f \in H$. Таким образом $\operatorname{Ker}(\varphi) = F \cap H$, и для завершения доказательства осталось лишь сослаться на теорему о гомоморфизме.

Задача. Пусть $f : G \longrightarrow G'$ — гомоморфизм групп, $H \leq G$. Покажите, что

$$|G : H| = |\operatorname{Ker}(f) : \operatorname{Ker}(f|H)| \cdot |\operatorname{Im}(f) : \operatorname{Im}(f|H)|.$$

Указание. Если группа G конечна, то это просто теорема о гомоморфизме + теорема Лагранжа. В общем случае придется рассмотреть группу $F = H \operatorname{Ker}(f)$ и воспользоваться теоремой Нетер.

Следующая задача иллюстрирует типичное использование теоремы Нетер. В дальнейшем мы много раз столкнемся с этим соображением. Подгруппа $H \leq G$ называется **холловской**, если порядок $|H| = m$ подгруппы H взаимно прост с ее индексом $n = |G : H|$.

Задача. Докажите, что если $H \trianglelefteq G$ — холловский нормальный делитель группы G, то H является *единственной* подгруппой в G порядка m.

Решение. Пусть $F \leq G$ — другая подгруппа порядка m. Тогда $|FH/H|$ делит $|G : H| = n$, а $|F : F \cap H|$ делит $|F| = m$. Но ведь из теоремы об изоморфизме следует, что $|FH/H| = |F : F \cap H|$. Тем самым $FH = H$ и, значит, $F \leq H$.

2. Вторая теорема об изоморфизме. Пусть $F \trianglelefteq G$. Из теоремы о гомоморфизме вытекает, что сопоставление $H \mapsto H/F$ определяет изоморфизм решетки $L(G, F)$ **промежуточных подгрупп** H, $F \leq H \leq G$, с решеткой $L(G/F, 1)$ **всех** подгрупп в фактор-группе G/F. Оказывается, при этом соответствии нормальным подгруппам отвечают нормальные подгруппы.

Лемма. *Пусть $F \leq H \leq G$, причем $F \trianglelefteq G$. Тогда $H \trianglelefteq G$ в том и только том случае, когда $H/F \trianglelefteq G/F$.*

Доказательство. Возьмем произвольные элементы $gF \in G/F$ и $hF \in H/F$, где $g \in G$ и $h \in F$ соответственно. Так как F нормальна в G, то

$$(gF)^{-1}(hF)(gF) = (g^{-1}hg)F.$$

Ясно, что этот класс в том и только том случае попадает в H/F, когда $g^{-1}hg \in H$.

Следующая теорема иногда называется **теоремой фон Дика**. В действительности, в работе 1882 года фон Дик [186] формулировал нечто, что сейчас истолковывается как частный случай этой теоремы, относящийся к ситуации, когда G свободная группа. Общий случай явно сформулирован де Сегье в его учебнике 1904 года, [**344**], с. 65.

Теорема. *Пусть $F, H \trianglelefteq G$ — нормальные подгруппы в G, причем $F \leq H$. Тогда имеет место канонический изоморфизм*

$$(G/F)/(H/F) \cong G/H.$$

Доказательство. Обозначим через $\pi : G \longrightarrow G/H$ каноническую проекцию. Так как $F \leq H = \mathrm{Ker}(\pi)$, π индукцирует гомоморфизм $\pi' : G/F \longrightarrow G/H$, $gF \mapsto gH$. Ядро этого гомоморфизма равно $\mathrm{Ker}(\pi)/F = H/F$. Осталось применить теорему о гомоморфизме.

3. Третья теорема об изоморфизме. Следующий результат описывает некоторые фактор-группы прямого произведения.

Вальтер фон Дик (Walther Franz Anton von Dyck, 6 декабря 1856, Мюнхен — 5 ноября 1934, ibid.) — выдающийся немецкий математик и общественный деятель. Основные математические работы фон Дика относятся к теории функций комплексного переменного, геометрии, топологии, теории групп и теории потенциала. Фон Дик (тогда еще просто Вальтер Дик!) учился в Мюнхене, Берлине и Лейпциге и в 1879 году получил докторат за диссертацию по римановым поверхностям, выполненную под руководством Клейна. После этого он на несколько лет последовал за Клейном в Лейпциг, где и написал свои знаменитые работы по теории групп. Однако в 1884 году фон Дик вернулся в Мюнхен профессором только что созданного Мюнхенского политехнического института — Technische Hochschule. В 1903–1906 и 1919–1925 годах он был ректором Technische Hochschule. Кроме того, Фон Дик был одним из создателей самого знаменитого Мюнхенского музея Deutsches Museum, а с 1906 года вторым директором этого музея! Среди прочих проектов, в которых он участвовал, было издание полного собрания трудов Кеплера.

Теорема. *Пусть $H_1 \trianglelefteq G_1$ и $H_2 \trianglelefteq G_2$. Тогда $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ и имеет место канонический изоморфизм*

$$G_1 \times G_2/H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2.$$

Доказательство. То, что $H_1 \times H_2 \trianglelefteq G_1 \times G_2$ – очевидно (операции в прямом произведении покомпонентные!) Зададим теперь отображение $\pi = \pi_1 \times \pi_2 : G_1 \times G_2 \longrightarrow G_1/H_1 \times G_2/H_2$, где $\pi_i : G_i \longrightarrow G_i/H_i$ – каноническая проекция на фактор-группу. Иными словами, мы полагаем $\pi(g_1, g_2) = (g_1H_1, g_2H_2)$. Прямое произведение гомоморфизмов является гомоморфизмом, причем, так как g_1 и g_2 независимы, π сюръективен. Вычислим $\mathrm{Ker}(\pi)$. Равенство $\pi(g_1, g_2) = (1, 1)$, означает в точности, что $g_1 \in H_1$ и $g_2 \in H_2$. Тем самым, $\mathrm{Ker}(\pi) = H_1 \times H_2$. Осталось сослаться на теорему о гомоморфизме.

В связи с этой теоремой уместно проиллюстрировать еще одно типичное применение взаимной простоты. Верно ли, что и обратно, любой нормальный делитель $H \trianglelefteq G_1 \times G_2$ имеет вид $H_1 \times H_2$? Ясно, что вообще говоря, это совершенно не так (приведите пример). Однако это всегда так для конечных групп взаимно простых порядков.

Задача. Пусть $|G_1| = m$, $|G_2| = n$, причем $\gcd(m, n) = 1$. Докажите, что тогда любая подгруппа $H \leq G_1 \times G_2$ имеет вид $H_1 \times H_2$ для некоторых $H_1 \leq G_1$ и $H_2 \leq G_2$.

Решение. В самом деле, пусть $(h, g) \in H$ для некоторых $h \in G_1$, $g \in G_2$. Тогда $(h, g)^m = (1, g^m) \in H$, а так как $m \perp n$, то найдется такое l, что $lm \equiv 1 \pmod{n}$, и, значит, $(1, g^m)^l = (1, g) \in H$.

§ 7♠. Категория групп

Кошку видали? Колыбельку видали?

Курт Воннегут—Маргарита Райт-Ковалева. *Колыбель для кошки*

Только теперь, когда мы определили *гомоморфизмы* групп, мы начинаем приближаться к пониманию того, что такое группа.

1. Категория групп. Определим **категорию групп** $\mathcal{G}r$, объектами которой являются группы, морфизмами — гомоморфизмы групп, а композиция морфизмов совпадает с их композицией как отображений. Эйленберг и Маклейн провозгласили, что целью теории групп является изучение категории групп $\mathcal{G}r$, в частности, ее подкатегорий, функторов из $\mathcal{G}r$ в $\mathcal{G}r$ или в другие категории и т. д. С категорией групп тесно связан ряд других категорий, которые тоже в той или иной форме обсуждаются в настоящей книге. Вот две полных подкатегории в $\mathcal{G}r$, которые мы используем особенно часто:

• **категория абелевых групп** $\mathcal{A}b$;

• **категория конечных групп** $\mathcal{F}in\mathcal{G}r$.

Кроме того, нам встречались другие категории, связанные с категорией групп, где морфизмами являются *не все* гомоморфизмы или *не совсем* гомоморфизмы:

• В главе 2 мы обсуждали **категорию виртуальных групп**, морфизмами которой являются *виртуальные гомоморфизмы*;

• В настоящей главе мы упомянули **категорию групп и сопряженных гомоморфизмов**, морфизмами которой являются *классы сопряженности* гомоморфизмов.

В Главе 1 мы уже обсуждали несколько категорий, состоящих из групп с дополнительными структурами:

• **категория топологических групп**: морфизмами это категории являются не любые гомоморфизмы, а только *непрерывные* гомоморфизмы;

• **категория групп Ли**: морфизмами это категории являются *аналитические* гомоморфизмы;

• **категория алгебраических групп**: морфизмами это категории являются *регулярные* гомоморфизмы.

Разумеется в математике встречается и много других похожих категорий: категория упорядоченных групп и т. д.

2. Перевод категорных понятий. Приведем краткий словарик, переводящий некоторые основные категорные понятия на привычный язык теории групп:

инициальный объект в $\mathcal{G}r$	1
терминальный объект в $\mathcal{G}r$	1
подобъект в $\mathcal{G}r$	подгруппа
ядро в $\mathcal{G}r$	нормальная подгруппа
фактор-объект в $\mathcal{G}r$	фактор-группа
произведение в $\mathcal{G}r$	прямое произведение
копроизведение в $\mathcal{G}r$	свободное произведение
копроизведение в $\mathcal{A}b$	прямая сумма

корасслоенная сумма в $\mathcal{G}r$	амальгамированное произведение
мономорфизм в $\mathcal{G}r$	инъективный гомоморфизм
эпиморфизм в $\mathcal{G}r$	сюръективный гомоморфизм
изоморфизм в $\mathcal{G}r$	биективный гомоморфизм

Заметим, что для эпиморфизмов эта эквивалентность совершенно не очевидна, она опирается на то, что каждая подгруппа может быть уравнителем, т. е. на существование амальгамированного произведения!

Задача. Постарайтесь понять, что все эти понятия значат с точки зрения других категорий, связанных с категорией групп. Например, что такое подобъект и фактор-объект в категории виртуальных групп или в категории групп и сопряженных гомоморфизмов?

Предостережение. Руководствуясь тем, что в категории групп эпиморфизмы совпадают с сюръективными гомоморфизмами, многие наивные писатели полагают, что и в других категориях алгебраических систем эпиморфизмы — это в точности то же самое, что сюръективные гомоморфизмы. Это действительно так для категории модулей R-$\mathcal{M}od$. Вот, однако, два контр-примера к этому утверждению в общем случае! Эти примеры известны из 2 и 3 класса начальной школы:

- в категории моноидов вложение $\mathbb{N} \hookrightarrow \mathbb{Z}$ является эпиморфизмом;
- в категории колец с 1 вложение $\mathbb{Z} \hookrightarrow \mathbb{Q}$ является эпиморфизмом.

Да что там говорить, если уже в категории *топологических* групп, эпиморфизмами являются вовсе не сюръективные, а **доминантные гомоморфизмы**, т. е. такие гомоморфизмы, $f : H \longrightarrow G$, что образ $f(H)$ плотен в G. Таким образом,

- в категории топологических групп вложение $\mathbb{Q}^+ \hookrightarrow \mathbb{R}^+$ является эпиморфизмом.

Эпиморфность этих трех *несюръективных* морфизмов широчайшим образом используется в математике! Например, именно на этом основано доказательство теоремы Коши о *непрерывных* эндоморфизмах $\mathbb{R}^+$.

Задача. Совпадает ли эпиморфность с сюръективностью в категории групп и сопряженных гомоморфизмов?

2. Некоторые функторы. Вот несколько очевидных примеров функторов из категории групп и/или в категорию групп. Начнем с четырех забывающих функторов.

- Забывающий функтор $\mathcal{G}r \longrightarrow \mathcal{S}et$ сопоставляет каждой группе подлежащее множество, забывая все элементы ее структуры.
- Однако гораздо естественнее рассматривать забывающий функтор $\mathcal{G}r \longrightarrow \mathcal{S}et_\bullet$, который забывает все, кроме того, что в множестве G есть выделенный элемент 1.
- Забывающий функтор $\mathcal{R}ing \longrightarrow \mathcal{A}b$, $R \quad R^+$, сопоставляющий кольцу его аддитивную группу.
- По существу такую же роль играет и функтор $\mathcal{R}ing \longrightarrow \mathcal{G}r$, $R \quad R^*$, сопоставляющий кольцу с 1 его мультипликативную группу.

А вот простейшие примеры функторов в самой категории групп.

- Коммутант $\mathcal{G}r \longrightarrow \mathcal{G}r$, $G \quad [G, G]$. Так как образ коммутатора под действием любого гомоморфизма есть снова коммутатор, то это действительно функтор.

• В главе 7 мы рассмотрим абелианизацию $\mathcal{G}r \longrightarrow \mathcal{A}b$, $G \quad G/[G,G]$.

4. Естественный изоморфизм. Одной из основ категорного мышления является акцент на *естественных* понятиях, в частности на *естественных* изоморфизмах, которые можно построить чисто категорно, не вникая в случайные обстоятельства происхождения рассматриваемых объектов. Например, в линейной алгебре мы обсуждаем, что *конечномерное* векторное пространство V над полем изоморфно — но не естественно изоморфно — своему двойственному пространству V^*, этот изоморфизм зависит от того *случайного* обстоятельства, что $\dim(V) = \dim(V^*)$ и, следовательно, между базисами V и V^* можно установить биекцию. В то же время V естественно изоморфно второму двойственному V^{**}, так как все выборы базиса в V приводят к одному и тому же изоморфизму.

В настоящий момент мы не находимся еще на уровне софистикации, который оправдывал бы систематическое обсуждение такого рода вопросов. Ограничусь поэтому одним маленьким примером. Действительно ли группы $\mathbb{Z}/n\mathbb{Z}$ и μ_n изоморфны? С элементарной точки зрения это так. Но с точки зрения человека, обладающего хотя бы рудиментарными сведениями в области теории чисел, алгебраической геометрии или алгебраических групп, группы $\mathbb{Z}/n\mathbb{Z}$ и μ_n весьма различны. Первая из них постоянна, а вторая — нет, на первой группа Галуа действует тривиально, на второй — нет, и т. д. Философ, который был бы в состоянии понять, о чем здесь идет речь, сказал бы, что изоморфизм групп $\mathbb{Z}/n\mathbb{Z}$ и μ_n в категории групп `акцидентален`, в то время как их различие во всех остальных смыслах `субстанциально`. Эти группы столь же отличаются друг от друга, как $\mathbb{Z}$ и $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$. В действительности группы $\mathbb{Z}/n\mathbb{Z}$ и μ_n как раз и находятся точно в таком же отношении, как $\mathbb{Z}$ и $\mathbb{T}$ — они **двойственны** друг другу.

§ 8♡. Характеристические и вполне характеристические подгруппы

Нормальная подгруппа $H \trianglelefteq G$ — это подгруппа, устойчивая под действием **внутренних** автоморфизмов. Сейчас мы усилим это понятие.

1. Характеристические подгруппы. Субнормальность является *ослаблением* понятия нормальности. Однако в настоящее время нас интересует вопрос, можно ли таким образом *усилить* понятие нормальности, чтобы все же быть в состоянии заключить, что F нормальна в G?

Определение. *Подгруппа $H \leq G$ называется* **характеристической**, *если $\varphi(H) \leq H$ для любого* **автоморфизма** $\varphi \in \mathrm{Aut}(G)$ *и* **вполне характеристической**, *если $\varphi(H) \leq H$ для любого* **эндоморфизма** $\varphi \in \mathrm{End}(G)$

Во многих старых книгах характеристические подгруппы называются **автоморфно допустимыми**, а вполне характеристические — **эндоморфно допустимыми**. По определению любая вполне харак-

теристическая подгруппа является характеристической, а любая характеристическая подгруппа — нормальной:

$$\text{вполне характеристическая} \Longrightarrow \text{характеристическая} \Longrightarrow \Longrightarrow \text{нормальная} \Longrightarrow \text{субнормальная}.$$

Легко убедиться в том, что все включения соответствующих классов подгрупп строгие, для последнего из них это уже было показано выше, вот два других примера.

• Центр $C(G)$ группы G является характеристической, но, вообще говоря, не вполне характеристической подгруппой;

• Подгруппы второго порядка группы $V = E_4$ являются нормальными, но не характеристическими.

Понятие характеристической подгруппы (`charakteristische Untergruppe`) было введено в 1895 году Фробениусом. Он называл нормальную подгруппу $F \trianglelefteq H$ характеристической, если она продолжает оставаться нормальной в любой группе G такой, что $H \trianglelefteq G$. Сейчас мы убедимся, что наше определение эквивалентно этому. Понятие вполне характеристической подгруппы (`vollinvariante Untergruppe`) ввел в 1933 году Ф. Леви при изучении подгрупп свободных групп.

Предложение. *Имеют место следующие импликации:*

• *Характеристическая подгруппа F нормальной подгруппы $H \trianglelefteq G$ нормальна в G.*

• *Характеристическая подгруппа F характеристической подгруппы $H \leq G$ является характеристической подгруппой в G.*

• *Пусть $F \leq H \leq G$, причем F характеристическая в G и H/F характеристическая в G/F. Тогда H является характеристической подгруппой в G.*

• *Вполне характеристическая подгруппа F вполне характеристической подгруппы $H \leq G$ является вполне характеристической подгруппой в G .*

Доказательство. Докажем для иллюстрации первую из них, доказательство двух других совершенно аналогично. Итак, пусть $H \trianglelefteq G$, а F — характеристическая подгруппа в H. Тогда для любого $g \in G$ ограничение I_g на H является автоморфизмом H и, следовательно, так как F характеристическая, то $I_g(F) \leq F$. Но это и значит, что $F \trianglelefteq G$.

2. Примеры характеристических подгрупп. Приведем несколько очевидных примеров характеристических подгрупп.

• Нормальная силовская p-подгруппа конечной группы G содержит все ее p-элементы и, следовательно, является характеристической — и даже вполне характеристической.

Этот пример легко обобщить. Подгруппа H конечной группы G называется **холловской**, если ее порядок и индекс взаимно просты, $|H| \perp |G:H|$.

Задача. Докажите, что любая нормальная холловская подгруппа H конечной группы G является вполне характеристической.

Решение. В самом деле, пусть $\varphi \in \mathrm{End}(G)$. Тогда $H\varphi(H) \leq G$ является подгруппой в G, так что $|H\varphi(H)|$ делит G. По формуле произведения

$$|H\varphi(H)| = \frac{|H||\varphi(H)|}{|H \cap \varphi(H)|} = |H||\varphi(H) : H \cap \varphi(H)|,$$

так что $|\varphi(H) : H \cap \varphi(H)|$ одновременно делит как $|H|$, так и $|G:H|$. Тем самым этот индекс равен 1, но это и значит, что $\varphi(H) \leq H$.

• Все подгруппы конечной циклической группы C_n являются вполне характеристическими.

• Коммутант $[G,G]$ группы G является вполне характеристической подгруппой;

• Подгруппа G^n, порожденная n-ми степенями элементов группы G, является вполне характеристической;

Последние два примера — это так называемые **вербальные** подгруппы, порожденных значениями некоторых слов в группе G: в первом случае слова $[x,y]$, а во втором — слова x^n.

Задача. Пусть $n \in \mathbb{Z}$. Докажите, что в том случае, когда множество $\{x \in G \mid x^n = 1\}$ решений уравнения $x^n = 1$ в группе G является подгруппой, это характеристическая — и даже вполне характеристическая — подгруппа G.

А вот несколько примеров характеристических, но, вообще говоря, не вполне характеристических подгрупп (во всех этих примерах мы рассматриваем подгруппы фиксированной группы G):

• подгруппа Фраттини $\Phi(G)$, т. е. пересечение всех максимальных подгрупп;

• **подгруппа Виландта** $\Psi(G)$, т. е. порождение всех минимальных подгрупп;

• пересечение всех подгрупп индекса n;

• пересечение всех подгрупп индекса $\leq n$;

• пересечение всех нормальных подгрупп индекса n;

• пересечение всех нормальных подгрупп индекса $\leq n$;

• **подгруппа Томпсона** $J(P)$ конечной p-группы P, т. е. подгруппа, порожденная всеми абелевыми подгруппами P максимального порядка.

§ 9♠. Характеристически простые группы

Как обобщение последнего примера из предыдущего параграфа заметим, что вообще в любой элементарной абелевой группе $G = E_{p^m}$ нет никаких характеристических подгрупп отличных от 1 и G. Фробениус предложил называть группу G, обладающую этим свойством, **элементарной**. Сегодня в этом смысле чаще всего говорят о **характеристически простых** группах (`characteristically simple`)*.

Теорема. *Конечная группа G тогда и только тогда является характеристически простой, когда она изоморфна прямому произведению попарно изоморфных простых групп.*

Доказательство. Покажем вначале достаточность. Пусть $G = H_1 \times \ldots \times H_s$, где все H_i изоморфны простой группе H. Если $H \cong C_p$ абелева, то $G = \mathbb{F}_p^s$ изоморфна векторному пространству над полем $\mathbb{F}_p$, где у группы $\mathrm{Aut}(G) = \mathrm{GL}(s, \mathbb{F}_p)$ нет нетривиальных собственных инвариантных подпространств. Если же H неабелева, то возьмем характеристическую подгруппу $F \neq 1$ группы G и рассмотрим элемент $f \neq 1$. Представим этот элемент в виде $f = h_1 \times \ldots \times h_s \neq 1$, пусть, например, $h_j \neq 1$. Так как $H_i \cong H$ неабелева, то найдется $g_j \in H_j$ такое, что $[f, g_j] = [h_j, g_j] \neq 1$. Таким образом, $F \cap H_j \neq 1$ и, так как группа H_j проста, $F \cap H_j = H_j$. Это значит, что $H_j \leq F$ и, так как группа $\mathrm{Aut}(G)$ транзитивно действует на факторах $H_1, \ldots, H_s$, мы можем заключить, что $H_i \leq F$ для всех i и, значит, $F = G$.

Доказать необходимость чуть сложнее. Ясно, что любая простая группа является характеристически простой. Поэтому в дальнейшем можно считать, что G не является простой. Пусть H — минимальный нормальный делитель G. Это значит, что $H \trianglelefteq G$, $H \neq 1$, и если $1 \leq F \leq H$ является нормальным делителем G, то $F = 1$ или

*В теории алгебр Ли алгебры без характеристических идеалов называются **дифференциально простыми**, поэтому некоторые специалисты предпочитают говорить об **автоморфно простых** группах.

$F = H$. Так как по условию подгруппа H не может быть характеристической, существует гомоморфизм $\varphi \in \mathrm{Aut}(G)$ такой, что $\varphi(H) \neq H$. Пусть $H_1 = H, H_2 \dots, H_s$, где $s \geq 2$, — множество всех различных подгрупп, в которые H переходит под действием $\mathrm{Aut}(G)$. Подгруппа $H_1 \dots H_s$ является характеристической в G и, значит, обязана совпадать с G. Ясно, что все H_i являются минимальными нормальными делителями G и, таким образом, $H_i \cap H_j = 1$ для любых $i \neq j$ (в самом деле, $H_i \cap H_j \trianglelefteq G$ строго содержится в H_i и, значит, обязано равняться 1). В частности, H поэлементно коммутирует со всеми подгруппами $H_2, \dots, H_s$. Тем самым, любой нормальный делитель группы H автоматически является нормальным делителем в G. В силу минимальности H это означает, что H обязана быть простой группой. Пересечение $H \cap H_2 \dots H_s$ содержится в центре H и, значит, мы имеем следующую альтернативу: либо $H \leq H_2 \dots H_s$, либо $H \cap H_2 \dots H_s = 1$. В первом случае H абелева, $H \leq C(G)$ и, так как $C(G)$ является характеристической подгруппой, $C(G) = G$. Тем самым, в этом случае G абелева и наше утверждение вытекает из теоремы о строении конечных абелевых групп. Во втором случае применяя автоморфизм группы G, переводящий H в H_i, мы можем заключить, что $H_i \cap H_1 \dots \widehat{H_i} \dots H_s = 1$. Но это и означает, что $G = H_1 \times \dots \times H_s$.

Замечание. В действительности в этой теореме конечность группы использовалась лишь для того, чтобы гарантировать существование в G минимального нормального делителя. Именно в такой форме и сформулирован этот результат в [**220**], стр.62, но приведенные там доказательства содержат пробелы.

§ 10♣. Хопфовость и отмеченные подгруппы

В настоящем параграфе мы обсудим два экзотических понятия.

1. Отмеченные подгруппы. Подгруппа $H \leq G$ называется **отмеченной**, если $\varphi(H) \leq H$ и **вполне отмеченной**, если $H = \varphi^{-1}(H)$ для любого **сюръективного эндоморфизма** $\varphi \in \mathrm{End}(G)$. Легко видеть, что вполне отмеченная подгруппа является отмеченной. Кроме того, очевидны следующие импликации:

$$\text{вполне характеристическая} \Longrightarrow \text{отмеченная} \Longrightarrow \text{характеристическая}$$

Задача. Убедитесь, что центр группы является отмеченной подгруппой.

Задача. Приведите пример отмеченной подгруппы, не являющейся вполне характеристической.

Указание. Постройте группу, центр которой не является вполне характеристической подгруппой.

Задача. Докажите, что пересечение (вполне) отмеченных подгрупп есть (вполне) отмеченная подгруппа.

2. Хопфовы группы. В действительности, большинство алгебраистов никогда не слышало об отмеченных и вполне отмеченных подгруппах. Почему? Дело в том, что эти понятия начинают жить самостоятельной жизнью только для нехопфовых групп, в то время как большинство встречающихся в природе групп, в частности все конечные группы, хопфовы. Напомним, что группа G называется **нехопфовой**, если в ней существует нетривиальная нормальная подгруппа $H \trianglelefteq G$ такая, что $G/H \cong G$. Если такой подгруппы $H \neq 1$ не существует, то группа G называется **хопфовой**. В действительности, до начала 1950-х годов [187], [188] было неизвестно даже, существуют ли вообще конечно порожденные (и конечно представимые) нехопфовы группы, этот вопрос известен как **проблема Хопфа**.

Задача. Докажите, что группа G в том и только том случае хопфова, когда каждый ее сюръективный эндоморфизм является автоморфизмом.

Решение. В самом деле, для любого сюръективного эндоморфизмома $\varphi \in \mathrm{End}(G)$ имеем $G \cong G/\operatorname{Ker}(\varphi)$, так что если $\operatorname{Ker}(\varphi) \neq 1$, то группа G нехопфова. Обратно, если $H \trianglelefteq G$, $H \neq 1$ таково, что $G/H \cong G$, то композиция $G \longrightarrow G/H \cong G$ является сюръективным эндоморфизмом G с нетривиальным ядром.

Задача. Убедитесь, что в хопфовой группе каждая характеристическая подгруппа является отмеченной.

Интересно, что двойственное понятие кохопфовой группы не имеет большого значения. Группа называется **кохопфовой**, если она не изоморфна никакой своей собственной подгруппе, а именно, если любой инъективный эндоморфизм $\varphi : G \longrightarrow G$ является автоморфизмом. Ясно, что уже группа $\mathbb{Z}$ не является кохопфовой.

§ 11♡. Группа автоморфизмов

В этом параграфе мы приводим несколько простейших примеров вычисления группы автоморфизмов.

1. Моноид/кольцо эндоморфизмов. Обозначим через $\mathrm{End}(G)$ множество всех эндоморфизмов группы G с операцией композиции. Ясно, что $\mathrm{End}(G)$ образует моноид, нейтральным элементом которого является тождественный автоморфизм группы G. Если группа G *абелева*, то, как мы знаем из § 3, на множестве $\mathrm{End}(G)$ можно, кроме композиции можно определить еще **поточечное сложение**, определяя сумму эндоморфизмов φ и ψ посредством $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$, для всех $x \in G$. Легко проверить (мы это делаем в книге III), что относительно операций поточечного сложения и композиции множество $\mathrm{End}(G)$ эндоморфизмов абелевой группы образует ассоциативное (но не обязательно коммутативное) кольцо с 1. Приведем несколько очевидных примеров колец эндоморфизмов

- $\mathrm{End}(\mathbb{Z}^+) \cong \mathbb{Z}$;
- $\mathrm{End}(C_n) \cong \mathbb{Z}/n\mathbb{Z}$;

• $\mathrm{End}(\mu_{p^\infty}) \cong \mathbb{Z}_p$ — есть кольцо **целых p-адических чисел** (это очевидно, если пользоваться определением $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, см., например, [**97**], с.57–58 по поводу доказательства);

• $\mathrm{End}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p$;

• $\mathrm{End}(\mathbb{Z}^n) \cong M(n, \mathbb{Z})$;

• $\mathrm{End}(E_{p^n}) \cong M(n, \mathbb{F}_p)$.

Почти все эти утверждения очевидны. Для доказательства двух первых достаточно заметить, что эндоморфизм циклической группы полностью определяется своим значением на образующей, которое может быть любым. Для доказательства последнего утверждения заметим, что эндоморфизмы элементарной абелевой группы E_{p^n} — это в точности эндоморфизмы векторного пространства $\mathbb{F}_p^n$.

2. Группа автоморфизмов. Напомним, что для группы G через $\mathrm{Aut}(G)$ обозначается группа всех ее автоморфизмов относительно композиции. Ясно, что $\mathrm{Aut}(G) = \mathrm{End}(R)^*$ состоит в точности из всех обратимых элементов моноида/кольца $\mathrm{End}(G)$.

Явное описание группы $\mathrm{Aut}(G)$ является одной из важнейших задач теории групп. Вот несколько примеров вычисления группы автоморфизмов. Следующие шесть примеров непосредственно получаются из соответствующих примеров предыдущего пункта.

• $\mathrm{Aut}(\mathbb{Z}^+) \cong C_2$;

• $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$;

• $\mathrm{Aut}(\mu_{p^\infty}) \cong \mathbb{Z}_p^*$;

• $\mathrm{Aut}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p^*$;

• $\mathrm{Aut}(\mathbb{Z}^n) \cong \mathrm{GL}(n, \mathbb{Z})$;

• $\mathrm{Aut}(E_{p^n}) \cong \mathrm{GL}(n, p)$.

• В главе 5 мы проверим, что $\mathrm{Aut}(S_n) = S_n$ при $n \neq 2, 6$ (**теорема Гельдера**).

• В следующей части книги мы вычислим группу $\mathrm{Aut}(\mathrm{GL}(n, K))$ и покажем, что каждый автоморфизм $\mathrm{GL}(n, R)$ является произведением внутреннего, полевого и центрального автоморфизмов и, возможно, контраградиента (**теорема Шрайера—ван дер Вардена**).

3. Группа автоморфизмов циклической группы. Конкретизируем, для примера, описание автоморфизмов циклической группы, к которому очень часто приходится обращаться при решении задач по теории конечных групп. Для этого сошлемся на вычисление $(\mathbb{Z}/n\mathbb{Z})^*$,

которое проводится в книге III. Мы не будем повторять здесь это вычисление, а лишь сформулируем получающийся результат. Прежде всего, если $n = p_1^{m_1} \dots p_s^{m_s}$, где p_i — попарно взаимно простые простые числа, то **китайская теорема об остатках** утверждает, что

$$(\mathbb{Z}/n\mathbb{Z})^* \cong (\mathbb{Z}/p_1^{m_1}\mathbb{Z})^* \oplus \dots \oplus (\mathbb{Z}/p_s^{m_s}\mathbb{Z})^*.$$

Таким образом, нам нужно только вычислить $\mathrm{Aut}(C_{p^m})$, где p простое число. Здесь проявляется ДРАМАТИЧЕСКОЕ отличие случая $p = 2$ от всех остальных, которое отражается во всех аспектах строения конечных p-групп.

Теорема. *Для нечетного p имеем*

$$\mathrm{Aut}(C_{p^m}) \cong C_{(p-1)p^{m-1}}.$$

При $p = 2$ имеем $\mathrm{Aut}(C_2) = 1$, $\mathrm{Aut}(C_4) \cong C_2$ и $\mathrm{Aut}(C_{2^m}) \cong C_2 \times C_{2^{m-2}}$.

Таким образом, группа автоморфизмов циклической группы *нечетного* примарного порядка тоже циклическая, в то время как при любом $n \geq 3$ группа автоморфизмов циклической группы порядка 2^n таковой не является. Именно это обстоятельство отвечает за появление дополнительных примеров 2-групп, по сравнению с p-группами при $p \geq 3$.

Следствие 1. *Для любого простого p имеем $\mathrm{Aut}(C_p) \cong C_{p-1}$.*

Особенно часто используется такое следствие этой теоремы.

Следствие 2. *Группа автоморфизмов $\mathrm{Aut}(G)$ циклической группы G абелева.*

Обратите внимание, что $\mathrm{Aut}(C_3) \cong \mathrm{Aut}(C_4) \cong C_2$. Можно доказать [189], что для данной конечной группы H существует конечное числа неизоморфных конечных групп G таких, что $\mathrm{Aut}(G) \cong H$. При этом далеко не всякая группа может быть представлена как группа автоморфизмов. Вот несколько простейших примеров групп H, для которых не существует группы G — конечной или бесконечной — такой, что $\mathrm{Aut}(G) \cong H$.

• Циклическая группа нечетного порядка C_{2l+1} — это одна из задач следующего параграфа.

• Симметрическая группа S_6 — это как раз то исключение, которое возникает в теореме Гельдера!

• Все нетривиальные знакопеременные группы A_n, кроме $A_8 \cong \mathrm{PSL}(4, 2)$.

• Многие другие группы, например, бесконечная циклическая группа $\mathbb{Z}$.

Задача. Убедитесь, что если G — конечная группа порядка n, то порядок $\mathrm{Aut}(G)$ не превосходит $(n-1)!$. Когда достигается эта граница?

4. Группа автоморфизмов диэдральной группы. Теперь разберем еще один ключевой пример.

Задача. Докажите, что $\mathrm{Aut}(D_3) \cong D_3$ и $\mathrm{Aut}(D_4) \cong D_4$. Какая гипотеза у Вас возникла? Теперь вычислите $\mathrm{Aut}(D_n)$.

Решение. Гипотеза неверна уже для $D_2 = V$, так как

$$\mathrm{Aut}(D_2) \cong \mathrm{GL}(2,2) \cong S_3 \cong D_3.$$

Пусть теперь $n \geq 3$. В этом случае группа D_n порождается элементом x порядка $n \geq 3$ и инволюцией y такой, что xy тоже является инволюцией. При этом $D_n = \{x^j, x^j y, j = 0, \dots, n-1\}$, причем все элементы $x^j y$ являются инволюциями. Пусть $\varphi \in \mathrm{Aut}(D_n)$. Так как автоморфизмы сохраняют порядок, то $\varphi(x) = x^i$ для какого-то i взаимно простого с n и, следовательно, так как $\varphi(x)$ и $\varphi(y)$ должны порождать группу D_n, $\varphi(y) = x^j y$ для какого-то $j = 0, \dots, n-1$. С другой стороны, очевидно, что любой такой выбор i и j приводит к автоморфизму D_n. Таким образом, $|\mathrm{Aut}(D_n)| = \varphi(n)n$. Небольшое дополнительное усилие [190], позволяет проверить, что $\mathrm{Aut}(D_n)$ раскладывается в полупрямое произведение $\mathrm{Aut}(D_n) \cong C_{\varphi(n)} \leftthreetimes C_n$, где $C_{\varphi(n)}$ действует на C_n как группа автоморфизмов, т. е., иными словами, $\mathrm{Aut}(D_n) \cong \mathrm{Hol}(C_n)$. Случаи $n = 3$ и $n = 4$, когда $\varphi(n) = 2$, являются *единственными* случаями, для которых $\mathrm{Aut}(D_n) \cong D_n$.

Задача. Докажите, что $\mathrm{Aut}(C_2 \oplus C_4) = D_4$. В частности, $\mathrm{Aut}(C_2 \oplus C_4) \cong \mathrm{Aut}(D_4)$. Вычислите $\mathrm{Aut}(C_2 \oplus C_n)$ для произвольного n.

§ 12♡. Строение группы автоморфизмов

В настоящем параграфе мы обсудим некоторые аспекты строения группы $\mathrm{Aut}(G)$, которые впервые начал изучать в 1893 году О. Гельдер. Именно он ввел группу $\mathrm{Inn}(G)$ внутренних изоморфизмов, заметил ее изоморфизм с $G/C(G)$ и то, что она нормальна в $\mathrm{Aut}(G)$, и начал рассматривать группу $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ внешних автоморфизмов.

1. Группа внутренних автоморфизмов. / Отображение $G \longrightarrow$

$\mathrm{Aut}(G)$, $g \mapsto I_g$, является гомоморфизмом, $I_{gh} = I_g I_h$. В самом деле,

$$I_{gh}(x) = (gh)x(gh)^{-1} = g(hxh^{-1})g^{-1} = I_g(hxh^{-1}) = I_g(I_h(x)) = I_g I_h(x).$$

Все внутренние автоморфизмы $\mathrm{Inn}(G) = \{I_g \mid g \in G\}$ образуют подгруппу в $\mathrm{Aut}(G)$, называемую **группой внутренних автоморфизмов** группы G.

Теорема. *Подгруппа* $\mathrm{Inn}(G)$ *нормальна в* $\mathrm{Aut}(G)$. *Имеет место изоморфизм* $\mathrm{Inn}(G) \cong G/C(G)$,

Доказательство. Для доказательства первого утверждения заметим, что вычисление

$$\varphi I_g \varphi^{-1}(x) = \varphi(g\varphi^{-1}(x)g^{-1}) = \varphi(g)x\varphi(x)^{-1}$$

показывает, что $\varphi I_g \varphi^{-1} = I_{\varphi(g)}$, так что любой автоморфизм, сопряженный с внутренним, сам является внутренним. Второе утверждение теоремы следует из теоремы о гомоморфизме, если заметить, что гомоморфизм I_g в том и только том случае тривиален, когда $g \in C(G)$, так что ядро гомоморфизма $G \longrightarrow \mathrm{Aut}(G)$, $g \mapsto I_g$, совпадает с $C(G)$.

Следствие. *Группа без центра* G *изоморфно вкладывается в свою группу автоморфизмов* $\mathrm{Aut}(G)$.

2. Группа внешних автоморфизмов. Фактор-группа

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

называется **группой внешних автоморфизмов** группы G. Для многих классов групп можно доказать, что $\mathrm{Out}(G) \neq 1$. Приведем пример классического результата в таком духе.

Теорема Гашюца. *Пусть* G *конечная* p*-группа, не являющаяся циклической. Тогда* $\mathrm{Out}(G) \neq 1$.

Уже эти простейшие наблюдения о строении группы $\mathrm{Aut}(G)$ позволяют вычислить эту группу в некоторых интересных случаях.

Задача. Вычислите группу автоморфизмов $\mathrm{Aut}(Q)$ группы кватернионов.

Задача. Докажите, что если $\mathrm{Aut}(G)$ циклическая, то G абелева.

Задача. Докажите, что не существует группы G такой, что $\mathrm{Aut}(G)$ циклическая группа *нечетного* порядка.

§ 13♡. Суммируемые эндоморфизмы

В предыдущем параграфе мы определили поточечное сложение на моноиде $\mathrm{End}(G)$ эндоморфизмов *абелевой* группы G, которое превратило $\mathrm{End}(G)$ в кольцо. Что мешает нам задать такую же операцию на $\mathrm{End}(G)$ в общем случае?

Мы можем, конечно, и для неабелевой группы G определить **сумму** двух эндоморфизмов формулой

$$(\varphi+\psi)(x)=\varphi(x)\psi(x),$$

к сожалению, получившееся при этом отображение $\varphi+\psi: G\longrightarrow G$ совершенно не обязано быть эндоморфизмом группы G.

Задача. Пусть $G=S_3$, $\varphi=I_{(123)}$, $\psi=I_{(132)}$. Проверьте, что $\varphi+\psi$ не является эндоморфизмом G.

Благодаря какому обстоятельству $\varphi+\psi$ все же было эндоморфизмом для абелевых групп? Разумеется, ровно потому, что $\varphi(x)$ и $\psi(y)$ коммутировали для любых $x,y\in G$. Это мотивирует следующее определение. Назовем эндоморфизмы φ и ψ **суммируемыми**, если группы $\varphi(G)$ и $\psi(G)$ поэлементно коммутируют.

Задача. Проверьте, что сумма двух суммируемых эндоморфизмов $\varphi,\psi\in\mathrm{End}(G)$ является эндоморфизмом.

Решение. В самом деле, для любых $x,y\in G$ имеем

$$(\varphi+\psi)(xy)=\varphi(xy)\psi(xy)=\varphi(x)\varphi(y)\psi(x)\psi(y)=\\ \varphi(x)\psi(x)\varphi(y)\psi(y)=(\varphi+\psi)(x)(\varphi+\psi)(y).$$

Сложение суммируемых эндоморфизмов обладает всеми обычными свойствами.

Задача. Предположим, что эндоморфизмы $\varphi,\psi\in\mathrm{End}(G)$ суммируемы. Тогда $\varphi+\psi=\psi+\varphi$.

Обратите внимание, что выполнение этого равенства не предполагает, что сами подгруппы $\varphi(G)$ и $\psi(G)$ абелевы, они лишь поэлементно коммутируют! Однако в действительности можно вовсе не вспоминать про $\varphi(G)$ и $\psi(G)$, а воспользоваться непосредственно тем, что $x\mapsto(\varphi+\psi)(x)=\varphi(x)\psi(x)$ эндоморфизм:

$$(\varphi+\psi)(x)=(\varphi+\psi)(x^{-1})^{-1}=(\varphi(x^{-1})\psi(x^{-1}))^{-1}=\\ \psi(x^{-1})^{-1}\varphi(x^{-1})^{-1}=\psi(x)\varphi(x)=(\psi+\varphi)(x).$$

Задача. Предположим, что эндоморфизмы $\varphi, \chi, \psi \in \mathrm{End}(G)$ попарно суммируемы. Проверьте, что тогда $\varphi + \chi$ суммируемо с ψ, φ суммируемо с $\chi + \psi$ и выполняется равенство

$$(\varphi + \chi) + \psi = \varphi + (\chi + \psi).$$

Задача. Предположим, что эндоморфизмы $\chi, \psi \in \mathrm{End}(G)$ суммируемы. Проверьте, что тогда для любого $\varphi \in \mathrm{End}(G)$ эндоморфизмы $\varphi\chi$ и $\varphi\psi$ суммируемы и выполняется равенство

$$\varphi(\chi + \psi) = \varphi\chi + \varphi\psi.$$

Решение. В самом деле, так как $\chi(G)$ и $\psi(G)$ поэлементно коммутируют, то для любых $x, y \in G$ имеем

$$\begin{aligned}(\varphi\chi)(x))(\varphi\psi(y)) = \varphi(\chi(x))\varphi(\psi(y)) = \varphi(\chi(x)\psi(y)) = \\ \varphi(\psi(y)\chi(x)) = \varphi(\psi(y))\varphi(\chi(x)) = (\varphi\psi)(y))(\varphi\chi(x)).\end{aligned}$$

Кроме того, для каждого $x \in G$ имеем

$$\begin{aligned}(\varphi(\chi + \psi))(x) = \varphi((\chi + \psi)(x)) = \varphi(\chi(x)\psi(x)) = \\ \varphi\chi(x)\varphi\psi(x) = (\varphi\chi + \varphi\psi)(x).\end{aligned}$$

Педагогический комментарий. Обычно мне быстро надоедает проводить идиотские вычисления подобного рода на доске и я прекращаю заниматься такими глупостями после двух–трех лекций. Дело в том, что сильному студенту подобные тривиальности вообще не нужны, а любому нормальному студенту проще (и гораздо полезнее!) проводить все такие вычисления самостоятельно, чем срисовывать их с доски. В то же время ничто не может способствовать росту техники безнадежно слабого или педагогически запущенного студента — всеми нужными здесь математическими навыками можно овладеть *только* в начальных классах школы и если это не было сделано, это не было сделано, так что *никакие* (сверх)усилия не могут компенсировать нанесенный ущерб. Так что единственная видимая цель подобного рода занятий — упражнение в **какографии**.

Задача. Предположим, что эндоморфизмы $\varphi, \chi \in \mathrm{End}(G)$ суммируемы. Проверьте, что тогда для любого $\psi \in \mathrm{End}(G)$ эндоморфизмы $\varphi\psi$ и $\chi\psi$ суммируемы и выполняется равенство

$$(\varphi + \chi)\psi = \varphi\psi + \varphi\psi.$$

В действительности, суммируемость эндоморфизмов теснейшим образом связана с возможностью разложения G в прямое (или центральное) произведение. Основным применением суммируемости в книге как раз и будет доказательство теоремы Ремака—Крулля—Шмидта о единственности слагаемых в прямых разложениях.

§ 14♡. Нормальные и центральные эндоморфизмы

1. Нормальные эндоморфизмы. Если x и y сопряжены при помощи g, то для любого эндоморфизма $\varphi(x)$ и $\varphi(y)$, по-прежнему сопряжены в G, но, конечно, теперь при помощи $\varphi(g)$. Огромную роль во многих доказательствах играет класс эндоморфизмов, для которых $\varphi(x)$ и $\varphi(y)$ продолжают оставаться сопряженными при помощи *того же самого* g, иными словами,

$$\varphi(ghg^{-1}) = g\varphi(h)g^{-1},$$

такие эндоморфизмы принято называть **нормальными**. Из этого определения ясно, что эндоморфизм φ группы G в том и только том случае нормален, когда он перестановочен со всеми внутренними автоморфизмами: $\varphi I_g = I_g\varphi$.

Упражнение. Убедитесь, что композиция двух нормальных эндоморфизмов является нормальным эндоморфизмом.

Упражнение. Убедитесь, что сумма двух суммируемых нормальных эндоморфизмов является нормальным эндоморфизмом.

Упражнение. Убедитесь, что если φ — нормальный эндоморфизм, а $H \trianglelefteq G$, то $\varphi(H) \trianglelefteq G$.

Следствие. *Для любого нормального эндоморфизма φ имеем $\varphi(G) \trianglelefteq G$.*

Очевидно, что, вообще говоря, образ эндоморфизма совершенно не обязан быть нормальной подгруппой в G — приведите пример!

2. Центральные эндоморфизмы. ?? ?? В большинстве книг нормальные *автоморфизмы* — или, если быть совсем точным, нормальные сюръективные эндоморфизмы — описываются несколько иначе. А именно, эндоморфизм $\varphi \in \mathrm{End}(G)$ называется **центральным**, если $g^{-1}\varphi(g) \in C(G)$ для всех $g \in G$. Очевидно, что любой центральный эндоморфизм нормален. Оказывается, для *сюръективных* эндоморфизмов верно и обратное.

Задача. Покажите, что сюръективный эндоморфизм в том и только том случае нормален, когда он централен.

Решение. В самом деле, по определению нормального эндоморфизма

$$\varphi(g)\varphi(h)\varphi(g)^{-1} = g\varphi(h)g^{-1}.$$

Это равенство в точности означает, что $g^{-1}\varphi(g)$ коммутирует со всеми $\varphi(h)$. Так как $\varphi(G) = G$, то $g^{-1}\varphi(g) \in C(G)$.

Задача. Покажите, что для центрального эндоморфизма отображение $\psi : G \longrightarrow C(G)$, $g \mapsto g^{-1}\varphi(g)$, является гомоморфизмом G в $C(G)$.

Решение. В самом деле, для любых $h, g \in G$ имеем

$$\psi(hg) = (hg)^{-1}\varphi(hg) = g^{-1}h^{-1}\varphi(h)\varphi(g) = \\ g^{-1}\psi(h)\varphi(g) = \psi(h)g^{-1}\varphi(g) = \psi(h)\psi(g).$$

В частности, все эти утверждения применимы к автоморфизмам. Особенно часто мы будем пользоваться такими их следствиями.

Следствие. *Все центральные автоморфизмы образуют подгруппу в* $\mathrm{Aut}(G)$.

Следствие. *Если* $C(G) = 1$, *то* $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$.

3. H-нормальные автоморфизмы. Развитую в предыдущих пунктах теорию легко обобщить.

Задача. Пусть $H \trianglelefteq G$ — нормальная подгруппа в G. Положим

$$\mathrm{Aut}(G, H) = \{\varphi \in \mathrm{Aut}(G) \mid \forall g \in G, g^{-1}\varphi(g) \in H\}.$$

Докажите, что $\mathrm{Aut}(G, H) \leq \mathrm{Aut}(G)$.

Группа $\mathrm{Aut}(G, H)$ состоит из тех автоморфизмов группы G, которые переводят H в себя и индуцируют тривиальный автоморфизм на фактор-группе G/H. В этих обозначениях группа центральных автоморфизмов совпадает с $\mathrm{Aut}(G, C(G))$.

Задача. Пусть $H \trianglelefteq G$. Положим

$$\mathrm{Aut}_1(G, H) = \{\varphi \in \mathrm{Aut}(G, H) \mid \varphi|_H = \mathrm{id}_H\}.$$

Докажите, что $\mathrm{Aut}_1(G, H) \trianglelefteq \mathrm{Aut}(G, H)$.

Задача. Пусть, по-прежнему, $H \trianglelefteq G$. Всегда ли можно утверждать, что $\mathrm{Aut}(G, H) \trianglelefteq \mathrm{Aut}(G)$? При каком предположении на H это заведомо верно? Положим

$$\mathrm{IAut}(G) = \mathrm{Aut}(G, [G, G]).$$

Докажите, что $\mathrm{IAut}(G) \trianglelefteq \mathrm{Aut}(G)$.

Следующая простая идея является одним из ключевых соображений в применении линейных групп к изучению конечных групп.

Задача. Пусть $H \trianglelefteq G$. Докажите, что $G/C_G(H)$ изоморфно вкладывается в $\mathrm{Aut}(H)$.

Следствие. *Если* $H \trianglelefteq G$ — *элементарная абелева* p*-группа порядка* p^n, *то* $G/C_G(H)$ *изоморфно вкладывается в* $\mathrm{GL}(n, p)$.

§ 15♠. Сюръективность = инъективность

Если группа G конечна, то принцип Дирихле утверждает, что эндоморфизм $\varphi \in \mathrm{End}(G)$ в том и только том случае является автоморфизмом, когда он является мономорфизмом или эпиморфизмом. Тем самым для *конечной* группы требование инъективности эндоморфизма равносильно требованию его сюръективности.

Оказывается, то же самое верно для любой группы, одновременно удовлетворяющей условиям `ACC` и `DCC`. Более того, при этом достаточно требовать выполнения условия `ACC` для нормальных подгрупп, а для *нормальных* эндоморфизмов и условие `DCC` нужно накладывать только на нормальные подгруппы! Точнее, имеют место следующие результаты, являющиеся одним из ключевых моментов в доказательстве теоремы Ремака—Крулля—Шмидта.

Начнем с проверки того, что инъективность влечет сюръективность.

Теорема. *Пусть $\varphi \in \mathrm{End}(G)$ — инъективный эндоморфизм группы G, удовлетворяющей условию* `DCC`*. Тогда φ является автоморфизмом.*

Доказательство. В первом случае предположим, вопреки ожиданиям, что φ не сюръективен. Мы утверждаем, что тогда

$$G > \varphi(G) > \varphi^2(G) > \dots$$

образует бесконечную строго убывающую цепочку подгрупп. Для этого нам достаточно для каждого $n \in \mathbb{N}$ найти элемент

$$x \in \varphi^n(G) \setminus \varphi^{n+1}(G).$$

В самом деле, пусть $g \notin \varphi(G)$. Включение $\varphi^n(g) \in \varphi^{n+1}(G)$ значило бы, что найдется элемент $h \in G$ такой, что $\varphi^n(g) = \varphi^{n+1}(h)$. Но так как φ^n инъективен, то $\varphi^n(g) = \varphi^{n+1}(h) = \varphi^n(\varphi(h))$ влечет $g = \varphi(h)$, что противоречит выбору g. Таким образом, $x = \varphi^n(g) \notin \varphi^{n+1}(G)$ как раз и будет требуемым элементом. Но по предположению теоремы в G не существует бесконечных строго убывающих цепочек подгрупп, противоречие.

То же, на `bis`.

Теорема bis. *Пусть $\varphi \in \mathrm{End}(G)$ — инъективный нормальный эндоморфизм группы G, удовлетворяющей условию* `DCC` *для нормальных подгрупп. Тогда φ является автоморфизмом.*

Доказательство. Достаточно слово в слово повторить доказательство предыдущей теоремы, вспомнив при этом, что:

• степень φ^n нормального эндоморфизма φ нормальна,

• образ $\varphi^n(G)$ нормального эндоморфизма является нормальной подгруппой в G.

Тем самым, тот же метод, что и в доказательстве предыдущей теоремы, позволяет построить бесконечную строго убывающую цепочку *нормальных* подгрупп.

Установим теперь, что и сюръективность в свою очередь влечет инъективность. Здесь ситуация несколько упрощается тем, что ядро любого эндоморфизма автоматически является *нормальной* подгруппой в G, так что никаких предположений относительно нормальности эндоморфизма не требуется.

Теорема. *Пусть $\varphi \in \mathrm{End}(G)$ — сюръективный эндоморфизм группы G, удовлетворяющей условию* ACC *для нормальных подгрупп. Тогда φ является автоморфизмом.*

Доказательство. Предположим, вопреки ожиданиям, что φ не инъективен. Мы утверждаем, что тогда

$$1 < \mathrm{Ker}(\varphi) < \mathrm{Ker}(\varphi^2) < \dots$$

образует бесконечную строго возрастающую цепочку нормальных подгрупп в G. Для этого нам достаточно для каждого $n \in \mathbb{N}$ найти элемент

$$x \in \mathrm{Ker}(\varphi^{n+1}) \setminus \mathrm{Ker}(\varphi^n).$$

В самом деле, пусть $g \neq 1$, но $\varphi(g) = 1$. В силу сюръективности φ^n найдется такой $x \in G$, что $\varphi^n(x) = g$. Тогда $\varphi^n(x) = g \neq 1$, но $\varphi^{n+1}(x) = \varphi(g) = 1$, так что x как раз и будет требуемым элементом. Но по предположению теоремы в G не существует бесконечных строго возрастающих цепочек нормальных подгрупп, противоречие.

§ 16♣. Группа автоморфизмов неабелевой простой группы

1. Группа автоморфизмов неабелевой простой группы. Следующий цикл задач взят со с.131 Бурбаки, Алгебра, т.I.

Задача. Пусть G — неабелева простая группа. Покажите, что $\mathrm{Inn}(G)$ характеристическая подгруппа в $\mathrm{Aut}(G)$.

Решение. Пусть $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$. Тогда $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) \trianglelefteq \mathrm{Aut}(G)$. Так как $\mathrm{Inn}(G) \cong G$ простая, то либо $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) = \mathrm{Inn}(G)$, в этом случае

доказательство закончено, либо $\mathrm{Inn}(G) \cap \varphi(\mathrm{Inn}(G)) = 1$. Во втором случае $\mathrm{Aut}(G)$ содержит прямое произведение $\mathrm{Inn}(G) \times \varphi(\mathrm{Inn}(G))$. Но ведь G группа без центра и, значит, по предыдущей задаче $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$.

Задача. Пусть G — группа без центра и $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$. Показать, что если $\varphi(I_g) = I_g$ для всех $I_g \in \mathrm{Inn}(G)$, то $\varphi = \mathrm{id}$.

Решение. По условию для любого $g \in G$ имеем $\varphi(I_g) = I_g$ и, тем самым,

$$\varphi(\pi) I_g \varphi(\pi)^{-1} = \varphi(\pi I_g \pi^{-1}) = \varphi(I_{\pi(g)}) = I_{\pi(g)} = \pi I_g \pi^{-1}$$

для любого $\pi \in \mathrm{Aut}(G)$. Это равенство можно переписать в виде $\pi^{-1}\varphi(\pi) I_g = I_g \pi^{-1}\varphi(\pi)$. По первой задаче автоморфизм $\pi^{-1}\varphi(\pi)$, центральный, но так как G группа без центра, то $\pi^{-1}\varphi(\pi)(g) = g$ для всех $g \in G$. Но это и значит, что $\varphi(\pi)(g) = \pi(g)$ так что действительно $\varphi(\pi) = \pi$, как и утверждалось.

Задача. Пусть G — неабелева простая группа. Показать, что каждый автоморфизм группы $\mathrm{Aut}(G)$ внутренний.

Решение. Сопоставим автоморфизму $\varphi \in \mathrm{Aut}(\mathrm{Aut}(G))$ автоморфизм π группы G следующим образом: $I_{\pi(g)} = \varphi(I_g)$. По первой задаче этого пункта $\mathrm{Inn}(G) \cong G$ характеристическая подгруппа в $\mathrm{Aut}(G)$. Утверждается, что тогда $\varphi(\psi) = \pi\psi\pi^{-1}$ для любого $\psi \in \mathrm{Aut}(G)$. Это равносильно тому, что автоморфизм $\psi \mapsto \pi^{-1}\varphi(\psi)\pi$ группы $\mathrm{Aut}(G)$ тождественный. В силу второй задачи для этого достаточно показать, что он оставляет на месте все внутренние автоморфизмы. В самом деле,

$$\pi^{-1}\varphi(I_g)\pi(x) = \pi^{-1} I_{\pi(g)} \pi(x) = \pi^{-1}(\pi(g)\pi(x)\pi(g)^{-1}) = gxg^{-1} = I_g(x),$$

что и требовалось.

Таким образом, резюмируя содержание этих задач, мы доказали следующий результат.

Теорема. *Если G неабелева простая группа, то* $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathrm{Aut}(G))$.

2. Теорема Виландта. В действительности в 1939 году Виландт доказал следующий результат. Положим $\mathrm{Aut}_0(G) = G$, $\mathrm{Aut}_1(G) = \mathrm{Aut}(G)$, $\mathrm{Aut}_2(G) = \mathrm{Aut}(\mathrm{Aut}(G))$, и далее $\mathrm{Aut}_n(G) = \mathrm{Aut}(\mathrm{Aut}_{n-1}(G))$. Каждая группа без центра вкладывается в свою группу автоморфизмов, и мы отождествим G с подгруппой в $\mathrm{Aut}(G)$. В свою очередь, группа автоморфизмов группы без центра — тоже группа без центра, так что мы получаем башню $G \leq \mathrm{Aut}(G) \leq \mathrm{Aut}_2(G) \leq \ldots$. Как мы только что показали, для неабелевых простых групп эта башня стабилизируется уже на первом шаге. Это утверждение допускает очень широкое обобщение.

Теорема Виландта. *Если G — конечная группа без центра, то существует n такое, что* $\mathrm{Aut}_n(G) = \mathrm{Aut}_{n+1}(G) = \ldots$.

Для бесконечных групп аналогичная стабилизация тоже происходит, но на бесконечном ординале (S.Thomas, 1985).

3. Гипотеза Шрайера. Одно из самых важных наблюдений, относящихся к строению группы $\mathrm{Aut}(G)$ для неабелевой простой группы G, состоит в следующем.

Хельмут Виландт (`Helmut Wielandt`, 19 декабря 1910, Нидереггенен — 14 февраля 2001) — замечательный немецкий алгебраист, один из классиков теории групп и линейной алгебры. В 1929 году Виланд поступил в Берлинский университет, где стал учеником Шмидта и Шура. Основные работы Виландта относятся к теории конечных групп и теории групп перестановок. К 1930-м годам изучение групп перестановок полностью вышло из моды, а многие важные результаты в этой области были практически забыты. Именно работы Виландта и его замечательная книга способствовали возрождению интереса к этой теории в 1960-е годы. В 1939 году Виландта призвали на военную службу, и с 1941 года он был привлечен к исследованиям по метеорологии и криптологии, а с 1942 года — к исследованиям в области аэродинамики. После окончания войны он был назначен доцентом в Майнце, а в 1951 году профессором в Тюбингене, где и оставался до ухода на пенсию в 1977 году. В нашем курсе встречается полтора десятка его теорем о группах и несколько предложенных им элегантных доказательств, в частности, его замечательное доказательство теоремы Силова.

Гипотеза Шрайера. *Группа* $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ *внешних автоморфизмов конечной простой группы* G *разрешима.*

В течение многих десятилетий эта гипотеза играла совершенно исключительную роль в теории конечных групп, как в силу своей важности — многие факты теории конечных групп легко проверяются по модулю гипотезы Шрайера, — так и в силу своей неприступности. В настоящее время справедливость гипотезы Шрайера *проверена* для всех простых групп. Скептик сказал бы: для всех **известных** простых групп. Однако поскольку никаких других простых групп *нет*, то гипотезу Шрайера можно теперь рассматривать как теорему. Хотя, конечно, никакого **прямого** доказательства этой теоремы, не опирающегося на классификацию конечных простых групп, нет.

§ 17♢. Матричные гомоморфизмы

Следующие примеры предполагают знакомство с умножением матриц.

• **Однопараметрические подгруппы.** Пусть R — произвольное кольцо, тогда отображение

$$d_{12} : R^* \longrightarrow \mathrm{GL}(2,R), \qquad x \mapsto \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix},$$

является гомоморфизмом, т. е. $d_{12}(xy) = d_{12}(x)d_{12}(y)$ для любых $x, y \in R^*$.

• **Однопараметрические подгруппы, bis.** Следующий исключительно важный пример показывает, что в умножение матриц вплетено не только умножение, но и *сложение* в основном кольце. Отображение

$$t_{12} : R^+ \longrightarrow \mathrm{GL}(2,R), \qquad x \mapsto \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix},$$

является гомоморфизмом аддитивной структуры в мультипликативную, т. е. $t_{12}(x+y) = t_{12}(x)t_{12}(y)$ для любых $x, y \in R$.

• Пусть K — поле характеристики $\neq 2$. Тогда

$$K^+ \longrightarrow \mathrm{SL}(2,K), \qquad x \mapsto \frac{1}{2}\begin{pmatrix} x+x^{-1} & x-x^{-1} \\ x-x^{-1} & x+x^{-1} \end{pmatrix},$$

является гомоморфизмом групп (проверьте!!)

Сейчас для поля $K = \mathbb{R}$ вещественных чисел мы построим еще два примера гомоморфизмов из аддитивной группы поля в мультипликативную группу матриц. Это вытекает из теорем сложения для тригонометрических и гиперболических функций соответственно, см. главу IV.

• **Тригонометрические функции.** Отображение

$$\mathbb{R}^+ \longrightarrow \mathrm{GL}(2,\mathbb{R}), \qquad x \mapsto \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix},$$

является гомоморфизмом. Этот гомоморфизм сопоставляет x эвклидов поворот на угол x.

• **Гиперболические функции.** Отображение

$$\mathbb{R}^+ \longrightarrow \mathrm{GL}(2,\mathbb{R}), \qquad x \mapsto \begin{pmatrix} \mathrm{ch}(x) & \mathrm{sh}(x) \\ \mathrm{sh}(x) & \mathrm{ch}(x) \end{pmatrix},$$

является гомоморфизмом. Этот гомоморфизм сопоставляет x лоренцев поворот на угол x.

В действительности, не будет большим преувеличением сказать, что **все** классические функции **только** потому и интересны, что они являются гомоморфизмами или компонентами гомоморфизмов важнейших алгебраических структур.

Задача (пифагоровы тройки). Пусть K — поле характеристики $\neq 2$, в котором -1 не является квадратом (например, $K = \mathbb{R}$). Определим на множестве K^2 умножение по правилу умножения комплексных чисел $(a,b)(c,d) = (ac-bd, ad+bc)$. Убедитесь, что отображение

$$K^2 \setminus \{(0,0)\} \longrightarrow \mathrm{SL}(2,K), \qquad x \mapsto \frac{1}{a^2+b^2}\begin{pmatrix} a^2-b^2 & 2ab \\ -2ab & a^2-b^2 \end{pmatrix},$$

является гомоморфизмом групп.

Задача (присоединенное представление SL_2). Пусть R — коммутативное кольцо с 1. Доказать, что отображение

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & 2ab & b^2 \\ ac & ad+bc & bd \\ c^2 & 2cd & d^2 \end{pmatrix}$$

представляет собой гомоморфизм групп $\mathrm{GL}(2,R) \longrightarrow \mathrm{GL}(3,R)$.

• **Миноры.** Сопоставим матрице $x \in \mathrm{GL}(n,R)$ матрицу $\bigwedge^m(x)$, составленную из всех ее миноров m-го порядка, упорядоченных лексикографически. Матрица $\bigwedge^m(x)$ называется **m-й внешней степенью** матрицы x. Одна из основных теорем теории определителей, **теорема Бине—Коши**, утверждает, что отображение $\bigwedge^m$ является гомоморфизмом группы $\mathrm{GL}(n,R)$ в группу $\mathrm{GL}(C_n^m,R)$, а именно,

$$\bigwedge^m(xy) = \bigwedge^m(x)\bigwedge^m(y).$$

Применяя эту теорему к первому нетривиальному случаю $n=4$, $m=2$, получим знаменитый гомоморфизм $\mathrm{SL}(4,R) \longrightarrow \mathrm{SO}(6,R)$, сопоставляющий матрице x степени 4 с определителем 1

$$x = \begin{pmatrix} x_{11} & x_{12} & x_{13} & x_{14} \\ x_{21} & x_{22} & x_{23} & x_{24} \\ x_{31} & x_{32} & x_{33} & x_{34} \\ x_{41} & x_{42} & x_{43} & x_{44} \end{pmatrix}$$

ортогональную матрицу $\bigwedge^2(x)$ степени 6

$$\begin{pmatrix} x_{11}x_{22}-x_{12}x_{21} & x_{11}x_{23}-x_{13}x_{21} & x_{11}x_{24}-x_{14}x_{21} \\ x_{11}x_{32}-x_{12}x_{31} & x_{11}x_{33}-x_{13}x_{31} & x_{11}x_{34}-x_{14}x_{31} \\ x_{11}x_{42}-x_{12}x_{41} & x_{11}x_{43}-x_{13}x_{41} & x_{11}x_{44}-x_{14}x_{41} \\ x_{21}x_{32}-x_{22}x_{31} & x_{21}x_{33}-x_{23}x_{31} & x_{21}x_{34}-x_{24}x_{31} \\ x_{21}x_{42}-x_{22}x_{41} & x_{21}x_{43}-x_{23}x_{41} & x_{21}x_{44}-x_{24}x_{41} \\ x_{31}x_{42}-x_{32}x_{41} & x_{31}x_{43}-x_{33}x_{41} & x_{31}x_{44}-x_{34}x_{41} \end{pmatrix}$$

$$\begin{pmatrix} x_{12}x_{23}-x_{13}x_{22} & x_{12}x_{24}-x_{14}x_{22} & x_{13}x_{24}-x_{14}x_{23} \\ x_{12}x_{33}-x_{13}x_{32} & x_{12}x_{34}-x_{14}x_{32} & x_{13}x_{34}-x_{14}x_{33} \\ x_{12}x_{43}-x_{13}x_{42} & x_{12}x_{44}-x_{14}x_{42} & x_{13}x_{44}-x_{14}x_{43} \\ x_{22}x_{33}-x_{23}x_{32} & x_{22}x_{34}-x_{24}x_{32} & x_{23}x_{34}-x_{24}x_{33} \\ x_{22}x_{43}-x_{23}x_{42} & x_{22}x_{44}-x_{24}x_{42} & x_{23}x_{44}-x_{24}x_{43} \\ x_{32}x_{43}-x_{33}x_{42} & x_{32}x_{44}-x_{34}x_{42} & x_{33}x_{44}-x_{34}x_{43} \end{pmatrix}$$

Эта матрица генерирована командой `Minors` в программе `Mathematica`.

Упражнение. Вычислите ядро этого гомоморфизма.

• **Подперманенты.** Этот пример полностью параллелен предыдущему, с заменой определителей на перманенты. Сопоставим матрице $x \in \mathrm{GL}(n,R)$ матрицу $S^m(x)$, составленную из всех ее перманентов m-го порядка, упорядоченных лексикографически. Такая матрица $S^m(x)$ называется **m-й симметрической степенью** матрицы x. **Теорема Бине—Коши для перманентов** [191] утверждает, что отображение S^m является гомоморфизмом группы $\mathrm{GL}(n,R)$ в группу $\mathrm{GL}(C^m_{m+n-1},R)$, а именно,

$$S^m(xy) = S^m(x)S^m(y).$$

§ 18♡. Линейные представления, 1st instalment: язык матриц

В этом и еще четырех параграфах мы на чисто лингвистическом уровне введем понятие линейного представления группы. Это понятие существовало всегда, но было впервые *явно* определено в работе Георга Фробениуса 1896 года [192] в процессе размышлений над задачей о групповых определителях, предложенной Дедекиндом. В 1896–1910 годах Фробениус, Бернсайд и Шур в основных чертах завершили создание классической (полупростой) теории представлений *конечных* групп, по существу эквивалентной теории полупростых алгебр, созданной примерно в то же время, в 1893–1908 годах, Федором Молиным, Эли Картаном и Веддербарном. Конечно, уже Фробениус полностью осознавал *аналогию* между этими теориями — ее трудно не заметить, глядя на формулу $|G| = n_1^2 + \ldots + n_s^2$! Однако то, что эти теории полностью *совпадают*, вряд ли было явно замечено до основополагающей работы Эмми Нетер 1929 года (считается, что в действительности основные идеи этой работы были развиты в 1925–1926 годах).

1. Матричные представления. Пусть R — коммутативное кольцо с $1 \neq 0$. В действительности, при доказательстве большинства содержательных результатов предполагается, что основное кольцо $R = K$ является полем — или, по крайней мере, областью целостности. Гомоморфизм $\varphi : G \longrightarrow \mathrm{GL}(n,R)$ называется **представлением** группы G над (`over`) кольцом R, при этом n называется **степенью** этого представления. По причинам, которые станут ясны в следующем параграфе, образ $\varphi(g)$ элемента $g \in G$ под действием φ обозначается через φ_g.

Оба обозначения имеют свои резоны и свои недостатки. Первое лучше согласовано с обычным обозначением матричных элементов, но приводит к тому, что

Федор Эдуардович Молин (Theodor Molien, 10 сентября 1861, Рига — 25 декабря 1941, Томск) — замечательный российский математик, основные работы которого относятся к теории алгебр (как тогда было принято говорить, *систем гиперкомплексных чисел*) и теории представлений групп. В 1883 году Молин окончил Университет Тарту, где он специализировалася в области астрономии и математики и поехал продолжать образование в Германии, главным образом в Лейпциге под руководством Клейна. Там он слушал лекции Штуди, Киллинга и других выдающихся математиков. В 1892–1893 годах Молин ввел понятие группового кольца и доказал то, что сегодня называется теоремой Веддербарна, для алгебр над $\mathbb{C}$. Позже Эли Картан доказал аналогичный результат для алгебр над $\mathbb{R}$, Веддербарну же принадлежит обобщение на случай произвольного поля. Однако Молин не мог получить постоянной позиции в Тарту — интересно, много ли было там математиков такого класса? Поэтому в 1900 году он переезжает в Томск, где сразу становится профессором политехнического института, а в 1918 году — профессором университета. К сожалению, в силу условий научной изоляции его исследования в этот период не достигли такой глубины и размаха, как в ранний период его деятельности.

формулы перегружены скобками. Второе лучше согласовано с языком операторов и действий, но тогда непонятно, как при этом обозначать элементы матрицы ρ_g и соответствующие координатные функции на группе G. Мы будем попеременно пользоваться и тем и другим обозначением, в зависимости от контекста.

По определению $\varphi_{hg} = \varphi_h\varphi_g$ для любых $h, g \in G$. Тем самым, $\varphi_e = e$ и $\varphi_{g^{-1}} = (\varphi_g)^{-1}$. К представлениям применима вся обычная терминология, используемая для гомоморфизмов, например, совершенно ясно, что подразумевается под ядром или образом представления. Если φ — мономорфизм, то такое представление называется **точным**.

Напомнимя, что как обычно, через x_{ij} обозначается элемент матрицы x в позиции (i, j), $1 \leq i, j \leq n$. Таким образом, $x = (x_{ij})$. Функция $\varphi_{ij} : G \longrightarrow R$, $g \mapsto \varphi(g)_{ij}$, называется **матричным элементом** представления. По определению $\varphi_{ij}(g) = \varphi(g)_{ij}$.

Задача. Напишите, какие условия на φ_{ij} накладываются тем условием, что φ гомоморфизм.

Терминологический комментарий. Профессионалы называют **представлением** группы G ее гомоморфизм в *какую-то* группу, в которой они умеют считать. Особенно часто этот термин используется для гомоморфизмов в группу преобразований *какого-то* множества X — совсем не обязательно векторного пространства или модуля! Так, в теории групп принято говорить о **пермутационных представлениях**, т. е. гомоморфизмах $G \longrightarrow S_n$ в симметрическую группу, **представлениях автоморфизмами**, т. е. гомоморфизмах $G \longrightarrow \mathrm{Aut}(H)$, в группу автоморфизмов какой-то другой группы H и т. д. Вообще, группы *представляют* практически чем угодно: симметриями геометрических объектов; бирациональными преобразованиями; преобразованиями, сохраняющими порядок и т. д. В этом случае, чтобы подчеркнуть, что речь идет именно о гомоморфизмах в полную линейную группу, используется термин **линейные представления** или

матричные представления. Однако физики (т. е. все **не** алгебраисты) используют термин **представление** почти исключительно в таком смысле. Многочисленные книги, в названии которых фигурируют **теория представлений**, **представления конечных групп**, **представления групп Ли**, посвящены именно теории *линейных*, а не каких-нибудь других представлений. Разумеется, **дефолтно** (=by default) мы здесь говорим только о **конечномерных** представлениях, т. е. гомоморфизмах в $\mathrm{GL}(n,R)$ для какого-то конечного n. Теория *бесконечномерных* представлений представляет собой совершенно другую науку, основные вопросы которой чисто алгебраически, без каких-то *суровых* топологических или аналитических предположений, не решаются.

Вот важнейший пример представления, которое есть у любой группы:

• Отображение $G \mapsto R^* = \mathrm{GL}(n,R)$, переводящее каждый элемент группы G в e, называется **тривиальным** представлением. Тривиальное представление размерности 1 называется **единичным** или **главным** (Hauptdarstellung, principal representation).

В действительности, у *общих* групп никаких других (конечномерных) представлений, кроме тривиальных, может и не быть. Однако мы будем интересоваться представлениями не общих, а *совершенно конкретных* групп, в первую очередь:

⋆ конечных групп,

⋆ групп типа Ли,

⋆ групп, близких к свободным,

А вот все *эти* группы имеют **море** интересных представлений, в том числе точных. Нам уже встречалось много примеров представлений конечных групп, и дальнейшие примеры упоминаются в § 18, в § 20 мы резюмируем несколько примеров представлений группы $\mathrm{GL}(n,R)$, а представления свободных групп обсуждаются в Главе XI.

2. Эквивалентность представлений. Классическая теория всегда рассматривает представления *с точностью до сопряженности* в $\mathrm{GL}(n,R)$. Линейные представления, которые сопряжены как гомоморфизмы, принято называть **эквивалентными**. Иными словами, если $\varphi \sim \psi$ два эквивалентных представления, то найдется $x \in \mathrm{GL}(n,R)$ такое, что $x\varphi_g x^{-1} = \psi_g$. Важно подчеркнуть, что это x одно и то же для всех g. Условие эквивалентности можно переписать в виде $x\varphi_g = \psi_g x$. Заметим, что в таком виде это условие имеет смысл даже в случае, когда φ и ψ представления разных степеней. Матрица x, удовлетворяющая этому условию, называется **сплетающим оператором** (intertwining operator). Таким образом, два представления

эквивалентны, если для них существует *обратимый* сплетающий оператор.

В дальнейшем мы не будем различать эквивалентные представления. Например, когда мы говорим, что φ и ψ — *различные* представления, конечно имеется в виду, что они *не эквивалентны*.

Задача. Пусть $G = \langle g \rangle \cong C_2$, а $R = \mathbb{Z}$. Сколько различных среди представлений

$$g \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \quad g \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}?$$

3. Проективные представления. В 1904 году Исайа Шур [193] начал изучение проективных представлений. **Проективным представлением** группы G над кольцом R степени n называется ее гомоморфизм $\varphi : G \longrightarrow \mathrm{PGL}(n, R)$ в проективную линейную группу над этим кольцом. Ограничимся для простоты случаем, когда $R = K$ — поле. В этом случае $\mathrm{PGL}(n, K)$ можно истолковать как факторгруппу полной линейной группы $\mathrm{GL}(n, K)$ по ее центру $C(n, R)$, состоящему из скалярных матриц. Обозначим через $\widetilde{\varphi} : G \longrightarrow \mathrm{GL}(n, R)$ любой **подъем** φ т. е. такое *отображение*, что $\varphi(g) = \widetilde{\varphi}(g)C(n, R)$. Так как

$$\widetilde{\varphi}(hg)C(n, R) = \varphi(gh) = \varphi(h)\varphi(g) = \widetilde{\varphi}(h)C(n, R)\widetilde{\varphi}(g)C(n, R) = \widetilde{\varphi}(h)\widetilde{\varphi}(g)C(n, R),$$

то для любых $h, g \in G$ матрица $\widetilde{\varphi}(hg)$ лишь на скалярный множитель отличается от $\widetilde{\varphi}(h)\widetilde{\varphi}(g)$. Пусть, скажем, $\widetilde{\varphi}(hg) = a_{hg}\widetilde{\varphi}(h)\widetilde{\varphi}(g)$, где $a_{hg} \in K^*$. Одна из важнейших проблем теории представлений состоит в том, когда проективное представление поднимается до линейного, т. е. когда изменяя выбор представителей можно добиться того, чтобы $\widetilde{\varphi}$ было гомоморфизмом.

Задача. Найдите, какое условие на факторы a_{hg} накладывается ассоциативностью умножения в G. А теперь прочтите § 16 главы VIII.

§ 19♡. Линейные представления, 2nd instalment: разложимость и приводимость

Сейчас мы рассмотрим несколько важнейших классов представлений, которые как раз и были выделены Фробениусом в его работе 1896 года.

1. Прямая сумма представлений. Сейчас мы введем простейшую конструкцию над представлениями. Пусть $\varphi : G \longrightarrow \mathrm{GL}(m, R)$ и $\psi : G \longrightarrow \mathrm{GL}(n, R)$ — два представления одной и той же группы G над одним и тем же кольцом R, степеней m и n, соответственно. Тогда их прямая сумма $\varphi \oplus \psi$ есть представление степени $m + n$:

$$\varphi \oplus \psi : G \longrightarrow \mathrm{GL}(m + n, R), \qquad g \mapsto \varphi(g) \oplus \psi(g) = \begin{pmatrix} \varphi(g) & 0 \\ 0 & \psi(g) \end{pmatrix}.$$

Представление называется **неразложимым**, если его нельзя разложить в прямую сумму двух представлений, в противном случае оно называется **разложимым**. Напомним, что представления всегда рассматриваются с точностью до сопряженности в $\mathrm{GL}(n,R)$. Поэтому условие неразложимости означает, что не существует матрицы $x \in \mathrm{GL}(n,R)$, сопряжение при помощи которой одновременно приводит все матрицы из $\varphi(G)$ к одному и тому же клеточно-диагональному виду:

$$x\varphi(G)x^{-1} \leq \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$$

2. Неприводимые представления. Пусть теперь $R = K$ — поле. Введем важнейший класс представлений более узкий, чем класс неразложимых представлений. Представление $\varphi : G \longrightarrow \mathrm{GL}(n,K)$ называется **неприводимым**, если не существует такой матрицы $x \in \mathrm{GL}(n,R)$, чтобы все матрицы из $\varphi(G)$ одновременно приводились к (одному и тому же) клеточно-треугольному виду $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$. В противном случае представление называется **приводимым**. Представление, являющееся конечной прямой суммой неприводимых, называется **вполне приводимым**.

Из определения ясно, что каждое неприводимое представление неразложимо, но, как показывают элементарные примеры, обратное *безнадежно* неверно. Пусть, скажем, $p \in \mathbb{P}$, $G = \langle g \rangle \cong C_p$, а $K = \mathbb{F}_p$ — поле из p элементов. Уже встречавшееся нам в § 16 приводимое представление

$$G \longrightarrow \mathrm{GL}(2,K), \qquad g \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

неразложимо (в группе $\mathbb{F}_p^*$ нет элементов порядка p, и поэтому матрица порядка p не может быть диагонализована).

Пусть φ — приводимое представление группы G степени n. По определению найдется такое $x \in \mathrm{GL}(n,K)$, что все элементы $\varphi(g)$, $g \in G$, одновременно приводятся к одному и тому же *верхнему* клеточно-треугольному виду

$$x\varphi(g)x^{-1} = \begin{pmatrix} \psi(g) & * \\ 0 & \rho(g) \end{pmatrix},$$

где $\psi(g) \in \mathrm{GL}(m,K)$, а $\rho(g) \in \mathrm{GL}(n-m,K)$, для некоторого m, $1 \leq m \leq n-1$. Легко видеть, что ψ и ρ являются представлениями группы G степеней m и $n-m$, соответственно. При этом, как мы только

что заметили, в общем случае нельзя ожидать, чтобы все $*$ в правом верхем углу равнялись 0. Если этого все же можно добиться, то это, как раз, и будет значить, что представление φ является прямой суммой ψ и ρ, которые входят в него на равных правах.

В общем случае, однако, роль ψ и ρ совершенно разная. При этом ψ называется **подпредставлением** φ, а ρ — **фактор-представлением** φ. Как запомнить, кто есть кто? Ну, это будет ясно после чтения следующего параграфа. А пока постарайтесь понять, кто будет подпредставлением, а кто фактор-представлением, если все матрицы $\varphi(g)$ одновременно приведены к *нижнему* клеточно-треугольному виду:

$$x\varphi(g)x^{-1} = \begin{pmatrix} \psi(g) & 0 \\ * & \rho(g) \end{pmatrix}.$$

Если же всякое фактор-представление одновременно является подпредставлением, или, что то же самое, всякое неразложимое представление автоматически неприводимо (в сочетании с некоторыми условиями минимальности, гарантирующими выполнение теоремы Крулля—Ремака—Шмидта), то говорят о **полной приводимости**.

§ 20♣. Линейные представления, 3rd instalment: язык модулей

В 1929 году Эмми Нетер [194] объяснила нам, что на линейные представления можно смотреть иначе, а именно, как на модули над групповой алгеброй. Кстати, это именно та работа, где в полной общности сформулированы теоремы об изоморфизме. Кроме того, именно в этой замечательной статье введены понятия противоположного кольца, бимодуля, и многие другие и впервые обращено внимание на трудности, связанные с несепарабельностью расширения основного поля! Я думаю, что в смысле смены `парадигмы` — или, как сказала бы Масяня, `по любому` — это одна из 10 наиболее важных статей за всю историю алгебры.

Строго говоря, алгебраисты называют **линейным представлением** группы G гомоморфизм $G \longrightarrow \mathrm{GL}(V)$, где V — некоторый R-модуль, а $\mathrm{GL}(V) = \mathrm{Aut}_R(V)$ — группа его R-автоморфизмов. В этом случае говорят, что задано представление G **на** (`on`) V. Иными словами, это значит, что каждому $g \in G$ сопоставлен *обратимый R-линейный оператор* $\varphi_g : V \longrightarrow V$. Напомним (это понятие подробнейшим образом обсуждается в книге IV), что R-линейность означает, что

$$\varphi_g(u+v) = \varphi_g(u) + \varphi_g(v), \qquad \varphi_g(\lambda v) = \lambda\varphi_g(v),$$

для любых $g \in G$, $u, v \in V$ и $\lambda \in R$. Кроме того, сопоставление $g \mapsto \varphi_g$ является гомоморфизмом групп. Так как умножением операторов является композиция, это условие записывается в виде $\varphi_{hg}(v) = \varphi_h(\varphi_g(v))$ для любых $h, g \in G$, $v \in V$.

Буковку φ в этом контексте часто опускают и пишут просто gv вместо $\varphi_g(v)$. В этих обозначениях сформулированные только что условия запишутся следующим образом:

$$g(u+v) = gu + gv, \qquad g(\lambda v) = \lambda(gv), \qquad (hg)v = h(gv).$$

Не сформулированное явно, но подразумеваемое словом `обратимые`, условие означает, что $ev = v$. Таким образом, линейное представление — это не что иное, как действие $G \curvearrowright V$, но **линейное действие**. Линейность здесь подразумевает, что *для каждого* $g \in G$ сопоставление $v \mapsto gv$ является R-линейным. Произвольный R-модуль V вместе с *линейным* действием группы G называется **G-модулем**. Легко убедиться в том, что это *в точности* то же самое, что *левый* $R[G]$-модуль. В самом деле, зададим действие элемента $\sum a_g g$, где сумма берется по всем $g \in G$, а $a_g \in R$, причем только конечное число из них отлично от 0, на элементе $v \in V$ формулой

$$\sum a_g g \quad v = \sum a_g (gv).$$

Упражнение. Проверьте, что это умножение действительно превращает V в $R[G]$ модуль.

Теперь мы можем начать изучать линейные представления групп на таком языке, не выбирая базиса в V — в общем случае в V и нет никакого базиса! — и не рисуя никаких матриц. Например, R-подмодуль $U \leq V$ называется **G-подмодулем**, если $gu \in U$ для любых $g \in G$ и $u \in U$. На классическом языке G-подмодули называются **инвариантными подпространствами**. Такие понятия, как прямая сумма G-модулей, фактор-модуль и пр. определяются обычным образом. Естественным кандидатом на роль морфизма G-модуля U в G-модуль V является отображение $\theta : U \longrightarrow V$, которое одновременно R-линейно и G-эквивариантно:

$$\theta(u+v) = \theta(u) + \theta(v), \qquad \theta(\lambda u) = \lambda\theta(u), \qquad \theta(gu) = g\theta(u),$$

для любых $u, v \in U$, $\lambda \in R$ и $g \in G$. Такое отображение называется **G-гомоморфизмом** или, если группа G однозначно определяется из контекста, просто гомоморфизмом G-модулей. На этом языке многие понятия определяются значительно проще и естественнее, чем на языке матриц. Например, теперь неприводимости представления $\varphi : G \longrightarrow \mathrm{GL}(V)$ отвечает **простота** V. Напомним, что $V \neq 0$ называется простым, если в нем нет неочевидных G-подмодулей. Иными словами, если $U \leq V$ является G-подмодулем, то либо $U = 0$, либо $U = V$.

Если $V \cong R^n$ — *свободный модуль конечного ранга*, то $\mathrm{GL}(V) \cong \mathrm{GL}(n, R)$, так что линейное представление превращается в матричное. Вот короткий словарик, при помощи которого можно переводить с одного языка на другой.

представление	модуль
эквивалентность	изоморфизм
инвариантное подпространство,	
подпредставление	подмодуль
фактор-представление	фактор-модуль
неразложимое представление	неразложимый модуль
неприводимое представление	простой модуль
полная неприводимость	полупростота
сплетающий оператор	эквивариантное отображение

Таким образом, в этом случае — в частности, в наиболее важном для приложений случае конечномерных векторных пространств — язык матриц и язык модулей полностью эквивалентны, все что можно выразить на одном из них, можно выразить на другом. В действительности, начинающий должен как можно раньше научиться тому, чтобы *не задумываясь* осуществлять такой перевод. Конечно,

изоморфизм между $\mathrm{GL}(V)$ и $\mathrm{GL}(n,R)$ не является каноническим, а зависит от выбора базиса в V. Однако и для двух изоморфных G-модулей $U \cong V$ их изоморфизм тоже, как правило, не является каноническим!

Меланхолический комментарий. Авторы XIX века и натуралисты XX века, интересовавшиеся представлениями главным образом с какой-то целью, сразу выбирали базис и их работы роятся и кишат явно нарисованными матрицами. В противоположность этому более продвинутые литераторы-абстракционисты, трудившиеся в жанре искусства для искусства, блюдя моральную чистоту, вообще никаких матриц не рисовали. Это, как раз, совершенно понятно; труднее понять, почему дискуссия о том, чем является представление — частицей или волной — и сегодня продолжается в учебной литературе. С моей точки зрения сегодня любые разговоры о преимуществе языка автоморфизмов перед матричным — в тех случаях, когда оба они применимы — показывают серьезную задержку в умственном развитии: *che cartoni o non cartoni*! Та профессиональная теория представлений, которой сегодня занимаются профессиональные алгебраисты, это *неполупростая* теория, в которой все изменилось: и объекты, и методы, и задачи. Для нее эта дискуссия неактуальна, потому что эта теория уже несколько десятилетий оперирует не модулями, а комплексами. С другой стороны, в связи с появлением компьютеров для нас сейчас нет проблемы в том, чтобы выбрать базис, что-то посчитать, и снова перевести ответ на понятный нам геометрический язык. Конечно, большинство понятий *гораздо* удобнее *определять* на инвариантном языке модулей. Но когда нужно использовать представления по прямому назначению — для того, чтобы при помощи них что-то *вычислить* — тогда, конечно, любой самый оголтелый **перебурбакист*** выберет базис и будет считать как все. Однако противопоставление инвариантного языка координатному по своей содержательности напоминает дискуссию о том, кто был раньше, тупоконечники или остроконечники. Раньше были все — и сейчас тоже, нужно только видеть разницу не между инвариантным и базисным, а между безбрежностью математической мысли и ограниченностью языков, на которых она выражается: *безбрежности мечты с конечностью мо-*

*Перебурбакист так же относится к **бурбакисту**, как **передембель** к **дембелю**. Иными словами, перебурбакист это самый отпетый, разнузданный, наглый и отвязный бурбакист. Главной отличительной чертой перебурбакиста является полная сакральная серьезность. Поясним это следующим примером в духе Шинкарева. Написаные в бурбакистском духе книги Серра нарочито эффектны и часто затушевывают реальные трудности, с которыми столкнется читатель в попытке применить прочитанное к конкретной ситуации, но они основаны на подлинном, глубоком и всеобъемлющем понимании математики, а их стиль в значительной степени модерируется огромным талантом и культурой автора. При этом не следует забывать, что лекции в College de France не совсем то же самое (вариант: совсем не то же самое), что лекции даже в самом в лучшем регулярном университете. Многие места **Алгебры** Ленга (например, определение многочленов) эпатажно бурбакистские, но в данном случае это сделано абсолютно сознательно, как противовес гиперреалистическому стилю, свойственному преподаванию для американских undergraduates. С другой стороны действующие сегодня французские линейные учебники алгебры — как школьные, так и университетские — написаны перебурбакистски, с полным озверением и без тени юмора.

*рей**. Кроме того, меня всегда поражала неспособность некоторых людей видеть параллели и аналогии: они требуют инвариантности относительно замены базиса, но при этом почему-то совершенно не замечают, что точно такое же требование можно предъявить к замене языка!

§ 21♡. Линейные представления, 4^{th} instalment: представления конечных групп

В настоящем параграфе мы в духе непринужденной застольной болтовни расскажем *кое-что* о представлениях конечных групп, с тем, чтобы начинающий понимал о чем *примерно* идет речь, когда в главах 8–10 мы упоминаем, что какой-то результат о конечных группах доказывается с помощью теории представлений. Доказательства всех этих и многих других близких результатов приведены в книге IIbis.

1. Регулярное представление. Любая конечная группа G имеет привилегированное представление, содержащее в себе все неприводимые представления. А именно, пусть $V = R[G]$, по определению V представляет собой R-модуль ранга $|G|$. Группа G действует на V *слева* несколькими различными *естественными* способами. Отметим два из них:

• $g(\sum a_h h) = \sum a_h gh$. Получающийся при этом G-модуль V называется **левым регулярным представлением** группы G.

• $g(\sum a_h h) = \sum a_h hg^{-1}$. Получающийся при этом G-модуль V называется **правым регулярным представлением** группы G.

Обратите внимание на переход к обратному во втором из этих примеров! Это делается потому, что мы хотим построить *гомоморфизм* $G \longrightarrow \mathrm{GL}(n, R)$, а не просто какой-то там антигомоморфизм, см. по этому поводу главу VI. А теперь ответьте на следующий вопрос: левое и правое регулярное представление — это два *разных* представления или одно и то же? В дальнейшем регулярное представление группы G обозначается через reg_G.

Матерый (`mature`) читатель знает, как действует группа G в регулярном представлении, но вот начинающему полезно понять, как именно это представление выглядит в матрицах. Сделать это можно либо концептуально, либо формульно. Формула выглядит примерно так. Пусть $\delta = \delta_e : G \longrightarrow R$ — **дельта-функция**, сконцентрированная в $e \in G$. Напомним, что $\delta(g) = 1$, если $g = e$, и $\delta(g) = 0$ иначе (`otherwise`).

Задача. Докажите, что если $G = \{g_1, g_2, \dots, g_n\}$, то в базисе $g_1, \dots, g_n$ левое регулярное представление задается следующим образом:

$$g \mapsto \begin{pmatrix} \delta(g_1^{-1}gg_1) & \delta(g_1^{-1}gg_2) & \dots & \delta(g_1^{-1}gg_n) \\ \delta(g_2^{-1}gg_1) & \delta(g_2^{-1}gg_2) & \dots & \delta(g_2^{-1}gg_n) \\ \dots & \dots & \dots & \dots \\ \delta(g_n^{-1}gg_1) & \delta(g_n^{-1}gg_2) & \dots & \delta(g_n^{-1}gg_n) \end{pmatrix}$$

Напишите аналогичную формулу для правого регулярного представления.

---

*А вот оригинал: bercant notre infini sur le fini des mers.

А *на самом деле* происходит следующее. Группа G действует левыми/правыми трансляциями на себе. Это определяет *перестановочное* представление $G \longrightarrow S_n$. Сопоставляя каждой перестановке соответствующую матрицу перестановки, мы и получим левое/правое регулярное представление.

При чем здесь конечность группы, почему мы не можем сделать то же самое для любой группы G? Можем-то можем, но только получающееся при этом представление будет бесконечномерным!

2. Полная приводимость. Устоем классической теории представлений является следующий результат, доказанный Машке в 1898 году [195].

> **Генрих Машке** (`Heinrich Mashcke`, 24 октября 1853, Бреслау, ныне Вроцлав, — 1 марта 1908, Чикаго) — выдающийся американский математик немецкого происхождения. Машке учился в Гейдельберге, Берлине — где его учителями были Кронекер, Вейерштрасс и Куммер — и Геттингене, где он работал у Клейна. После этого он несколько лет преподавал в гимназии в Берлине, однако не смог найти постоянной университетской позиции и в 1981 году эмигрировал в США, где в 1892 году стал профессором университета Чикаго. Под влиянием Клейна Машке начал работать в области теории групп и дифференциальной геометрии. Сегодня Машке помнят главным образом благодаря теореме о полупростоте групповой алгебры.

Теорема Машке. *Пусть G — конечная группа, а K — поле характеристики p. Если p не делит $|G|$, то для представлений G над K неразложимость эквивалентна неприводимости.*

В частности, в этой ситуации *все* представления вполне приводимы! В случае, когда p не делит $|G|$ принято говорить об **обыкновенных представлениях**. Им противопоставляются **модулярные представления**, изучение которых было начато Рихардом Брауэром, т. е. представления над полем характеристики p, делящей $|G|$. Мы уже приводили примеры, показывающие, что для модулярных представлений утверждение теоремы становится безнадежно неверным. Например, у p-группы нет вообще никаких неприводимых представлений над полем характеристики p, кроме главного, в то время как у любой p-группы $G \neq 1$ всегда есть максимальные подгруппы и, значит, нетривиальные неразложимые представления.

3. Степени неприводимых представлений. Предположим теперь, что K алгебраически замкнутое поле, характеристика которого не делит порядок G. В качестве поля K заведомо можно взять, например, поле $\overline{\mathbb{Q}}$ алгебраических чисел или поле $\mathbb{C}$ комплексных чисел. Следующие результаты были в основном доказаны Фробениусом и Бернсайдом между 1896 и 1904 годами. Студенту, конечно, совершенно незачем запоминать, который из этих результатов называется второй теоремой Бернсайда, а который — семнадцатой теоремой Фробениуса. В лекциях ПОМИ-группе я обычно собираю весь этот комплекс утверждений в одну теорему под названием **теорема Бернсайда—Фробениуса** (может быть следовало бы добавить еще Шура, ведь утверждение о делимости опирается на его лемму) и потом лекции две ее доказываю.

• Количество различных неприводимых представлений равно количеству классов сопряженности группы G (**вторая теорема Бернсайда**).

В контексте теории колец следующие утверждения называются **теоремой Веддербарна**. Разумеется, Веддербарн доказал ее для *произвольного* основного поля, для случая поля $K = \mathbb{C}$, которым только и интересовались Фробениус и Бернсайд в данном контексте, этот результат был на другом языке доказан Молиным и Картаном.

• Каждое неприводимое представление конечной группы G входит в разложение reg_G в качестве прямого слагаемого с кратностью, равной его степени (Фробениус).

• Пусть теперь $\varphi_1, \ldots, \varphi_s$ суть все различные неприводимые представления группы G над полем K, а $n_1, \ldots, n_s$ — степени этих представлений. Тогда

$$|G| = n_1^2 + \ldots + n_s^2$$

(**первая теорема Бернсайда**).

А вот последний элемент, которого в сочетании с двумя предыдущими обычно достаточно, чтобы определить степени всех неприводимых представлений для небольших примеров.

• Если $H \trianglelefteq G$ — *абелев* нормальный делитель G, то степень n любого неприводимого представления группы G делит $|G : H|$. В частности, n делит $|G : C(G)|$. Часто достаточно даже того, что n делит $|G|$.

Скажем, в группе S_3 три класса сопряженных элементов. Поэтому у группы S_3 ровно три неприводимых комплексных представления, а их степени n_1, n_2, n_3 подчинены условию $n_1^2 + n_2^2 + n_3^2 = 6$. Ясно, что единственной возможностью является случай $n_1 = n_2 = 1$ и $n_3 = 2$. Разумеется, все эти представления нам уже известны, это главное представление, знак и представление S_3 как группы симметрий правильного треугольника (в матричном виде это представление изображено в § 12 главы 1).

4. Характеры. Фробениус ввел специальный инструмент, позволяющий не различать эквивалентные представления. А именно, **характером** представления $\varphi : G \longrightarrow \mathrm{GL}(n, R)$ называется функция $\chi_\varphi : G \longrightarrow R$, $g \mapsto \mathrm{tr}(\varphi_g)$. Ясно, что характер является **центральной функцией**, т. е. постоянен на классах сопряженных элементов. Характер неприводимого представления называется **неприводимым характером**.

Следующий результат объясняет, что для *конечных* групп над полем характеристики 0 вместо классов эквивалентности представлений можно говорить о характерах. Разумеется, в классической теории так и поступают.

Теорема. *Если G — конечная группа, а K — поле характеристики 0, то*

$$\varphi \sim \psi \quad \Longleftrightarrow \quad \chi_\varphi = \chi_\psi.$$

Пусть теперь K — алгебраически замкнутое поле характеристки 0. В этом случае число различных неприводимых характеров равно числу классов сопряженности группы G, которое, в свою очередь, равно размерности пространства центральных функций на G. Совпадение двух чисел редко бывает случайным. Игорь Френкель учит даже, что совпадение *никогда* не бывает случайным: COINCIDENCES SHOULDN'T BE TAKEN LIGHTLY — К СОВПАДЕНИЯМ НУЖНО ОТНОСИТЬСЯ ВСЕРЬЕЗ.

И действительно, Фробениус доказал, что в этом случае неприводимые характеры образуют базис пространства центральных функций. На этом, в сочетании с различными уравнениями, связывающими значения неприводимых характеров (соотношения ортогональности и т. д.) вкупе с арифметическими условиями на эти значения (целочисленность, делимость и т. д.) как раз и основаны небанальные приложения теории представлений в теории конечных групп. Например, пользуясь этими условиями часто удается строить в группе G нетривиальные нормальные подгруппы (как ядра неприводимых представлений). Именно так и доказываются теорема Фробениуса о нормальном дополнении и pq-теорема Бернсайда.

5. Метафилософия теории представлений. Что здесь происходит, зачем это нужно и почему кольцо R с самого начала предполагалось коммутативным? Большинство приложений теории линейных представлений — в полной мере это относится к ее применениям в теории конечных групп! — основано на том, что представления прячут тривиальную часть группы G (абелевы нормальные делители) в кольцо R, выставляя интересные неабелевы части группы для пристального рассмотрения. С этой точки зрения представление может скрыть слишком много — либо, наоборот, недостаточно. Некоммутативные кольца сразу отбраковываются тем, что для них мультипликативная группа может иметь сколь угодно сложное строение и мы ничего не выигрываем в смысле вычислений. Например, любая группа G вкладывается в мультипликативную группу своего группового кольца $R = \mathbb{Z}[G]$, и, значит, над некоммутативными кольцами имеет точное представление степени один! С другой стороны мультипликативная группа коммутативных колец устроена не слишком сложно. Например, если предположить, как это обычно делается, что R является областью целостности, то любая конечная подгруппа в R^* циклическая (этот результат и его обобщения в различных направлениях подробно обсуждаются в книге III). В частности, это относится к случаю, когда $R = K$ поле. Поэтому представления над полем заведомо прячут не слишком много. Проблема, однако, состоит в том, что *произвольное* поле прячет недостаточно, и поэтому изучение представлений группы над таким полем может быть все еще не проще, чем вычисления в самой этой группе. Дело в том, что в нем может быть слишком мало корней из 1, чтобы вместить произвольную циклическую группу. Поэтому, если мы хотим зафиксировать одно и то же поле K для *всех* конечных групп, то уместно предположить, что оно содержит корни *всех* степеней из 1 в нужном количестве. Алгебраически замкнутое поле характеристики 0 заведомо удовлетворяет этому условию. Как мы узнаем в книге III, поле $\mathbb{C}$ как раз и определяется как *единственное* алгебраически замкнутое поле характеристики 0 (и мощности континуум). Именно поэтому классически представления конечных групп изучались именно над полем $\mathbb{C}$. С другой стороны, поля характеристики $p > 0$ делают видимым строение всей силовской p-подгруппы и поэтому изучение модулярных представлений дает *гораздо* больше информации о строении группы G, чем изучение ее представлений над $\mathbb{C}$. Точно так же, чем меньше корней из 1 в поле K, например, если $K = \mathbb{Q}$, тем большая часть абелевых подгрупп переводится из скрытой формы в явную. В еще большей степени это относится к представлениям над $\mathbb{Z}$. Поэтому начиная с 1939 года теория представлений конечных групп развивалась в первую очередь как теория модулярных и целочисленных представлений. Но в отличие от классической теории здесь нет свойства полной приводимости, в связи с чем нужно переосмыслить всю проблематику теории представлений. Например, в неполупростой теории неприводимые представления утрачивают свою

центральную роль. Их классификация по-прежнему является очень важным шагом в понимании представлений группы G. Однако теперь от этого шага бесконечно далеко до решения подлинной задачи теории представлений, классификации *неразложимых* представлений!

§ 22♣. Эндоморфизмы аддитивной группы поля

Для любого кольца R гомотетия $\theta_c : R \longrightarrow R$, $x \mapsto cx$, с коэффициентом $c \in R$ является эндоморфизмом аддитивной группы R^+. В самом деле, $\theta_c(x+y) = c(x+y) = cx + cy = \theta_c(x) + \theta_c(y)$ — это просто закон дистрибутивности. Существуют ли другие эндоморфизмы R^+?

1. Автоморфизмы $\mathbb{Q}^+$. Легко видеть, что $\mathrm{End}(\mathbb{Z}^+) \cong \mathbb{Z}$.

Задача. Убедитесь, что $\mathrm{End}(\mathbb{Q}^+) \cong \mathbb{Q}$.

Решение. Пусть φ — эндоморфизм $\mathbb{Q}^+$, $\varphi(1) = c \in \mathbb{Q}$. Покажем, что тогда $\varphi(x) = cx$ для всех $x \in \mathbb{Q}$. В самом деле, для любого $m \in \mathbb{Z}$ имеем $\varphi(m) = m\varphi(1) = cm$. Кроме того, для любого $n \in \mathbb{Z}$, выполняется $n\varphi(m/n) = \varphi(n \cdot m/n) = \varphi(m) = cm$, так что действительно $\varphi(m/n) = c(m/n)$.

Мы уже знали, что $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q}) = \mathbb{Q}$, решение задачи состояло в том, что мы заметили, что любой эндоморфизм $\mathbb{Q}$ полностью определяется своим ограничением на $\mathbb{Z}$.

Следствие 1. $\mathrm{Aut}(\mathbb{Q}^+) = \mathbb{Q}^*$.

Следствие 2. *Две подгруппы $A, B \leq \mathbb{Q}^+$ тогда и только тогда изоморфны, когда найдется $x \in \mathbb{Q}^*$ такое, что $A = xB$.*

Легко видеть, что аддитивные подгруппы в $\mathbb{Q}$ устроены так. Для каждого простого зададим $m_p \in \mathbb{Z} \cup \{\pm\infty\}$:

$$A = \{x \in \mathbb{Q}^+ \mid \forall p \in \mathbb{P}, v_p(x) \geq m_p\}.$$

Таким образом, имеется континуум классов изоморфизма аддитивных подгрупп в $\mathbb{Q}^+$.

2. Непрерывные автоморфизмы $\mathbb{R}^+$. Вопрос о существовании у группы $\mathbb{R}^+$ автоморфизма, не являющегося гомотетией, поставленный в начале XIX века Коши, решил лишь Гамель в 1905 году [196]. Гамель построил чертову прорву таких автоморфизмов. Его подход основан на том, что как аддитивные группы $\mathbb{R}$ и $\mathbb{R}^n$ изоморфны, а у $\mathbb{R}^n$ при $n \geq 2$, море автоморфизмов. Разумеется, построение изоморфизма между

Георг Гамель (Georg Karl Wilhelm Hamel, 12 сентября 1877, Дюрен — 4 октября 1954, Ландсхут) — замечательный немецкий математик, основные работы которого относятся к геометрии, теории функций, теории дифференциальных уравнений, гидродинамике, основаниям математики и криптографии. Однако, сегодня его вспоминают главным образом именно в связи с работой 1905 года, в которой аксиома выбора использована для построения базиса Гамеля.

В 1897 Гамель поступил в Берлинский университет, а через 3 года продолжил обучение в Геттингене и в 1901 году защитил диссертацию под руководством Гильберта. Уже через год он получил хабилитацию в TU Карлсруэ и после этого работал в TU Брюнн, RWTH Аахен и TU Шарлоттенбург (Берлин). Гамель придерживался право-националистических взглядов, и в 30-е годы пришел к прямой поддержке нацизма, хотя и несколько менее радикальной, чем Бибербах, Тейхмюллер или Витт.

$\mathbb{R}$ и $\mathbb{R}^n$ зависит от аксиомы выбора, кроме того, такой изоморфизм заведомо не может быть непрерывным.

Теорема Коши. *Гомотетии $\theta_c : \mathbb{R}^+ \longrightarrow \mathbb{R}^+$, $x \mapsto cx$, где $c \in \mathbb{R}$, являются единственными* **непрерывными** *эндоморфизмами $\mathbb{R}^+$.*

Так как группа $\mathbb{R}_{>0}$ изоморфна $\mathbb{R}^+$, причем взаимно обратные изоморфизмы задаются отображениями $x \mapsto \ln(x)$ и $x \mapsto e^x$, соответственно, то эту теорему можно сформулировать еще любым из трех следующих **эквивалентных** образов. Эти результаты, собственно, и объясняют, почему в школьном курсе принято рассматривать степенные, показательные и логарифмические функции — никаких других гомоморфизмов между аддитивными и мультипликативными структурами на $\mathbb{R}$ построить невозможно[♮].

Следствие 1. *Отображения $\mathbb{R}_{>0} \longrightarrow \mathbb{R}_{>0}$, $x \mapsto x^c$, где $c \in \mathbb{R}$, являются единственными* **непрерывными** *эндоморфизмами $\mathbb{R}_{>0}$.*

Следствие 2. *Отображения $\mathbb{R}^+ \longrightarrow \mathbb{R}^*$, $x \mapsto c^x$, где $c \in \mathbb{R}_{>0}$, являются единственными* **непрерывными** *гомоморфизмами $\mathbb{R}^+$ в $\mathbb{R}^*$.*

Следствие 3. *Отображения $\mathbb{R}_{>0} \longrightarrow \mathbb{R}^+$, $x \mapsto \log_c(x)$, где $c \in \mathbb{R}_{>0}$, $c \neq 1$, являются единственными* **непрерывными** *гомоморфизмами $\mathbb{R}_{>0}$ в $\mathbb{R}^+$.*

В книжке Фихтенгольца все эти четыре утверждения трактуются как независимые теоремы, с четырьмя разными (не слишком короткими) доказательствами! Применяя эти результаты к фактор-группе $\mathbb{T} \cong \mathbb{R}/\mathbb{Z}$, мы получаем еще такие следствия. Разумеется, как обычно, операция в $\mathbb{T}$ записывается мультипликативно.

[♮]Разумеется, они существуют, вот только **построить** их невозможно!

Следствие 5. *Отображения* $\mathbb{R}^+ \longrightarrow \mathbb{T}$, $x \mapsto e^{icx}$, *где* $c \in \mathbb{R}$, *являются единственными* **непрерывными** *гомоморфизмами* $\mathbb{R}^+$ *в* $\mathbb{T}$.

Следствие 6. *Отображения* $\mathbb{T} \longrightarrow \mathbb{T}$, $x \mapsto x^n$, *где* $n \in \mathbb{Z}$, *являются единственными* **непрерывными** *эндоморфизмами* $\mathbb{T}$.

А что Вы можете сказать о гомоморфизмах $\mathbb{T}$ в $\mathbb{R}^+$?

3. Полиномиальные автоморфизмы K^+. Над произвольным полем нельзя говорить о непрерывности, но можно спросить себя, каковы **полиномиальные** гомоморфизмы $K^+ \longrightarrow K^+$ и $K^* \longrightarrow K^*$? Иными словами, предлагается найти все **многочлены** $f \in K[x]$ такие, что $f(x+y) = f(x) + f(y)$ или, соответственно, $f(xy) = f(x)f(y)$. В этом утверждении содержится некоторая двусмысленность: как следует понимать равенство $f(xy) = f(x)f(y)$ — **функционально**, т. е. как совпадение значений $f(ab) = f(a)f(b)$ для любых $a, b \in K$ или **формально**, как равенство многочленов в $K[x, y]$? Впрочем, как мы узнаем в книге III, если поле K бесконечно, этого вопроса не возникает (теорема о формальном и функциональном равенстве, принцип несущественности алгебраических неравенств). Следующий результат моментально вытекает также из леммы Дедекинда—Артина, которую мы доказываем в книге IV, так что речь здесь идет о линейной зависимости.

Задача. Докажите, что если K бесконечное поле, а $f \in K[x]$ — многочлен такой, что $f(ab) = f(a)f(b)$ для любых $a, b \in K$, то $f = x^n$.

Решение. По только что помянутому принципу несущественности алгебраических неравенств многочлены $f(xy)$ и $f(x)f(y)$ совпадают как элементы $K[x, y]$. Пусть $f = a_n x^n + \ldots + a_1 x + a_0$. Сравнивая коэффициенты при $x^n y^n$ мы видим, что $a_n = 1$, а сравнивая коэффициенты при $x^n y^i$, $i = 0, \ldots, n-1$, получаем $a_n a_i = 0$.

Как показывает пример $x^3 + x^2 + x \in \mathbb{F}_2[x]$, для конечного поля это утверждение не имеет места.

§ 23♣. Линейные представления, 5th instalment: рациональные представления

> Personally, following the value scheme of my teacher Claude Chevalley, I rank Cartan and Weyl as the two greatest mathematicians of the first half of the twentieth century.
>
> John Coleman. [197]

Типичным примером групп типа Ли является сама группа $G = \mathrm{GL}(n, R)$. Фактически значительная часть полилинейной алгебры как

раз и состоит в изучении представлений группы $\mathrm{GL}(n,R)$. Именно с этой целью вводятся линейные функционалы, поливекторы, тензоры и т. д. Вот несколько простейших примеров.

• Отображение $G \longrightarrow \mathrm{GL}(n,R)$, $g \mapsto g$, называется **естественным**, **натуральным** или **векторным** представлением.

• Отображение $G \longrightarrow \mathrm{GL}(n,R)$, $g \mapsto (g^t)^{-1}$, называется **двойственным естественному** или **ковекторным** представлением.

• Отображение $G \longrightarrow \mathrm{GL}(\binom{n}{m},R)$, $g \mapsto \bigwedge^m(g)$, называется **внешней степенью** естественного представления или **поливекторным** представлением.

• Отображение $G \longrightarrow \mathrm{GL}(\binom{n+m-1}{n},R)$, $g \mapsto S^m(g)$, называется **симметрической степенью** естественного представления

Все перечисленные представления **полиномиальны** в том смысле, что все их матричные элементы являются многочленами относительно коэффициентов матрицы g. Иными словами, каждый $\varphi_{ij}(g)$, $1 \le i,j \le t$, выражается как многочлен относительно $g_{11},\dots,g_{nn}$. А вот еще один пример:

• Отображение $G \longrightarrow \mathrm{GL}(n^2,R)$, $g \mapsto \mathrm{Ad}_g$, где Ad_g есть матрица линейного преобразования $M(n,R) \longrightarrow M(n,R)$, $x \mapsto gxg^{-1}$, называется **присоединенным представлением**.

Для того, чтобы это представление стало гомоморфизмом именно в $\mathrm{GL}(n^2,R)$, а не просто в $\mathrm{GL}(M(n,R))$, в кольце матриц нужно еще, конечно, выбрать базис над R. Обычно в $M(n,R)$ выбирается базис, состоящий из стандартных матричных единиц, e_{ij}, $1 \le i,j \le n$. Например, в $M(2,R)$ этот базис состоит из

$$e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad e_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Задача. Докажите, что в базисе $e_{11}, e_{12}, e_{21}, e_{22}$ присоединенное представление задается следующим образом:

$$\mathrm{Ad}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \frac{1}{ad-bc}\begin{pmatrix} ad & -ac & bd & -bc \\ -ab & a^2 & -b^2 & ba \\ cd & -c^2 & d^2 & -cd \\ -bc & ac & -bd & ad \end{pmatrix}.$$

Проверьте, что это сопоставление действительно определяет гомоморфизм $\mathrm{GL}(2,R) \longrightarrow \mathrm{GL}(4,R)$. Посмотрите на матрицу в правой части, угадайте `паттерн` и обобщите ответ на случай произвольного n.

Разумеется, я не утверждаю, что такой выбор базиса действительно является правильным с точки зрения изучения присоединенного представления! Более того, он совершенно неправильный — и вот почему.

Задача. Пусть $2 \in R^*$. Найдите, как выглядит матрица Ad_g в базисе $e_{12}, e_{11}-e_{22}, e_{21}, e=e_{11}+e_{22}$.

Если мы посмотрим на матричные элементы присоединенного представления, то увидим, что они являются не многочленами, а рациональными функциями относительно элементов g_{ij}. Более того, знаменатель этих рациональных функций обратим для всех элементов $g \in \mathrm{GL}(n,R)$. Такие представления принято называть **рациональными**. В действительности, матричные элементы рациональных представлений тоже многочлены, но многочлены не от n^2 переменных, а от n^2+1 переменной. А именно, профессиональные алгебраисты полагают, что в описании матрицы из $\mathrm{GL}(n,K)$ участвуют не n^2 параметров, как считают широкие неумытые массы, а n^2+1 параметров: коэффициенты $g_{11},\dots,g_{nn}$ и величина $y=1/\det(g)$ обратная к определителю.

2. Конечномерные представления $\mathrm{GL}(n,K)$**.** В случае поля K характеристики 0 полиномиальные представления $\mathrm{GL}(n,K)$ полностью классифицируются **теорией Картана-Вейля**, которую можно выражать либо на классическом языке (тензоры, диаграммы Юнга), либо на лиевском языке (корни, веса, модули со старшим весом). В середине 1950-х годов Клод Шевалле к *огромному* изумлению окружающих обнаружил, что часть этой теории, относящаяся к параметризации *неприводимых* представлений, продолжает оставаться верной в произвольной характеристике! Иными словами, в **теории Шевалле** из любого неприводимого рационального представления $\mathrm{GL}(n,\mathbb{C})$ регулярным образом изготавливается единственное неприводимое рациональное представление $\mathrm{GL}(n,K)$ над любым полем K, может быть слегка меньшей размерности. Теории Картана—Вейля и Шевалле являются несомненными вершинами математики XX века и лежат в основе громадного числа приложений и в самой математике и в физике. Кроме того, они послужили образцом для многочисленных обобщений и подражаний. Основные результаты этих теорий также доказываются в книге IIB.

В этом месте у начинающего может возникнуть устойчивая иллюзия, что у группы $\mathrm{GL}(n,R)$ вообще не существует никаких представлений, кроме рациональных. Esistono, e come!

• Пусть $\varphi : K \longrightarrow L$ — гомоморфизм полей. Тогда отображение $\mathrm{GL}(n,K) \longrightarrow \mathrm{GL}(n,L)$, $g \mapsto (\varphi(g_{ij}))$, является представлением группы $\mathrm{GL}(n,K)$.

Для того, чтобы это представление было полиномиальным, необходимо, чтобы само φ задавалось многочленом! Но, как мы узнали в предыдущем параграфе, уже у мультипликативной группы бесконечного поля K нет никаких эндоморфизмов, кроме $x \mapsto x^n$. Однако при $n \geq 2$ возведение в n-ю степень очень редко является аддитивным гомоморфизмом. Иными словами, трудно ожидать, что для любых $x,y \in K$ выполняется равенство $(x+y)^n = x^n + y^n$. В действительности, никаких полиномиальных гомоморфизмов полей, кроме тех, которые получаются как композиция степени эндоморфизма Фробениуса с последующим вложением, и не суще-

ствует. Поэтому, например, у поля характеристики 0 нет вообще никаких полиномиальных автоморфизмов, кроме тождественного. Разумеется, в случае конечного поля полиномиальность не накладывает практически никакого ограничения. Однако в случае, когда поле K бесконечно, замечательная **теорема Бореля—Титса** утверждает, что никаких других *конечномерных* представлений, кроме тех, которые получаются композиции полиномиальных, у $\mathrm{GL}(n, K)$ по существу нет. `По существу` здесь следует понимать примерно так: если представление разложено в тензорное произведение, то разные сомножители могут быть подкручены *разными* полевыми гомоморфизмами. С другой стороны, изучение бесконечномерных представлений является наукой уже абсолютно другого порядка. Ни о какой подобной классификации бесконечномерных представлений без каких-нибудь условий топологического характера, не может быть и речи.

§ 24◇. Ряды подгрупп

1. Нормальные и субнормальные ряды. Упорядоченную по включению *цепочку* подгрупп группы G

$$1 = G_0 \leq G_1 \leq \ldots \leq G_{n-1} \leq G_n = G$$

в теории групп чаще всего называют **рядом подгрупп** (`series`, `Reihe`), при этом G_i называются **членами** этого ряда, а n — **длиной** ряда. Если все включения $G_{i-1} < G_i$ являются строгими, то такой ряд называется **рядом без повторений**, в противном случае — **рядом с повторениями**. Чаще всего мы будем иметь дело с рядами подгрупп следующих трех типов:

• Ряд подгрупп, все члены которого нормальны в G, называется **нормальным** (`normal series`). Таким образом, для нормального ряда $G_i \trianglelefteq G$ для всех i.

• Ряд подгрупп называется **субнормальным** (`subnormal series`), если выполняется более слабое условие $G_{i-1} \trianglelefteq G_i$ для всех $i \geq 1$.

Условие субнормальности гарантирует, что каждый член ряда нормален в следующем — но, вообще говоря, не во всей группе G! В частности, субнормальный ряд состоит из субнормальных подгрупп. Обратное, конечно, неверно: не любой ряд, состоящий из субнормальных подгрупп, субнормален.

• Ряд подгрупп, состоящий из (вполне) характеристических подгрупп называется **(вполне) характеристическим**.

Терминологический комментарий. Начинающий должен иметь в виду, что для обозначения `цепочки` подобъектов в различных алгебраических теориях традиционно используются *разные* термины. Это вопрос устоявшихся привычек, от которых никто не собирается отказываться. Так, в теории колец говорят о **цепочках идеалов** (`chain`, `Kette`), в то время как в теории Галуа — о **башнях полей**

(`tower`, `Turm`). Кстати, в некоторых контекстах, этот термин выжил и в теории групп, например, в главе IX нам встретятся **`силовские башни`**. С другой стороны, в линейной алгебре, теории представлений, дифференциальной, алгебраической и комбинаторной геометрии говорят как о **рядах подмодулей**, так и о **флагах подпространств**. Чудовищная неразбериха создается тем, что в некоторых старых книгах **нормальным рядом** называется то, что мы называем *субнормальным* рядом, в этом случае то, что мы называем *нормальным* рядом, называется **инвариантным рядом**. Однако эта доморощенная терминология — опирающаяся на полностью вышедший из употребления термин **инвариантная подгруппа** — представляется мне абсолютно чудовищной, так как в этом случае членами *нормального* ряда оказываются *субнормальные* подгруппы! Проблема усугублялась тем, что английское **`normal series`** случайным образом переводилось то как **`нормальный ряд`**, то как **`инвариантный ряд`**. Например, я помню свою полную растерянность, когда в двух разных книгах — а может и в одной и той же книге! — встретил два *абсолютно идентичных* определения, одно из которых, *по мнению автора*, определяло композиционный ряд, а другое — главный. Разумеется, дело здесь в том, что авторы этих книг по разному понимали выражение **`нормальный ряд`**, забыв предупредить об этом читателя, так как каждый из них считал свою терминологию единственно возможной! Кроме того, следует иметь в виду, что многие авторы называют **`длиной`** ряда количество *строгих* включений между подгруппами G_i, иными словами, количество *различных* подгрупп G_i, $i \geq 1$. Однако для наиболее важного случая рядов без повторений это определение совпадает с нашим.

Пусть

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_{n-1} \trianglelefteq G_n = G$$

субнормальный ряд. Фактор-группы G_i/G_{i-1} называются **факторами** этого ряда. *Нормальный* ряд называется **центральным**, если все его факторы *центральны*, т. е., иными словами, $G_i/G_{i-1} \leq C(G/C_{i-1})$.

Выше мы нумеровали ряд подгрупп как *возрастающий*. В действительности, во многих ситуациях значительно удобнее пользоваться **убывающими рядами подгрупп**:

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_{n-1} \trianglerighteq G_n = 1.$$

Обычно мы говорим просто о ряде подгрупп, при этом из контекста ясно, рассматривается ли он как возрастающий или убывающий.

2. Неуплотняемые ряды. Ряд подгрупп

$$1 = H_0 \leq H_1 \leq \ldots \leq H_{n-1} \leq H_m = G$$

называется **уплотнением** (`refinement, Verfeinerung`) ряда

$$1 = G_0 \leq G_1 \leq \ldots \leq G_{n-1} \leq G_n = G$$

если каждая подгруппа G_i совпадает с какой-то подгруппой H_j. Ряд называется **неуплотняемым**, если $G_i \neq G_{i+1}$ для всех i, причем каждая G_i является максимальной нормальной подгруппой в G_{i+1}. Неуплотняемые ряды без повторений играют центральную роль в теории конечных групп и имеют специальные названия.

• Неуплотняемый субнормальный ряд с различными членами называется **композиционным** рядом группы G. Факторы композиционного ряда называются **композиционными факторами** группы G.

• Неуплотняемый нормальный ряд с различными членами называется **главным**. Факторы главного ряда называются **главными факторами** группы G.

Отметим, что для абелевых групп — в частности, для модулей — понятия главного и композиционного ряда совпадают. В действительности, обобщением понятия композиционного ряда модуля является именно понятие главного

Из теоремы Жордана—Гельдера, которую мы докажем в двух следующих параграфах, будет следовать, что композиционный/главный ряд имеет наибольшую возможную длину среди всех субнормальных/-нормальных рядов с различными членами.

Задача. Композиционные факторы являются *простыми* группами. Что можно сказать про главные факторы?

Задача. Докажите, что абелева группа в том и только том случае имеет композиционный ряд, когда она конечна.

Например, группа рациональных чисел вообще не имеет максимальных нормальных делителей. Однако обычное рассуждение на тему `sowohl artinsch als auch noethersch`, известное как **качели Артина—Нетер**, показывает, что для групп, удовлетворяющих подходящим условиям максимальности и минимальности, композиционные и главные ряды обязаны существовать.

Теорема. *Группа G тогда и только тогда обладает главным рядом, когда она удовлетворяет условиям* `ACC` *и* `DCC` *для нормальных подгрупп.*

Доказательство. Мы проведем здесь только доказательство существования главного ряда, обратное утверждение следует из теоремы Жордана—Гельдера.

По условию минимальности для нормальных подгрупп в G найдется минимальная нормальная подгруппа G_1. Теперь, снова по тому же условию в G найдется минимальная подгруппа G_2 среди нормальных подгрупп, строго содержащих G_1. Продолжая действовать

таким образом, мы построим строго возрастающий нормальный ряд $1 = G_0 \lhd G_1 \lhd G_2 \lhd \dots$ В силу условия максимальности для нормальных подгрупп этот ряд обязан оборваться, причем оборваться он может только на главном ряде.

Доказательство существования композиционного ряда проводится точно так же, причем для разнообразия мы проведем его не в форме Артина—Нетер, а в двойственной форме Нетер—Артина.

Теорема bis. *Группа G, удовлетворяющая условиям* `ACC` *и* `DCC`*, обладает композиционным рядом.*

Доказательство. По условию максимальности в G найдется максимальная нормальная подгруппа G_1. Теперь, снова по тому же условию, в G_1 найдется максимальная нормальная подгруппа G_2, строго содержащаяся в G_1. Обратите внимание, что по сравнению с предыдущим доказательством слово `нормальная` переползло здесь в другое место! А именно, условие максимальности примененно здесь к множеству всех нормальных подгрупп в G_1 — но они совсем не обязаны оставаться нормальными в G. Это значит, что если условие максимальности для всех подгрупп и слишком сильно для наших целей, то условия максимальности для нормальных подгрупп может оказаться недостаточно — в действительности, нужно что-то вроде условия максимальности для субнормальных подгрупп, но, конечно, мы не будем заниматься глупостями такого рода (Курош, § 16). Продолжая действовать таким образом, мы построим строго убывающий субнормальный ряд $G = G_0 \rhd G_1 \rhd G_2 \rhd \dots$ В силу условия минимальности (для субнормальных подгрупп) этот ряд обязан оборваться, причем оборваться он может только на композиционном ряде.

Чаще всего мы будем использовать эти теоремы в такой форме.

Следствие. *Каждая конечная группа G имеет композиционный ряд и главный ряд.*

Мы уже видели, что группы $\mathbb{Z}$, μ_{p^∞} и $\mathbb{Q}$ не имеют композиционных рядов.

§ 25♠. Лемма Цассенхауза и Verfeinerungssatz Шрайера

Следующий важный результат был доказан Гансом Цассенхаузом в 1934 году [198]. Он известен как **лемма Цассенхауза**, **лемма о бабочке** или, полностью, **лемма Цассенхауза о бабочке**. Почему? Для этого нужно нарисовать диаграмму Хассе всех фигурирующих в доказательстве подгрупп и посмотреть на получившуюся картинку.

Лемма о бабочке. *Пусть $F \trianglelefteq F^*$, $H \trianglelefteq H^*$ четыре подгруппы группы G. Тогда $F(F^* \cap H) \trianglelefteq F(F^* \cap H^*)$, $H(F \cap H^*) \trianglelefteq H(F^* \cap H^*)$, и имеет место изоморфизм*

$$F(F^* \cap H^*)/F(F^* \cap H) \cong H(F^* \cap H^*)/H(F \cap H^*).$$

Доказательство. Ясно, что $F^* \cap H \trianglelefteq F^* \cap H^*$ и $F \cap H^* \trianglelefteq F^* \cap H^*$. Отсюда следует, что $(F \cap H^*)(F^* \cap H) \trianglelefteq F^* \cap H^*$. Легко видеть, что $F(F^* \cap H)(F^* \cap H^*) = F(F^* \cap H^*)$ и $F(F^* \cap H) \cap (F^* \cap H^*) = (F \cap H^*)(F^* \cap H)$. Таким образом по теореме об изоморфизме,

$$F(F^* \cap H^*)/F(F^* \cap H) \cong (F^* \cap H^*)/(F \cap H^*)(F^* \cap H).$$

Совершенно аналогично мы убеждаемся в том, что, $H(F \cap H^*)(F^* \cap H^*) = H(F^* \cap H^*)$ и $H(F \cap H^*) \cap (F^* \cap H^*) = (F \cap H^*)(F^* \cap H)$. Снова применяя теорему об изоморфизме, получаем

$$H(F^* \cap H^*)/H(F \cap H^*) \cong (F^* \cap H^*)/(F \cap H^*)(F^* \cap H).$$

Сравнение двух этих изоморфизмов и доказывает лемму.

Следующий результат был доказан Отто Шрайером в 1928 году [199] но, конечно, мы приводим более позднее доказательство, основано на лемме Цассенхауза.

Теорема Шрайера об уплотнении. *Любые два субнормальных ряда подгрупп обладают эквивалентными субнормальными уплотнениями.*

Доказательство. В самом деле, пусть

$$1 = F_0 \leq F_1 \leq \ldots \leq F_m = G, \qquad 1 = H_0 \leq H_1 \leq \ldots \leq H_n = G,$$

Произведем вставки в F следующим образом. Уплотним $F_i \leq F_{i+1}$, пересекая все члены второго ряда с F_{i+1} и домножая их на F_i. При этом получится сегмент вида

$$F_1 = F_{i0} \leq F_{i1} \leq \ldots \leq F_{in} = F_{i+1},$$

где $F_{ij} = (F_{i+1} \cap H_j)F_i$. Аналогичным образом уплотним первый ряд

$$H_j = H_{j0} \leq H_{j1} \leq \ldots \leq H_{jm} = H_{j+1},$$

где $H_{ji} = (H_{j+1} \cap F_i)H_j$. Легко видеть, что из леммы Цассенхауза вытекает

$$F_{i,j+1}/F_{ij} \cong (F_{i+1} \cap H_{j+1})F_i/(F_{i+1} \cap H_j)F_i \cong$$
$$(F_{i+1} \cap H_{j+1})H_j/(H_{j+1} \cap F_i)H_j \cong H_{j,i+1}/H_{ji}.$$

Это и значит, что нам удалось построить эквивалентные уплотнения.

§ 26♠. Теорема Жордана—Гельдера

В этом параграфе мы докажем, что каждая конечная группа может быть собрана из простых кусков, причем классы изоморфизма этих кусков и их кратности не зависят способа сборки.

1. Теорема Жордана—Гельдера для композиционных рядов. Совпадение *порядков* факторов композиционного ряда доказал Жордан в 1869 году [200]. В действительности же это утверждение высказал (без намека на доказательство, но как твердо установленный факт) еще Галуа! Изоморфность факторов установил Гельдер в 1889 году [201]. Впрочем, трудно ожидать, что кто-то мог доказать — или даже сформулировать — утверждение об изоморфизме факторов до того, как Гельдер ввел понятие фактор-группы!

Теорема Жордана—Гельдера. *Если группа G имеет композиционный ряд, то набор его факторов не зависит от выбора композиционного ряда.*

Иными словами, утверждается, что любые два композиционных ряда имеют одинаковую длину и что после подходящей перестановки соответствующие факторы изоморфны.

Доказательство. В самом деле, пусть

$$1 = F_0 \leq F_1 \leq \ldots \leq F_m = G, \qquad 1 = H_0 \leq H_1 \leq \ldots \leq H_n = G,$$

два композиционных ряда группы G. По теореме Шрайера у них есть эквивалентные уплотнения. Но так как композиционный ряд — это неуплотняемый субнормальный ряд, любое его уплотнение состоит в повторении членов. Это значит, что уже сами рассматриваемые ряды эквивалентны.

Таким образом, если $1 = G_0 < G_1 < \ldots < G_n = G$ — композиционный ряд (без повторений), то как его длина, так и *набор* композиционных факторов G_i/G_{i-1}, $i = 1, \ldots n$, являются инвариантами самой группы G. В частности, **разрешимая группа** может быть охарактеризована как группа, все композиционные факторы которой абелевы.

Задача. Пусть G — группа, обладающая композиционным рядом, и $H \trianglelefteq G$. Докажите, что в G существует композиционный ряд, проходящий через H.

2. Композиционные подгруппы. Подгруппа $H \leq G$ называется **композиционной подгруппой**, если существует *неуплотняемый*

субнормальный ряд с различными членами

$$H = G_0 \lhd G_1 \lhd \ldots \lhd G_{n-1} \lhd G_n = G,$$

такой ряд называется **композиционным рядом между** H и G — или между G и H, это вопрос вкуса. Напомним, что субнормальная подгруппа $H \trianglelefteq\trianglelefteq G$ соединена с G конечным субнормальным рядом. В частности, любая композиционная подгруппа субнормальна, но обратное, конечно, вообще говоря, неверно, так как между H и G может не существовать *неуплотняемых* рядов. Обычные композиционные ряды — это композиционные ряды между 1 и G.

Задача. Пусть $H \trianglelefteq\trianglelefteq G$ — композиционная подгруппа в G. Сформулируйте и докажите аналог теоремы Жордана—Гельдера для композиционных рядов между H и G

Упражнение. Пусть $F \trianglelefteq\trianglelefteq H \trianglelefteq\trianglelefteq G$, причем F — композиционная подгруппа в H, а H — композиционная подгруппа в G. Тогда F — композиционная подгруппа в G. Что можно сказать про *набор* композиционных факторов композиционного ряда между F и G?

Задача. Пусть F — композиционная подгруппа в G, а $H \lhd G$ — максимальная нормальная подгруппа. Тогда либо $F \leq H$, либо $F \cap H$ — максимальная нормальная подгруппа в H.

Задача. Пусть $F, H \trianglelefteq\trianglelefteq G$ — композиционные подгруппы в G. Докажите, что $F \cap H$ тоже является композиционной подгруппой. Что можно сказать про *множество* композиционных факторов композиционного ряда между $F \cap H$ и G?

Задача. Пусть $F, H \trianglelefteq\trianglelefteq G$ — композиционные подгруппы в G. Докажите **теорему Виландта**, утверждающую, что $\langle F, H\rangle \trianglelefteq\trianglelefteq G$ тоже является композиционной подгруппой. Что можно сказать про *множество* композиционных факторов композиционного ряда между $\langle F, H\rangle$ и G?

Указание. Постарайтесь переписать доказательство теоремы Виландта (Глава 3, § 10) о порождении субнормальных подгрупп, заменив при этом всюду индукцию по индексам $|G : F|$ и $|G : H|$ на индукцию по длине композиционных рядов, соединяющих F и H с G. Еще раз задумайтесь на тему, почему мы не могли провести такое же рассуждение в терминах длин произвольных субнормальных рядов, и Вы поймете, что теперь это рассуждение проходит.

3. Теорема Жордана—Гельдера для главных рядов. Сейчас мы убедимся в том, что аналог теоремы Жордана—Гельдера справедлив и для главных рядов.

Теорема Жордана—Гельдера bis. *Если группа G обладает главным рядом, то набор его факторов не зависит от выбора главного ряда.*

Доказательство слово в слово повторяет доказательство теоремы Жордана—Гельдера, если воспользоваться следующей версией теоремы Шрайера.

Теорема Шрайера об уплотнении bis. *Любые два нормальных ряда подгрупп обладают эквивалентными нормальными уплотнениями.*

Для доказательства этого варианта в свою очередь достаточно заметить, что если $F_i, H_j \trianglelefteq G$ — а не только $F_i \trianglelefteq F_{i+1}$, $H_j \trianglelefteq H_{j+1}$, как предполагалось в первоначальном доказательстве, — то $F_{ij} = (F_{i+1} \cap H_j)F_i \trianglelefteq G$ и $H_{ji} = (H_{j+1} \cap F_i)H_j \trianglelefteq G$, так что уплотнения будут нормальными, а не просто субнормальными рядами. Весь остальной текст доказательства повторяется буквально.

Чаще всего мы будем пользоваться теоремой Жордана—Гельдера для конечных групп. Так как конечные группы удовлетворяют всем мыслимым условиям конечности, то предположение о существовании в них композиционных/главных рядов выполнено в них автоматически. Тем самым, в этом случае *теоремы* Жордана—Гельдера принимают следующий вид.

Следствие. *Набор всех композиционных/главных факторов конечной группы G не зависит от выбора композиционного/главного ряда.*

Неуплотняемый ряд с различными членами в G, состоящий из характеристических подгрупп, называется **характеристическим рядом** (`characteristic series`).

Задача. Сформулируйте и докажите теорему Жордана—Гельдера для характеристических рядов. Что Вам для этого понадобится?

Комментарий. Часто, чтобы не повторять одно и то же рассуждение дважды или трижды, вводят понятие **операторной группы** или **Ω-группы**, где $\Omega \subseteq \mathrm{End}(G)$ — некоторое множество операторов. В этом случае можно рассмотреть Ω-субнормальные ряды, состоящие из Ω-инвариантных членов. Как обычно, Ω-композиционный ряд может быть определен как неуплотняемый Ω-субнормальный ряд. В случае, когда $\Omega = \mathrm{id}_G$, мы получаем обычные композиционные ряды, в случае $\Omega = \mathrm{Inn}(G)$ — главные ряды, в случае $\Omega = \mathrm{Aut}(G)$ — характеристические ряды, в случае $\Omega = \mathrm{End}(G)$ — вполне характеристические ряды и т. д. Читатель без труда проверит, что все результаты предыдущего и настоящего параграфов сразу обобщаются на этот более общий случай (для этого вначале нужно, конечно, обобщить на операторные группы теорему о гомоморфизме и теоремы об изоморфизме). Однако с моей точки зрения, подобный способ действий, вполне уместный в исследовательской статье, совершенно недопустим в учебной литературе! Не только начинающему, но и любому неспециалисту много проще проследить за двумя

безыскусными параллельными рассуждениями, и самостоятельно понять, как выглядит доказательство в общем случае, чем увидеть частные случаи за подобным обобщением: слова нужны, чтобы поймать мысль; после того, как мысль поймана, о словах забывают.

4. Основная теорема арифметики. Отметим, что теорему Жордана—Гельдера можно рассматривать как очень широкое некоммутативное обобщение основной теоремы арифметики. Покажем, что основная теорема арифметики вытекает из теоремы Жордана—Гельдера.

Теорема. *Разложение целого числа на простые множители однозначно.*

Доказательство. Пусть $n \in \mathbb{N}$, $n = p_1 \dots p_m$, где $p_i \in \mathbb{P}$ суть простые числа, не обязательно различные. Рассмотрим циклическую группу $G = C_n$ порядка n, порожденную g. Тогда

$$G = \langle g \rangle > \langle g^{p_1} \rangle > \langle g^{p_1 p_2} \rangle > \ldots > \langle g^{p_1 \cdots p_{m-1}} \rangle > 1$$

представляет собой композиционный ряд этой группы. Теорема Жордана—Гельдера утверждает, что набор чисел $[p_1, \dots, p_m]$ однозначно определяется числом n.

Раздел II. ДЕЙСТВИЯ ГРУПП

Мы уже много раз отмечали, что в подавляющем большинстве приложений — да и в самой теории групп — группа возникает не как абстрактная группа, а как группа преобразований, т. е. как группа действующая на каком-то множестве. В этом разделе мы начинаем изучение групповых действий, вначале на примере естественного действия симметрической группы S_n, а потом в общем случае.

В главе 5, посвященной симметрической группе, вводится несколько ключевых понятий, таких как цикленный тип, знак перестановки, знакопеременная группа A_n, транзитивность, примитивность, кратная транзитивность и доказывается несколько ключевых классических теорем: теорема Галуа о простоте A_n, $n \geq 5$, теорема Гельдера об автоморфизмах S_n и т. д. Кроме того, здесь мы начинаем обсуждать один из самых замечательных классических примеров групп: группы Матье M_{11}, M_{12}, M_{22}, M_{23}, M_{24}. Эти группы — исторически первые спорадические простые группы — естественно возникают во многих геометрических и комбинаторных вопросах, в теории кодирования и т. д.

В главе 6 действия групп обсуждаются с нескольких точек зрения. В этой главе вводятся ключевые понятия, связанные с действиями: орбиты и стабилизаторы, однородные и главные однородные множества и т. д. и основные конструкции над G-множествами. Но главное, здесь детально обсуждаются несколько примеров групп, возникающих в самой теории групп, геометрии, алгебраической геометрии, анализе и т. д. Все эти вещи будут постоянно сопровождать нас в дальнейшем. Например, основные теоремы о конечных группах естественнее всего доказывать, рассматривая действия группы на себе и различные связанные с ними действия (действия на подгруппах, подмножествах, надгруппах, смежных классах, etc.)

В целом изложение этого материала в общем курсе занимает обычно 2–3 лекции и, тем самым, даже самый слабо подготовленный студент должен быть в состоянии полностью изучить этот раздел за один день. Естественно, пропуская при этом все более сложные примеры!

Единственная причина, по которой в этом разделе нет специальной главы, трактующей *линейные* действия, состоит в том, что начиная

с раздела 6 *все* дальнейшие части этой книги посвящены именно их изучению!

Глава 5. СИММЕТРИЧЕСКАЯ ГРУППА

> При любом числе колоколов ровно половина всех вариаций имеет одну природу и ровно половина — другую. В чем именно заключается эта природа, мне не дано судить, но, как станет малопомалу ясно, в ней непременно следует разобраться, прежде чем мы сможем постичь науку композиции звонов и их исполнения.
>
> C. A. W. Troyte. *Change Ringing*

В этой главе мы разберем **архетипичный** пример: **симметрические группы конечных множеств**. Эти группы играют совершенно особую роль во всей теории.

• **История**: теория групп возникла в работах Лагранжа, Руффини, Абеля, Галуа и Коши именно как теория групп перестановок и на протяжении большей части XIX века и даже в начале XX века в работах Жордана, Силова, Матье, Гельдера, Миллера и других классиков теория групп развивалась *в первую очередь* как теория групп перестановок. Лишь на рубеже XIX и XX веков Молин, Фробениус, Бернсайд, Диксон, Шур и Блихфельд превратили теорию групп в теорию матричных групп.

Ганс Блихфельд (Hans Frederick Blichfeldt, 9 января 1873, Иллар — 16 ноября 1945, Пало Альто, Калифорния) — замечательный американский алгебраист датского происхождения, основные работы которого относятся к теории групп и геометрии чисел. Спасаясь от бедности его семья эмигрировала в США, когда Гансу было 15 лет, и несколько лет он батрачил на фермах в Калифорнии. В 1894 году он поступил в незадолго до этого созданный Стенфордский университет, а в 1897 году продолжил обучение в Лейпциге, где под руководством Софуса Ли в течение одного года написал диссертацию по группам преобразований. Следующие 40 лет Блихфельд работал в Стенфорде, где он дослужился от инструктора до декана математического факультета.

Сегодня Блихфельда вспоминают главным образом в связи с несколькими ключевыми результатами о конечных линейных группах и двумя замечательными классическими книгами *Finite Collineation Groups* и написанной вместе с Миллером и Диксоном *Theory and Application of Finite Groups*.

• **Вычисления**: в симметрических группах сравнительно легко проводить явные вычисления и, поэтому, изучение пермутационных представлений (т. е. гомоморфизмов $G \longrightarrow S_n$) и сегодня остается одним из основных инструментов теории групп, в особенности конечных. В некоторых системах компьютерной алгебры **все** вычисления

Огюстен Луи Коши (Augustin Louis Cauchy, 21 августа 1789, Париж — 23 мая 1857, Се) — один из крупнейших французских математиков XIX века. Его основные достижения, сразу получившие широчайшее признание, относятся к комплексному анализу, обоснованию вещественного анализа и теории дифференциальных уравнений. Наиболее значителен его вклад в теорию функций комплексной переменной. Однако, среди 600 или 700 написанных им работ есть несколько десятков алгебраических, главным образом относящихся к определителям и группам перестановок, а также многочисленные статьи по оптике, механике, теории упругости, etc.

В области вещественного анализа в своем *Cours d'analyse* (1821) и последующих книгах он дал изложение, которое и сегодня, за исключением незначительных деталей, является общепринятым в элементарных учебниках. Однако, здесь заслуга Коши менее бесспорна, так как он своротил анализ в болото второстепенных вопросов сходимости, которые под влиянием его авторитета были гипертрофированы в ущерб принципиальным структурным вопросам, волновавшим его предшественников.

После июльской революции 1830 года из-за своих крайних клерикально-монархических взглядов он был вынужден покинуть Францию и 8 лет жил за границей, главным образом в Турине и Праге. После возвращения во Францию в 1838 Коши преподавал в школе иезуитов. Только в 1848 году ему было разрешено преподавать не принося присяги новому правительству.

В нашем курсе встречаются последовательности Коши, теорема Коши о существовании элементов порядка p, теорема Бине—Коши, неравенство Коши (конечный случай обсуждаемого в анализе неравенства Коши—Буняковского—Шварца). В других курсах вам придется столкнуться с большим количеств теорем Коши, в том числе со знаменитой интегральной теоремой Коши, задачей Коши, уравнениями Коши—Римана (они же уравнения Эйлера—д'Аламбера), многочисленными признаками Коши, главным значением интеграла в смысле Коши, распределением Коши, остаточным членом в форме Коши и т. д.

в группах (даже вычисления с матрицами!) реализованы именно как вычисления в группах перестановок.

• **Приложения**: значительная часть применений теории групп как в самой математике (теории колец, алгебрах Ли, коммутативной алгебре, полилинейной алгебре, комбинаторике, геометрии, теории вероятностей), так и за ее пределами (теории твердого тела, квантовой химии, теории атома и ядра и т. д.) это именно приложения симметрической группы или тесно связанных с ней групп (октаэдральная группа, группы Вейля, группы Коксетера и т. д.)

• **Образец для обобщений**: S_n это очень интересный пример группы. Дело в том, что группа S_n очень близка к простым группам, и с одной стороны, ответы на основные вопросы для этой группы уже достаточно небанальны, а с другой стороны, все еще вполне обозримы, и их доказательства гораздо короче и проще, чем для групп типа Ли.

§ 1◇. Перестановки, симметрическая группа

> Двадцать две основные буквы: Бог их нарисовал, высек в камне, соединил, взвесил, *переставил* и создал из них все, что есть, — и все, что будет.
>
> *Сефер Йецира*

В настоящем параграфе мы введем полную запись перестановки и вычислим порядок симметрической группы.

1. Перестановки, симметрическая группа. Пусть вначале X — произвольное множество, $S_X = \mathrm{Bij}(X, X)$ – симметрическая группа множества X.

Задача. Убедитесь, что если $|X| = |Y|$ и $\varphi : X \longrightarrow Y$ произвольная биекция из X в Y, то $\pi \mapsto \varphi \circ \pi \circ \varphi^{-1}$ представляет собой изоморфизм S_X на S_Y.

Поскольку здесь нас интересуют главным образом перестановки конечных множеств, в дальнейшем мы можем считать, что $X = \underline{n} = \{1, \dots, n\}$ — множество первых n натуральных чисел. **Перестановкой** степени n называется биективное отображение множества $\underline{n}$ на себя. Множество всех перестановок степени n с произведением, заданным композицией отображений, называется **симметрической группой** степени n alias **группой перестановок** n **символов** и обозначается S_n.

Комментарий 1, исторический. В русской учебной литературе часто проводится различие между **перестановками** и **подстановками**. При этом **перестановками** называются линейные порядки на I, а биективные отображения I на себя именуются **подстановками**. Я полностью согласен с Алексеем Ивановичем Кострикиным (*Введение в алгебру*), что эта терминология представляет собой *злостный* анахронизм. Дело в том, что **перестановка** представляет собой перевод термина `permutation`, а **подстановка** — термина `substitution`. Ранние авторы (Лагранж, Руффини) использовали термин `permutation` (`permutazione`) для отображения, а термин `substitution` (`sostituzione`) для *композиции* двух функций.

Различие же между **перестановками** как порядком букв и **подстановками** как переходом от одной **перестановки** к другой, было введено Коши в 1815 году [202]. У Галуа встречаются оба термина: “Donc, si dans un pareil groupe on a les substitutions S et T, on est sûr d'avoir la substitution ST”, но, с другой стороны, “Le plus petit nombre de permutations que puisse avoir un groupe indécomposable, quand ce nombre n'est pas premier, est $3 \cdot 4 \cdot 5$”. В XIX веке термин **группа подстановок** широко использовался. Книга Жордана так и называлась *Traité des substitutions* (**Трактат о підстановках** — sic!), еще Ли говорил о `Substitutionsgruppe`.

Однако за последний век в западных языках термин `substitution` в этом значении повсеместно вытеснен словом `permutation`. Естественно, эта форма победила и в русской научной литературе, и нашла отражение в новых заимствованиях (**перестановочное представление**, **перестановочные игры** и т. д.). Тем не менее, в учебной

литературе на русском языке архаизм **подстановка** оказался удивительно живучим, несмотря даже на то, что перестановки **переставляют**, а подстановки **подставляют**. Конечно, если бы мне нужно было переводить этот термин на русский сегодня, я *без затей* сказал бы **пермутация**.

Комментарий 2, криптологический. Двумя простейшими типами шифров, рассматриваемыми в криптографии, являются шифры подстановки (`substitution cipher`) и шифры перестановки (`permutation code`, `transposition cipher`). По этому поводу см., например, замечательную статью Клода Шеннона, *Теория связи в секретных системах* [203], следующий абзац представляет собой пересказ двух первых примеров на страницах 344–345.

Напомним, что в простейшем варианте **шифром** называется любая инъективная функция $f : X \longrightarrow Y$, где X — некоторое множество, называемое множеством **исходных текстов** или **сообщений**, а Y — некоторое другое (возможно то же самое!) множество, называемое множеством **шифрованных текстов** или **криптограмм**. Можно, например, считать, что $X = W(A)$ — множество слов в некотором алфавите A, скажем, состоящем из пробела, букв латинского алфавита, индийских* цифр и знаков препинания. Все эти символы будут называться буквами, а количество букв, входящих в сообщение — длиной сообщения. **Шифр подстановки** состоит в том, что каждая буква сообщения заменяется на некоторую другую букву. Иными словами, мы фиксируем перестановку $\pi \in S_A$ и определяем функцию $f(x_1 \dots x_n) = \pi(x_1) \dots \pi(x_n)$. С другой стороны, **шифр перестановки** состоит в том, что исходное сообщение длины n разбивается на блоки длины $m|n$ (в любое сообщение можно дорисовать нужное количесто пробелов с тем, чтобы n делилось на m), к каждому из которых применяется фиксированная перестановка $\sigma \in S_m$. Иными словами, в этом случае функция f определяется посредством

$$f(x_1 \dots x_n) = (x_{\sigma(1)} \dots x_{\sigma(m)}) \ \dots \ (x_{\sigma(1)+n-m} \dots x_{\sigma(m)+n-m}).$$

Ясно, что шифр подстановки и шифр перестановки — это совсем не одно и то же, так как в одном случае перестановка применяется к аргументам, а во другом — к значениям функции! Именно консерватизм математиков, цепляющихся за украинизм **підстановка**, вынудил криптографов использовать вместо перевода термина `substitution cipher` гораздо менее точный парафраз **`шифры замены`**!

2. Полная запись перестановки. Обычно перестановки изображаются двумя строками следующим образом. В первой строке перечисляются элементы множества $\underline{n}$ в естественном порядке, а во второй строке под каждым элементом записывается его образ под действием перестановки. Пусть, например, π — перестановка, переводящая j в $\pi(j) = i_j$. Тогда пишут $\pi = \begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ — это так называемая **полная** или **развернутая запись перестановки** π. Например, тождественная перестановка записывается как $\mathrm{id} = \begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix}$.

*Некоторые упрямцы настойчиво называют эти цифры “арабскими” — естественно, *только* потому, что они никогда не видели *настоящих* арабских цифр.

Ясно, что при этом π вполне определяется своей второй строкой и иногда пишут просто $\pi = (i_1, \dots, i_n)$, это так называемая **сокращенная запись перестановки**, но мы будем избегать это сокращение, так как оно понадобится нам для обозначения циклов, см. ниже. Преимущество развернутой записи состоит еще и в том, что при этом не нужно требовать, чтобы элементы первой строки стояли в естественном порядке, что особенно удобно при образовании обратной перестановки. Иными словами, если $j_1, \dots, j_n$ — любое расположение чисел $1, \dots, n$, и $\pi(j_h) = k_h$, то перестановка π может быть записана и как $\pi = \begin{pmatrix} j_1 & \dots & j_n \\ k_1 & \dots & k_n \end{pmatrix}$. Например,

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 2 & 1 & 3 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

3. Действия над перестановками. Напомним, что **произведение перестановок** определяется как композиция отображений. В приведенных обозначениях умножение двух перестановок σ и π осуществляется так: нужно записать первую строку σ как вторую строку π, тогда $\sigma\pi$ — это перестановка, первая строка которой совпадает с первой строкой π, а вторая строка — со второй строкой σ в этой новой записи. Пусть, например,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}, \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix},$$

переписывая σ в виде $\sigma = \begin{pmatrix} 5 & 1 & 2 & 4 & 3 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}$, получим

$$\sigma\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 1 & 5 \end{pmatrix}.$$

Обратите внимание, что перестановки умножаются как отображения, а именно, **справа налево**: первой действует правая перестановка, а потом левая.

Особенно наглядно в этих обозначениях выглядит вычисление **обратной перестановки**. Чтобы найти π^{-1}, достаточно поменять местами первую и вторую строку двухрядной таблицы, изображающей перестановку π. Например, для такого же π, как выше, имеем

$$\pi^{-1} = \begin{pmatrix} 5 & 1 & 2 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix}.$$

4. Порядок симметрической группы. Ясно, что имеется одна перестановка степени 1 — тождественная; и 2 перестановки степени 2 — тождественная и транспозиция (12) и 6 перестановок степени 3 (все они были изображены в главе 3). Вообще, справедлив следующий результат.

Предложение. *Порядок группы S_n равен $n!$.*

Доказательство. Имеется n различных возможностей для образа 1 относительно перестановки π. Так как π биекция, то $\pi(2) \neq \pi(1)$ и, следовательно, для каждого из n выборов $\pi(1)$ имеется ровно $n-1$ различных возможностей для образа 2 относительно π. По той же причине при фиксированных $\pi(1), \pi(2)$ имеется ровно $n-2$ возможностей для $\pi(2)$ и т. д. Наконец, при выбранных $\pi(1), \ldots, (n-1)$, имеется единственная оставшаяся возможность для $\pi(n)$.

Число $n!$ растет довольно быстро. Ниже мы приводим значения нескольких первых факториалов, вместе с их традиционными кампанологическими названиями: $3! = 6$ (`singles`), $4! = 24$ (`minimus`), $5! = 120$ (`doubles`), $6! = 720$ (`minor`), $7! = 5040$ (`triples`), $8! = 40320$ (`major`), $9! = 362880$ (`caters`), $10! = 3628800$ (`royal`), $11! = 39916800$ (`cliques`), $12! = 479001600$ (`maximus`). Число $8!$ фигурирует в *Книге рекордов Гиннеса* в связи с вызваниванием переборов с вариациями на 8 колоколах [204].

§ 2♢. Циклы

Для этого нам придется вначале обсудить орбиты перестановок (в главе 6 мы вернемся к анализу этого понятия в более общем контексте).

1. Орбиты. Фиксируем какую-то перестановку $\pi \in S_n$. Определим на множестве $\underline{n} = \{1, \ldots, n\}$ отношение $\sim$, полагая $i \sim j$, если $j = \pi^k(i)$ для $k \in \mathbb{Z}$.

Лемма. *Отношение $\sim$ является эквивалентностью.*

Доказательство. 1) Рефлексивность: $i = \mathrm{id}(i) = \pi^0(i)$.

2) Симметричность: если $j = \pi^k(i)$, то $i = \pi^{-k}(j)$.

3) Транзитивность: если $j = \pi^k(i)$ и $h = \pi^l(j)$, то $h = \pi^{k+l}(i)$.

Таким образом, с каждой перестановкой π связано разбиение множества $\underline{n}$ на классы эквивалентности $\sim$, эти классы называются **орбитами** π. Тем самым, $\underline{n} = X_1 \sqcup \ldots \sqcup X_m$, где $X_1, \ldots, X_m$ суть орбиты

перестановки π. Иногда множество орбит перестановки σ обозначается через $\underline{n}/\sigma = \{X_1, \dots, X_m\}$. Орбиты, содержащие более одного элемента, будут называться **нетривиальными**.

Задача. Докажите, что орбита элемента i совпадает с его **траекторией** $\{i, \pi(i), \pi^2(i), \dots\}$.

Решение. *Обратимое* преобразование *конечного* множества имеет конечный порядок.

Подмножество $X \subseteq \underline{n}$ называется **устойчивым** под действием π, если $\pi(i) \in X$ для любого $i \in X$. Ясно, что устойчивые подмножества — это в точности объединения орбит.

2. Фикс и подвижные элементы. С каждой перестановкой $\pi \in S_n$ можно связать два подмножества в $\underline{n}$, а именно, множества

$$\mathrm{Fix}(\pi) = \{i \in \underline{n} \mid \pi(i) = i\}, \qquad \mathrm{Mob}(\pi) = \{i \in \underline{n} \mid \pi(i) \neq i\}$$

неподвижных alias **стабильных** точек и **подвижных** alias **мобильных** точек (`Wirkungsbereich`). Иными словами, $\mathrm{Fix}(\pi)$ является объединением всех одноэлементных орбит, в то время как $\mathrm{Mob}(\pi)$ является объединением всех нетривиальных орбит. Ясно, что $\mathrm{Fix}(\pi)$ и $\mathrm{Mob}(\pi)$ устойчивы под действием π, причем $\underline{n} = \mathrm{Fix}(\pi) \sqcup \mathrm{Mob}(\pi)$.

Перестановки π и σ называются **независимыми**, если

$$\mathrm{Mob}(\pi) \cap \mathrm{Mob}(\sigma) = \varnothing.$$

Следующее утверждение очевидно.

Лемма. *Независимые перестановки коммутируют.*

3. Циклы. Перестановка $\sigma \in S_n$ называется **циклом**, если множество ее мобильных элементов представляет собой одну орбиту под действием σ. В этом случае $\mathrm{Mob}(\sigma)$ часто называется также **носителем** цикла σ, а порядок $|\mathrm{Mob}(\sigma)|$ – его **длиной**. Циклы длины 1 называются тривиальными, цикл длины ≥ 2 называется **истинным циклом** (`echter Zyklus`). В дальнейшем, говоря о циклах, мы всегда имеем в виду истинные циклы. Циклы настолько часто используются в вычислениях, что нам будет удобно ввести для них специальные обозначения.

Пусть $i_1, \dots, i_l \in \underline{n}$ — набор попарно различных символов. Тогда через $(i_1 \dots i_l)$, обозначается цикл длины l с носителем $\{i_1, \dots, i_l\}$, под действием которого

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \dots \mapsto i_l \mapsto i_1,$$

а все остальные элементы множества $\underline{n}$ остаются на месте. Один и тот же цикл может быть записан по разному:

$$(i_1 i_2 \dots i_l) = (i_2 \dots i_l i_1) = \dots = (i_l i_1 \dots i_{l-1}).$$

Обратный к циклу $(i_1 \dots i_l)$ равен $(i_l \dots i_1)$.

4. Длинные циклы. Перестановка σ называется **длинным циклом**, если все множество $\underline{n}$ образует одну орбиту под действием σ. Длинные циклы, называемые также **элементами Коксетера**, представляют собой один из наиболее интересных типов перестановок. Особенно часто используются следующие два взаимнообратных длинных цикла:

$$\texttt{RotateRight} = (123\dots n), \qquad \texttt{RotateLeft} = (n, n-1, n-2, \dots 1).$$

Задача. Найдите количество длинных циклов в S_n.

Решение. Запись длинного цикла имеет вид $(\pi(1), \dots, \pi(n))$ для некоторого $\pi \in S_n$. Таким образом, количество различных *записей* длинных циклов равно $n!$. Однако, как было уже замечено, применение `RotateRight` к записи длинного цикла не меняет этот цикл. Так как порядок `RotateRight` равен n, то любой длинный цикл допускает ровно n различных записей. Это значит, что количество n-циклов на n-элементном множестве равно $n!/n = (n-1)!$.

§ 3♡. Большая се[к]стина

> Форма всякого зрелого искусства по существу математична.
>
> Освальд Шпенглер

> ... современный читатель, привыкший к свободным стихам, не улавливает сложной гармонии в такой строфике. Возможно, что в XII веке все было иначе. Изощренные в придворных турнирах стихотворцев трубадуры добивались, вероятно, соответствия между развитием мысли и чередованием рифм, чего не получилось в секстинах наших поэтов.
>
> Александр Соломонович Компанеец. [205]

Одной их самых тонких стихотворных форм классической европейской поэзии была изобретенная великим провансальским трубадуром XII века Арнаутом Даниэлем[♮] секстина (`sestina`). Он решил написать стихотворение, удовлетворяющее следующим правилам:

[♮] **Arnaut Daniel**, или, как называет его Данте, считавший Арнаута *итальянским* поэтом, `Arnaldo Daniello`, `Arnaldus Danielis`: "*O frate*," *disse*, "*questi ch'io ti cerno col dito*", *e additò un spirto innanzi*, "*fu miglior fabbro del parlar materno.*" — Purgatorio, XXVI, 115–117.

- Количество строф равно количеству строк в строфе;
- Наборы **рифм** (финальных слов) любых двух строф идентичны;
- Для каждого финального слова его положения в различных строфах различны.

Сам Арнаут Даниэль использовал схему `retrogradatio cruciata`, при которой последовательность рифм от строфы к следующей преобразуется следующим образом: последняя рифма становится первой, первая второй, предпоследняя третьей, вторая — четвертой и т. д. Это в точности преобразование, встречавшееся нам в главе 2 под именем **тасования Монжа**! Иными словами, в простейшем интересном случае **секстины**, когда в в стихотворении **шесть** строф, в каждой из которых по **шесть** строк, мы получаем схему

$$\begin{array}{cccccc} a & b & c & d & e & f \\ f & a & e & b & d & c \\ c & f & d & a & b & e \\ e & c & b & f & a & d \\ d & e & a & c & f & b \\ b & d & f & e & c & a \end{array}$$

Здесь через a, b, c, d, e, f обозначены рифмы, строки таблицы отвечают строфам, а номер столбца указывает положение рифмы в соответствующей строфе. Таким образом, каждая следующая строфа начинается той же самой рифмой, которой заканчивается предыдущая, а последняя строфа заканчивается первой рифмой первой строфы! Эта перестановка является 6-циклом, так что если применить ее к последней строфе, получится та же последовательность рифм, что в первой строфе!

Часто к секстине добавляли **посылку**, состоящую из трех строк — шести полустрок! — в каждой из которых встречалось по *две* рифмы. Позже эта форма в чуть измененном виде культивировалась Данте и Петраркой, причем в отличие от провансальских поэтов, использовавший белый стих, у итальянцев рифмы кроме повторов с перестановкой между строфами фактически были еще и рифмами внутри строфы! После этого (за исключением коротких эпизодов, когда поэты Плеяды тщетно пытались адаптировать эту стихотворную форму к французскому, а Опитц — к немецкому языку) секстина надолго вышла из употребления. Однако в XIX веке провансальские поэты возродили секстину. По-английски секстины писал Суинберн, а по-русски — поэты Серебрян[н]ого века: Брюсов, Кузмин и другие. Однако с моей точки зрения все попытки написать секстину на каком-либо другом языке, кроме провансальского и итальянского, или хотя бы убедительно перевести на современные языки секстины трубадуров, не имели большого успеха.

Так как не все студиозы свободно читают провансальских поэтов XII века в оригинальной орфографии, проиллюстрируем понятие секстины на более привычном материале. Вот одна из самых знаменитых секстин Данте (*Rime per la donna Pietra*):

Al poco giorno e al gran cerchio d'ombra
son giunto, lasso!, ed al bianchir de'colli,
quando si perde lo color ne l'erba;
e 'l mio disio però non cangia il verde,

sì è barbato ne la dura petra
che parla e sente come fosse donna.

Similemente questa nova donna
si sta gelata come neve a l'ombra;
che non la move, se non come petra,
il dolce tempo che riscalda i colli
e che li fa tornar di bianco in verde
perché li copre di fioretti e d'erba

Quand'ella ha in testa una ghirlanda d'erba,
trae de la mente nostra ogn'altra donna;
perché si mischia il crespo giallo e 'l verde
sì bel, ch'Amor lì viene a stare a l'ombra,
che m'ha serrato intra piccioli colli
più forte assai che la calcina petra.

La sua bellezza ha più vertù che petra,
e 'l colpo suo non può sanar per erba;
ch'io son fuggito per piani e per colli,
per potere scampar da cotal donna;
e dal suo lume non mi può far ombra
poggio né muro mai né fronda verde.

Io l'ho veduta già vestita a verde
sì fatta, ch'ella avrebbe messo in petra
l'amor ch'io porto pur a la sua ombra;
ond'io l'ho chesta in un bel prato d'erba
innamorata, com'anco fu donna,
e chiuso intorno d'altissimi colli.

Ma ben ritorneranno i fiumi a' colli
prima che questo legno molle e verde
s'infiammi, come suol far bella donna,
di me; che mi torrei dormire in petra
tutto il mio tempo e gir pascendo l'erba,
sol per veder do' suoi panni fanno ombra.

Quandunque i colli fanno più nera ombra,
sotto un bel verde la giovane donna
la fa sparer, com'uom petra sott'erba.

Дальнейшие вариации на ту же тему включают **двойную секстину**, состоящую из 12 строф по 12 строк в каждой (+ посылка из 12 полустрок).

§ 4♢. Разложение перестановки на независимые циклы

В этом параграфе мы введем цикленную запись перестановки значительно более короткую и удобную для вычислений, чем развернутая запись.

1. Разложение на независимые циклы. В соответствии с общим определением два цикла называются **независимыми**, если их носители дизъюнктны. Иными словами, циклы $(i_1, \dots, i_l)$ и $(j_1, \dots, j_m)$ независимы, если $\{i_1, \dots, i_l\} \cap \{j_1, \dots, j_m\} = \varnothing$. Следующий результат, известный как **разложение на независимые циклы** (`Zyklenzerlegung`), несмотря на свою простоту лежит в основе всей теории групп перестановок.

Теорема. *Каждая перестановка можно представить как произведение попарно независимых истинных циклов. Такое представление единственно с точностью до перестановки сомножителей.*

Доказательство. Существование: пусть $X_1, \dots, X_s$ суть все все нетривиальные орбиты перестановки π. Ограничение π на нетривиальную орбиту X_i задает истинный цикл, который мы обозначим через π_i. Так как различные орбиты не пересекаются, то циклы $\pi_1, \dots, \pi_s$, независимы. Так как каждый элемент лежит в какой-то орбите, то $\pi = \pi_1 \dots \pi_l$.

Единственность: пусть $\pi = \pi_1 \dots \pi_l$ есть разложение π в произведение независимых истинных циклов. Для каждого i множество $\mathrm{Mob}(\pi_i)$ обязано совпадать с какой-то нетривиальной орбитой π. А так как π является произведением π_i, то множество носителей этих циклов должно совпадать с множеством всех таких орбит.

Следствие 1. *Группа S_n порождается циклами.*

Ясно, что порядок цикла $o(\pi) = l(\pi)$ равен его длине.

Следствие 2. *Если $\pi = \pi_1 \dots \pi_l$ есть разложение перестановки π на независимые циклы, то $o(\pi) = \mathrm{lcm}(o(\pi_1), \dots, o(\pi_l))$.*

2. Каноническое разложение на циклы. Следующий способ позволяет сделать разложение на циклы единственным. А именно, обозначим через π_1 цикл, содержащий наименьший элемент из $\mathrm{Mob}(\pi)$, через π_2 – цикл, содержащий наименьший элемент из $\mathrm{Mob}(\pi)$, который не попал в $\mathrm{Mob}(\pi_1)$, через π_3 — цикл, содержащий наименьший элемент из $\mathrm{Mob}(\pi)$, который не попал в $\mathrm{Mob}(\pi_1) \cup \mathrm{Mob}(\pi_2)$, и т. д. Полученное в результате разложение называется **каноническим разложением π на циклы** (`kanonische Zyklendarstellung`).

Приведем пример канонического разложения:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 3 & 8 & 9 & 7 & 2 & 1 & 6 \end{pmatrix} = (148)(25967)$$

Предыдущая строка порождена командами `RandomPermutation[9]` и `ToCycles`. Видно, насколько цикленная запись компактнее полной.

3. Умножение циклов. Цикленная запись не только компактнее полной, но — при некотором навыке — удобнее для вычислений. А именно, пусть $\sigma = \sigma_1 \dots \sigma_s$ — *произвольное* произведение циклов. Перестановку σ можно вычислить следующим образом. Чтобы определить образ i под действием σ, начнем с того, что найдем самый правый цикл, скажем, σ_p, в запись которого входит фрагмент вида $(\dots ij \dots)$ либо $(j \dots i)$, этот цикл переводит i в j. Если i не входит в запись ни одного из циклов σ_p, то $\sigma(i) = i$. Найдем теперь самый правый цикл σ_q левее σ_p, в запись которого входит фрагмент вида $(\dots jh \dots)$ либо $(h \dots j)$, этот цикл переводит j в h. Если j не входит в запись ни одного из циклов σ_q, $q < p$, то $\sigma(i) = j$. В противном случае, продолжая действовать таким же образом, мы в конце концов найдем $\sigma(i)$.

Для иллюстрации этого алгоритма рассмотрим перестановку

$$\sigma = (1753)(162)(46)(3574).$$

Вычислим, для примера, $\sigma(7)$. Цикл (3574) переводит 7 в 4, цикл (46) переводит 4 в 6, цикл (162) переводит 6 в 2, наконец, цикл (1753) оставляет 2 на месте. Поэтому $\sigma(7) = 2$. В действительности, вычисляя теперь образ $\sigma(2)$, мы видим, что $\sigma(2) = 7$, так что в разложение σ на независимые циклы входит цикл (27).

Упражнение. Закончите вычисление σ и запишите каноническое разложение σ на независимые циклы. Проведите аналогичное вычисление для перестановки (184)(253)(67)(142635)(78).

§ 5♠. Количество перестановок степени n с m циклами

В этом параграфе мы хотим сформулировать классический комбинаторный результат, отвечающий на вопрос о количестве перестановок n символов с m циклами. Ответ дается в терминах **чисел Стирлинга** и сейчас мы совсем коротко напомним их определение.

Джеймс Стирлинг (`James Stirling`, 1692, St. Ninians — 5 декабря 1770, Leadhills) — шотландский математик, основные работы которого относятся к теории рядов, интерполяции и теории алгебраических кривых. Как приверженец Стюартов Стирлинг вынужден был эмигрировать и в 1714–1725 годах жил в Венеции. Позже он вернулся в Шотландию, где занимался горным делом, которое оставляло ему мало досуга для математических штудий.

1. Числа Стирлинга первого рода. Рассмотрим **убывающий факториал**

$$[x]_n = x(x-1)\dots(x-n+1) \in \mathbb{Z}[x]$$

и **возрастающий факториал**

$$[x]^n = x(x+1)\dots(x+n-1) \in \mathbb{Z}[x].$$

Мы интересуемся разложениями $[x]_n$ и $[x]^n$ по стандартному базису $1, x, x^2, \dots$ кольца $\mathbb{Z}[x]$. Коэффициент при x^m в разложении $[x]^n$ называется **числом Стирлинга первого рода** и обозначается $\left[\begin{matrix} n \\ m \end{matrix}\right]$, $m, n \in \mathbb{N}_0$. Таким образом, по определению

$$[x]^n = \sum_{m=0}^{n} \left[\begin{matrix} n \\ m \end{matrix}\right] x^m.$$

Заменяя здесь x на $-x$ мы видим, что $[-x]_n = (-1)^n [x]^n$, так что

$$[x]_n = \sum_{m=0}^{n} (-1)^{n-m} \left[\begin{matrix} n \\ m \end{matrix}\right] x^m.$$

Предостережение. Приведенное выше определение совпадает с определением в *Искусстве программирования* и *Конкретной математике* и *отличается* от обычного определения **знаком**! В большинстве классических руководств по комбинаторике числами Стирлинга первого рода принято называть коэффициент при x^m в разложении $[x]_n$, равный $(-1)^{n-m}\left[\begin{matrix} n \\ m \end{matrix}\right]$, который при этом обозначается через s_{nm} или $s(n,m)$. Классическое определение удобнее тем, что становится более наглядной связь чисел Стирлинга первого рода с более известными числами Стирлинга второго рода. Однако, так как нас интересует только комбинаторный смысл чисел Стирлинга, мы пользуемся определением Кнута[♮]. Кроме того, мы пользуемся пропагандируемым Кнутом обозначением Йована Карамата [208], [209], достоинство которого состоит в том, что оно подчеркивает аналогию чисел Стирлинга с биномиальными коэффициентами.

Числа Стирлинга первого рода можно определить **граничными условиями**

$$\left[\begin{matrix} n \\ 0 \end{matrix}\right] = \delta_{n0}, \qquad \left[\begin{matrix} n \\ m \end{matrix}\right] = 0 \quad \text{при } m > n$$

и **треугольным рекуррентным соотношением** аналогичным тому, при помощи которого определяются биномиальные коэффициенты:

$$\left[\begin{matrix} n \\ m \end{matrix}\right] = (n-1) \left[\begin{matrix} n-1 \\ m \end{matrix}\right] + \left[\begin{matrix} n-1 \\ m-1 \end{matrix}\right].$$

[♮]Как известно, биографии современников не приводятся. Однако мы не можем не не прорекламировать серию книг Дональда Кнута под общим названием *Искусство программирования*, ставшую уникальным явлением в мировой литературе. Три первых тома этой серии имеются в русском переводе [76], [206], [207] Еще одним замечательным достижением Кнута является создание издательских систем TEX и `METAFONT`, которые позволили *каждому* создавать тексты на полиграфическом уровне, ранее доступном только немногим профессионалам. Всего Кнут является автором 19 книг, из которых еще некоторые переведены на русский язык, в том числе [5]. Из книг, пока не переведенных на русский, начинающему можно порекомендовать *Surreal numbers*, содержащую изложение теории **сверхвещественных** (`сюрреалистических`) чисел Конвея.

Пользуясь этим соотношением несложно вычислить несколько первых строк **треугольника Стирлинга первого рода**:

1	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0	0
0	2	3	1	0	0	0	0	0	0	0
0	6	11	6	1	0	0	0	0	0	0
0	24	50	35	10	1	0	0	0	0	0
0	120	274	225	85	15	1	0	0	0	0
0	720	1764	1624	735	175	21	1	0	0	0
0	5040	13068	13132	6769	1960	322	28	1	0	0
0	40320	109584	118124	67284	22449	4536	546	36	1	0
0	362880	1026576	1172700	723680	269325	63273	9450	870	45	1

Число Стирлинга $\left[\begin{matrix} n \\ m \end{matrix}\right]$ расположено здесь на пересечении n-й строки и m-го столбца, причем нумерация начинается с 0. Конечно, в действительности я (как всегда!) ничего не считал руками, вычисление этой таблицы произведено посредством

```
Table[Abs[StirlingS1[n, m]],{n,0,10},{m,0,10}].
```

Так как `Mathematica` пользуется классическим определением чисел Стирлинга, применение функции `Abs` необходимо, чтобы убрать лишний знак. Из треугольного рекуррентного соотношения (либо непосредственно из определения) легко вытекает, что $\left[\begin{matrix} n \\ n \end{matrix}\right] = 1$, а $\left[\begin{matrix} n \\ 1 \end{matrix}\right] = (n-1)!$.

2. Числа Стирлинга второго рода. В действительности, значительно чаще используются числа Стирлинга второго рода, которые отвечают за разложение x^n по убывающим или возрастающим факториалам $[x]_m$ или $[x]^m$. А именно, коэффициент при $[x]_m$ в разложении x^n называется **числом Стирлинга второго рода** и обозначается $\left\{\begin{matrix} n \\ m \end{matrix}\right\}$, $m, n \in \mathbb{N}_0$. В большинстве классических книг по комбинаторике используется обозначение S_{nm} или $S(n,m)$. Таким образом, по определению

$$x^n = \sum_{m=0}^{n} \left\{\begin{matrix} n \\ m \end{matrix}\right\} [x]_m.$$

Как и выше, пользуясь тем, что $[-x]_n = (-1)^n [x]^n$, мы видим, что

$$x^n = \sum_{m=0}^{n} (-1)^{n-m} \left\{\begin{matrix} n \\ m \end{matrix}\right\} [x]^m.$$

По самому определению, имеют место формулы

$$\sum_i (-1)^{n-i} \left[\begin{matrix} n \\ i \end{matrix}\right] \left\{\begin{matrix} i \\ m \end{matrix}\right\} = \delta_{mn} = \sum_i (-1)^{n-i} \left\{\begin{matrix} n \\ i \end{matrix}\right\} \left[\begin{matrix} i \\ m \end{matrix}\right],$$

называемые **формулами обращения Стирлинга**. В классических обозначениях, когда знак включен в определение числа Стирлинга первого рода, эти формулы принимают более простой вид $\sum s(n,i)S(i,m) = \sum S(n,i)s(i,m) = \delta_{mn}$.

Числа Стирлинга второго рода удовлетворяют тем же граничным условиям $\left\{ {n \atop 0} \right\} = \delta_{n0}$, $\left\{ {n \atop m} \right\} = 0$ при $m > n$, что и числа Стирлинга первого рода, а **треугольное рекуррентное соотношение** для них принимает вид:

$$\left\{ {n \atop m} \right\} = m \left\{ {n-1 \atop m} \right\} + \left\{ {n-1 \atop m-1} \right\}.$$

Как и выше, при помощи `Table[StirlingS2[n, m], {n, 0, 10}, {m, 0, 10}]` можно вычислить несколько первых строк **треугольника Стирлинга второго рода**:

1	0	0	0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0	0	0	0
0	1	3	1	0	0	0	0	0	0	0
0	1	7	6	1	0	0	0	0	0	0
0	1	15	25	10	1	0	0	0	0	0
0	1	31	90	65	15	1	0	0	0	0
0	1	63	301	350	140	21	1	0	0	0
0	1	127	966	1701	1050	266	28	1	0	0
0	1	255	3025	7770	6951	2646	462	36	1	0
0	1	511	9330	34105	42525	22827	5880	750	45	1

Формулы обращения Стирлинга утверждают в точности, что рассматриваемые как матрицы степени $n+1$ верхние левые углы треугольников Стирлинга взаимно обратны, если, конечно, сменить знак у стоящих в нечетных позициях элементов треугольника Стирлинга первого рода. Для примера запишем вторую формулу обращения 4-го порядка:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 1 & 7 & 6 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 2 & -3 & 1 & 0 \\ 0 & -6 & 11 & -6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Числа Стирлинга второго рода имеют чрезвычайно наглядную комбинаторную интерпретацию. А именно, $\left\{ {n \atop m} \right\}$ представляет собой количество отношений эквивалентности на n элементном множестве X с m классами, или, как принято говорить в комбинаторике, количество разбиений X на m **блоков**. Например, $\left\{ {4 \atop 2} \right\} = 7$, так что существуют ровно 7 разбиений множества $X = \{1,2,3,4\}$ на два блока, а именно, $X = \{1\} \sqcup \{2,3,4\}$, $X = \{2\} \sqcup \{1,3,4\}$, $X = \{3\} \sqcup \{1,2,4\}$, $X = \{4\} \sqcup \{1,2,3\}$, $X = \{1,2\} \sqcup \{3,4\}$, $X = \{1,3\} \sqcup \{2,4\}$, $X = \{1,4\} \sqcup \{2,3\}$.

3. Количество перестановок с m циклами. Теперь у нас все готово для того, чтобы вернуться к перестановкам. В предыдущем параграфе мы убедились, что количество длинных циклов, которые можно образовать из n символов, равно $(n-1)! = \left[{n \atop 1} \right]$. Это простейший частный случай следующего результата.

Теорема. *Количество перестановок n символов, в разложение которых входит ровно m циклов, равно $\left[\begin{matrix} n \\ m \end{matrix}\right]$.*

Доказательство. Обозначим количество перестановок n символов, в разложение которых входит ровно m циклов, через $x(n,m)$. Ясно, что $x(0,0)=1$, $x(n,0)=0$ для всех $m \geq 1$ и $x(n,m)=0$ для всех $m>n$. Поэтому для того, чтобы убедиться в том, что $x(n,m)=\left[\begin{matrix} n \\ m \end{matrix}\right]$, достаточно доказать, что $x(n,m)$ удовлетворяет тому же рекуррентному соотношению, что и числа Стирлинга первого рода. В самом деле, рассмотрим перестановку $\pi \in S_n$ и сфокусируемся на символе n. Имеется следующая альтернатива:

• n образует отдельную орбиту π. Убирая эту орбиту мы получаем перестановку $\sigma \in S_n$ с $m-1$ орбитой, так что количество таких перестановок равно $x(n-1,m-1)$.

• n входит в какой-то цикл длины ≥ 2. В этом случае вычеркивая в цикленной записи перестановки π символ n мы получим перестановку $\sigma \in S_{n-1}$, у которой по прежнему m орбит, причем каждая такая перестановка получится из некоторой перестановки $\pi \in S_n$ с m орбитами. Обратно, рассмотрим произвольную перестановку $\sigma \in S_{n-1}$ с m циклами длин $l_1, \ldots, l_m$. Чтобы восстановить из нее перестановку π, мы должны врисовать символ n в какой-то цикл. Имеется ровно $l+1$ способов врисовать n в цикл $(i_1 \ldots i_l)$ длины l, но $(ni_1 \ldots i_l)=(i_1 \ldots i_l n)$ являются просто разными записями одного и того же цикла. Таким образом, среди этих $l+1$ способов ровно l различных. Так как мы можем врисовать n в каждый из m циклов перестановки σ, это значит, что общее количество перестановок π, превращающихся в σ после вычеркивания n, равно $l_1+\ldots+l_m=n-1$, и не зависит от σ. Таким образом, общий вклад этого случая равен $(n-1)x(n-1,m)$

Суммируя полученные результаты, получаем $x(n,m)=(n-1)x(n-1,m)+x(n-1,m-1)$, как и утверждалось.

Например, $\left[\begin{matrix} 4 \\ 2 \end{matrix}\right]=11$, так что существует 11 перестановок 4 символов, представимых в виде произведения двух циклов, а именно (1)(234), (1)(243), (2)(134), (2)(143), (3)(124), (3)(142), (4)(123), (4)(132), (12)(34), (13)(24), (14)(23). Заметим, что так как число Стирлинга второго рода $\left\{\begin{matrix} n \\ m \end{matrix}\right\}$ совпадает с количеством всевозможных разбиений $X=\underline{n}$ на m орбит, и для каждого такого разбиения имеется по крайней мере одна перестановка с данным разбиением на орбиты, то $\left\{\begin{matrix} n \\ m \end{matrix}\right\} \leq \left[\begin{matrix} n \\ m \end{matrix}\right]$. При этом в случае, когда имеется хотя бы одна трехэлементная орбита имеется более такой одной перестановки. Тем самым, как правило, $\left\{\begin{matrix} n \\ m \end{matrix}\right\} < \left[\begin{matrix} n \\ m \end{matrix}\right]$.

§ 6♢. Классы сопряженности S_n

В этом параграфе мы опишем классы сопряженности группы S_n.

1. Цикленный тип перестановки. Пусть $\pi \in S_n$ и

$$\underline{n}/\pi=\{X_1,\ldots,X_t\}.$$

Обозначим через $n_i=|X_i|$ порядок орбиты X_i.

Определение. Цикленным типом *перестановки* $\pi \in S_n$ *называют набор* $[n_1, \ldots, n_t]$ *порядков ее орбит.*

Обычно этот набор записывают как тупель $(n_1, \ldots, n_t)$, считая, что n_i расположены в порядке убывания. Обратите внимание, что говорят о **цикленном** или, изредка, **цикловом**, (но **не** циклическом!) типе. Впрочем, часто эпитет **цикленном** опускают и говорят просто о **типе** перестановки. Ясно, что $n_1 + \ldots + n_t = n$, так что с точки зрения комбинаторики $(n_1, \ldots, n_t)$ определяет **разбиение** числа n. Порядок длин здесь безразличен, поэтому n_i принято располагать не в том порядке, в котором они идут в каноническом разложении на циклы, а в порядке убывания. В группе S_2 элемент определяется своим цикленным типом, а именно, тождественная перестановка имеет тип $(1,1)$, а нетождественная – тип (2). В S_3 имеется три возможных типа: тождественная перестановка $(1,1,1)$, транспозиции $(2,1)$ и 3-циклы (3). В S_4 возможных типов уже 5: тождественная перестановка $(1,1,1,1)$, транспозиция $(2,1,1)$, произведение двух независимых транспозиций $(2,2)$, 3-цикл $(3,1)$ и 4-цикл (4).

Задача. Перечислите все возможные типы перестановок на 5,6,7,8 и 9 символах.

Впрочем, часто перечисляют только порядки нетривиальных орбит, подразумевая, что потом их сумма дополняется до n нужным количеством единиц. Удобство такого соглашения состоит в том, что в этом случае мы можем — независимо от n — говорить о транспозиции как об элементе цикленного типа (2); о произведении двух независимых транспозиций — как об элементе цикленного типа $(2,2)$; о 3-цикле — как об элементе цикленного типа (3); и т. д.

Теорема. *Две перестановки в* S_n *тогда и только тогда сопряжены, когда их цикленные типы совпадают.*

Доказательство. Пусть вначале $\pi, \sigma \in S_n$ – две сопряженные перестановки, скажем, $\pi = \rho\sigma\rho^{-1}$ для некоторого $\rho \in S_n$. Ясно, что если $\sigma(i) = j$, то $\pi\rho(i) = \rho(j)$. Тем самым, если $X_1, \ldots, X_t$ — орбиты σ, то $\rho(X_1), \ldots, \rho(X_t)$ — орбиты π, а так как $\rho \in S_n$, то $|\rho(X_h)| = |X_h|$, так что цикленные типы сопряженных перестановок совпадают.

Обратно, предположим, что

$$\pi = (i_{11} \ldots i_{1l}) \ldots (i_{t1} \ldots i_{tm}),$$

$$\sigma = (j_{11} \ldots j_{1l}) \ldots (j_{t1} \ldots j_{tm}),$$

две перестановки одинакового цикленного типа. Мы утверждаем, что $\pi = \rho\sigma\rho^{-1}$, где

$$\rho = \begin{pmatrix} i_{11} & \dots & i_{1l} & \dots & i_{t1} & \dots & i_{tm} \\ j_{11} & \dots & j_{1l} & \dots & j_{t1} & \dots & j_{tm} \end{pmatrix}.$$

В самом деле, посмотрим, во что h-й элемент r-го цикла переходит под действием перестановки $\rho\sigma\rho^{-1}$: $i_{rh} \mapsto j_{rh} \mapsto j_{r,h+1} \mapsto i_{r,h+1}$. Поскольку то же верно для всех элементов, перестановка $\rho\sigma\rho^{-1}$ совпадает с π. Но это и означает, что две перестановки одинакового цикленного типа сопряжены.

Следствие. *В S_n каждый элемент сопряжен со своим обратным.*

По причинам, которые становятся понятными только при изучении теории представлений, группа G, в которой $g \sim g^{-1}$ для всех $g \in G$, называется **вещественной**.

§ 7♣. Наибольший порядок элемента S_n

Рассмотрим **стандартную карточную колоду** P (`pack`) из 52 карт (это понятие определяется в I–3–3). Элементы симметрической группы $S(P) \cong S_{52}$ принято называть **тасовками** (`shuffles`). Сколько раз нужно повторить фиксированную тасовку, чтобы порядок карт совпал с первоначальным? Какое наибольшее число раз нам может при этом понадобиться стасовать колоду? В настоящем параграфе (который основан на [211] [212]) мы установим, что это число равно 180180.

1. Эмпирические данные. С математической точки зрения речь здесь идет о нахождении наибольшего порядка перестановки $\pi \in S_n$. Обозначим этот порядок через $G(n) = \max(o(\pi))$, где максимум берется по всем $\pi \in S_n$. Что можно сказать о функции $G(n)$? Ясно, что для $n = 2, 3, 4$ наибольший порядок в группе S_n имеет соответствующий длинный цикл. Но для $n = 5$ это уже не так, порядок длинного цикла равен 5, в то время принадлежащий S_5 элемент цикленного типа $(3, 2)$ имеет порядок $3 \cdot 2 = 6$. Еще более замечательные явления происходят для $n = 6$, в этом случае как длинный цикл, так и элемент цикленного типа $(3, 2, 1)$ имеют порядок 6. В то же время, как мы установили в предыдущем параграфе, они не сопряжены в S_6. Однако сюрпризы здесь не кончаются! Как мы знаем, количество 6-циклов в группе S_6 равно $5! = 120$. С другой стороны, количество элементов типа $(3, 2, 1)$ там равно $2!\binom{6}{3}\binom{3}{2} = 120$. Тем самым, порядки обоих классов элементов максимального порядка в S_6 равны. В действительности, как мы увидим в § 20, у группы S_6 существует внешний автоморфизм, переставляющий эти два класса. С этим явлением связано исключительное поведение групп S_5 и S_6, которое накладывает отпечаток на всю теорию симметрических групп.

Как уже было сказано, в случае $n \leq 4$ наибольший порядок в S_n имеет длинный цикл, так что $G(n) = n$. Однако, начиная с $n = 5$ жизнь становится веселее. Приведем несколько следующих значений $G(n)$, которые я обычно предлагаю вычислить студентам на практических занятиях по теории групп. Кроме того, в

рубрике `cycle type` указаны цикленные типы элементов наибольшего порядка:

n:	5	6	7	8	9	10	11
$G(n)$:	6	6	12	15	20	30	30
`cycle type:`	$(3,2)$	$(3,2,1)$ или (6)	$(4,3)$	$(5,3)$	$(5,4)$	$(5,3,2)$	$(5,3,2,1)$ или $(6,5)$

Вот еще несколько значений, которые легко вычисляются от руки:

n:	12	13	14	15	16	17	18
$G(n)$:	60	60	84	105	140	210	210
`cycle type:`	$(5,4,3)$	$(5,4,3,1)$	$(7,4,3)$	$(7,5,3)$	$(7,5,4)$	$(7,5,3,2)$	$(7,5,3,2,1)$ или $(7,6,5)$

Уильям Миллер обрывает свою таблицу в этом месте. Вычислим еще несколько значений $G(n)$, так как начиная с $n = 19$ они становится интереснее в нескольких отношениях (значения $G(n)$ для $n \geq 20$ вычислялись с помощью программы `Mathematica`). При этом мы будем указывать не все классы наибольшего порядка, а *какой-то* из них:

n:	19	20	21	22	23
$G(n)$:	420	420	420	420	840
`cycle type:`	$(7,5,4,3)$	$(7,5,4,3,1)$	$(7,5,4,3,1,1)$	$(7,5,4,3,1,1,1)$	$(8,7,5,3)$

Сразу бросаются в глаза два обстоятельства. Во-первых, появляется длинная серия $G(19) = G(20) = G(21) = G(22) = 420$ когда $G(n)$ не растет. Во-вторых, начиная с $n = 21$ известный нам контрпример, связанный с существованием двух классов сопряженности элементов максимального порядка, перестает быть единственным. Например, ясно, что элемент цикленного типа $(7,5,4,3,2)$ имеет то же порядок, что элемент цикленного типа $(7,5,4,3,1,1)$ (кстати, это служит контрпримером к заявлению на странице 501 статьи Миллера). В действительности в 1969 году Николя [213] доказал удивительный результат, утверждающий, что существуют сколь угодно длинные отрезки натурального ряда, на которых функция $G(n)$ постоянна! Приведем еще несколько значений $G(n)$, уже без указания соответствующих элементов: $G(24) = 840$, $G(25) = 1260$, $G(26) = 1260$, $G(27) = 1540$, $G(28) = 2310$, $G(29) = 2520$, $G(30) = 4620$, $G(31) = 4620$, $G(32) = 5460$, $G(33) = 5460$, $G(34) = 9240$, $G(35) = 9240$, $G(36) = 13860$, $G(37) = 13860$, $G(38) = 16380$, $G(39) = 16380$, $G(40) = 27720$. Ну и, как уже отмечалось в самом начале параграфа, $G(52) = 180180$ (вычисление этого значения в дуболомном стиле, использующем разложения на простые множители всех чисел до нескольких миллионов, требует около 7 минут машинного времени, используя задачу следующего параграфа будет быстрее сделать это вручную).

2. The prime connection. Как вычислялись эти значения? Пусть π — перестановка цикленного типа $(m_1, \ldots, m_s)$. Как мы знаем, $o(\pi) = m = \operatorname{lcm}(m_1, \ldots, m_2)$ является наименьшим общим кратным длин циклов. Сейчас мы убедимся в том,

что единственный интересный случай с точки зрения максимизации порядка — это случай примарных $m_1, \ldots, m_s$. Следующие соображения приводятся на страницах 500–501 работы Миллера.

Задача. Пусть $m = \operatorname{lcm}(m_1, \ldots, m_s)$ — наименьшее общее кратное натуральных чисел $m_1, \ldots, m_s \in \mathbb{N}$, а $m = {p_1}^{l_1} \ldots {p_s}^{l_s}$ — его каноническое разложение на простые. Докажите, что тогда

$$\operatorname{spread}(m) = {p_1}^{l_1} + \ldots + {p_s}^{l_s} \leq m_1 + \ldots + m_s.$$

Указание. По уровню и типу это образцовая задача районной олимпиады для 6-го класса, поэтому ограничимся следующим комментарием. Достаточно показать, что если $m_1, \ldots, m_s$ *не являются* степенями попарно различных простых, то существует другая последовательность натуральных чисел $(n_1, \ldots, n_t)$ такая, что $m = \operatorname{lcm}(n_1, \ldots, n_t)$, но при этом $n_1 + \ldots + n_t < m_1 + \ldots + m_s$.

Следствие 1. *В группе S_n тогда и только тогда существует элемент порядка m, когда* $\operatorname{spread}(m) \leq n$.

Это следствие можно сформулировать чуть иначе.

Следствие 2. *Если в группе S_n существует элемент порядка m, то в ней существует элемент порядка m, все длины нетривиальных циклов которого являются степенями попарно различных простых.*

В частности, это относится к элементам наибольшего порядка. Тем самым мы получаем следующую характеризацию $G(n)$, при помощи которой на компьютере легко вычислить первые несколько десятков значений этой функции.

Следствие 3. *Имеет место равенство $G(n) = \max(m)$, где максимум берется по всем $m \leq n!$ таким, что* $\operatorname{spread}(m) \leq n$.

3. Асимптотическое поведение $G(n)$. Итак, вычисление $G(n)$ сводится к теоретико-числовой задаче. Однако получение явной формулы для $G(n)$ представляется довольно сомнительным предприятием. Лучшее, на что мы можем надеяться, — это получение асимптотических оценок. Первый нетривиальный результат в этом направлении был получен Эдмундом Ландау [214], [215].

При $n \geq 3$ группа S_n не является циклической. Следующая теорема дает количественную оценку того, *насколько* она далека от циклической. Напомним, что две арифметические функции $f, g : \mathbb{N} \longrightarrow \mathbb{C}$ называются **асимптотичными** (`asymptotic`), если $\lim_\infty \frac{f}{g} = 1$ (понятие предела определено в книге III), в этом случае мы пишем $f \sim g$.

Теорема Ландау. $\ln(G(n)) \sim \sqrt{n \ln(n))}$

Первоначальное доказательство Ландау в полном объеме использовало теорему о распределении простых. В действительности позже были получены явные верхние оценки $G(n)$, причем Массиа [216] вычислил значение n, для которого отклонение $|\ln(G(n)) - \sqrt{n \ln(n)}|$ максимально. Заметим, что некоторые из этих оценок получены в предположении гипотезы Римана!

Теорема Ландау представляет собой один из исторически первых результатов в том направлении, которое сегодня принято называть **асимптотической теорией**

групп или **вероятностной теорией групп**. А именно, во многих ситуациях не удается явно вычислить различные функции, определяемые в терминах конкретной группы или класса групп (например, количество элементов данного порядка, количество слов данной длины относительно фиксированной системы образующих, количество подгрупп данного конечного индекса, и т. д.) В этом случае для таких функций стремятся получить асимптотики или оценки. Это направление, находящееся на стыке теории групп с комбинаторикой, теорией чисел и теорией вероятностей, долгое время апеллировало исключительно к аналитической технике и считалось достаточно маргинальным. До 60-х годов почти все работы на подобные темы были написаны венгерскими математиками. Однако за последние два-три десятилетия здесь был получен *фантастический* прогресс, связанный с классификацией конечных простых групп и внедрением мощных геометрических и алгебро-геометрических методов.

4. Что порождают две перестановки? Теорема Ландау говорит нам, что даже в лучшем случае одна перестановка $\pi \in S_n$ порождает не слишком большую подгруппу. В действительности дела обстоят *гораздо* хуже, и перестановки порядка $G(n)$ представляют собой большую редкость. В 1965 году Эрдёш и Туран [217] показали, что типичная перестановка имеет $\ln(n)$ циклов и логарифм ее порядка приблизительно равен $\ln(n)^2/2$.

> **Поль Туран** (Paul Turán, 28 августа 1910, Будапешт — 26 сентября 1976, ibid.) — замечательный венгерский математик, основные работы которого относятся к аналитической теории чисел, теории вероятностей, комбинаторике и асимптотической теории групп. В 1935 году под руководством Фейера он защищает диссертацию и в течение следующих лет публикует десятки блестящих статей по теории чисел, продолжающих исследования Харди и Рамануджана. Поскольку в Венгрии расовые законы были введены уже в 1920 году, на 13 лет раньше, чем в Германии, то будучи евреем — впрочем, в этом отношении он мало отличался от *всех* остальных **венгерских математиков** — Туран не мог получить вообще никакой позиции, даже в школе, и вынужден был преподавать в йешиве! С 1940 по 1944 год он провел в трудовом лагере, где придумал теорию экстремальных графов. Только в 1949 году, уже после избрания в Венгерскую Академию Наук, его, наконец, допустили к преподаванию в Будапештском университете!

Однако если взять не одну, а две перестановки, то с вероятностью 1 они порождают *очень* большую подгруппу. Вот типичный результат асимптотической теории групп, ставший классическим и послуживший образцом для десятков обобщений [218].

Теорема Диксона. *Вероятность того, что два элемента $\pi, \sigma \in S_n$ порождают S_n или A_n, стремится к 1, когда $n \longrightarrow \infty$.*

Разумеется, так как наугад выбранная перестановка принадлежит A_n с вероятностью $1/2$, то оговорка насчет A_n здесь существенна. Вероятность того, что две случайные перестановки порождают именно S_n, стремится к $3/4$. В действительности по модулю классификации конечных простых групп в 1989 году Бабаи получил значительно более точный результат.

Поль Эрдёш (Paul Erdös, урожденный Engländer, 26 марта 1913, Будапешт — 20 сентября 1996, Варшава) — замечательный венгерский математик, основные работы которого относятся к комбинаторике, теории чисел, теории графов, теории вероятностей и асимптотической теории групп.

Эрдёш опубликовал около 1500 работ, вероятно, это весьма близко к мировому рекорду, по крайней мере в области математики. Впрочем, большинство из этих работ написаны в соавторстве и очень короткие, часто 2-3 страницы. Обилие совместных работ мотивирует введение **числа Эрдёша**. Это число определяется рекурсивно следующим образом. Число Эрдёша самого Эрдёша равно 0. Тем математикам, у которых есть совместная статья с Эрдёшем, присваивается число Эрдёша 1. Тем математикам, кроме самого Эрдёша, у кого нет совместной статьи с Эрдёшем, но есть совместная статья с тем, у кого есть совместная статья с Эрдёшем — число 2 и т.д.

Широкой публике Эрдёш известен главным образом как один из самых неконвенциональных и забавных математиков XX века. Его родители были учителями математики и много лет он не посещал школу, а обучался дома. Несмотря на расовые законы, действовавшие в Венгрии с 1920 года, в 1930 году Эрдёшу как победителю национального конкурса все же разрешили поступить в один из университетов в Будапеште. Уже в 1934 году он защищает диссертацию и практически сразу уезжает вначале в Великобританию, а потом в США. С тех пор Эрдёш никогда не имел ни постоянного дома, ни постоянной работы.

В 1949 году Эрдёш одновременно с Атле Сельбергом находит элементарное доказательство закона распределения простых, однако (вопреки первоначальной договоренности!) Сельберг опережает его с публикацией в следующем году получает за эту работу Филдсовскую премию. В начале 1950-х годов Эрдёш уже *почти* получил постоянную работу в Университете Нотр-Дам, но попал в поле зрения *Комиссии по расследованию антиамериканской деятельности*, в результате чего ему было отказано в продлении американской визы. Между 1954 и 1963 годами он жил главным образом в Израиле, но в середине 1960-х годов ему все же удалось получить американскую визу и с тех пор он постоянно перемещался из одного университета в другой, живя дома у своих коллег. Эрдёшу приписывается огромное количество шуток и изречений, отличающихся крайней мизантропией и пессимизмом, что из этого было игрой, а что сказано всерьез, сейчас трудно судить.

Теорема Бабаи. *Вероятность того, что* $\pi, \sigma \in S_n$ *порождают* S_n *или* A_n *равна*

$$1 - \frac{1}{n} + O\left(\frac{1}{n^2}\right).$$

5. Цикл Зингера. Совершенно поразительно то обстоятельство, что в отличие от S_n для групп типа Ли наибольший порядок элемента в них легко явно вычислить. Это в точности наибольший среди порядков циклических торов в них. Например, в группе $\mathrm{GL}(n, q)$ с точностью до сопряженности имеется единственный циклический тор $\mathbb{F}_{q^n}^*$, отвечающий длинному циклу в S_n. Таким образом, наибольший порядок элемента в $\mathrm{GL}(n, q)$ равен $q^n - 1$. Любой элемент такого порядка называется **циклом Зингера**. Кроме теории конечных групп циклы Зингера играют громадную роль в комбинаторике, статистике, конечных геометриях и т. д.

В частности, $\mathrm{GL}(2,2) \cong S_3$, так что наибольший порядок элемента в S_3 равен $2^2 - 1 = 3$, что нас не должно удивлять. Мы обсуждаем явное построение цикла Зингера в книге IIB.

§ 8♢. Порождение S_n фундаментальными транспозициями

В настоящем параграфе мы покажем, что симметрическая группа порождается самыми простыми мыслимыми перестановками.

1. Транспозиции. Циклы длины 2 называются **транспозициями**. Таким образом, каждая транспозиция имеет вид $w_{ij} = (ij)$, $1 \leq i \neq j \leq n$, она переставляет элементы $i \neq j$ и оставляет все остальные элементы множества $\underline{n}$ на месте. Ясно, что $w_{ij} = w_{ji}$, так что в действительности различных транспозиций вдвое меньше, чем пар (i,j), $i \neq j$, они отвечают тем парам (i,j), в которых $i < j$. По определению каждая транспозиция является инволюцией, т. е. элементом порядка 2. Иными словами, $w_{ij}^{-1} = w_{ij}$

Теорема. *Группа S_n порождается транспозициями*

$$S_n = \langle (ij), i < j \rangle.$$

Доказательство. Мы уже знаем, что S_n порождается циклами, так что нам достаточно доказать, что каждый цикл является произведением транспозиций. Мы утверждаем, что в действительности каждый цикл длины l является произведением $l-1$ транспозиции. В самом деле, легко видеть, что

$$(i_1 i_2 \dots i_{l-1} i_l) = (i_1 i_2) \dots (i_{l-2} i_{l-1})(i_{l-1} i_l).$$

2. Фундаментальные транспозиции. Построенная в предыдущем пункте система образующих далеко не минимальна. В действительности, чтобы породить группу S_n, достаточно воспользоваться лишь частью транспозиций. Следующая система образующих S_n была детально изучена Коксетером и поэтому часто называется **коксетеровской системой образующих**. Назовем **фундаментальной транспозицией** транспозицию двух *соседних* символов,

$$s_i = w_{i,i+1} = (i, i+1), \qquad i = 1, \dots, n-1.$$

Теорема. *Группа S_n порождается фундаментальными транспозициями*

$$S_n = \langle s_1, \ldots, s_{n-1} \rangle.$$

Доказательство. В силу предыдущей теоремы нам достаточно доказать, что любая транспозиция w_{ij}, $i < j$, является произведением фундаментальных. Будем вести индукцию по $j - i$. База индукции $j - i = 1$, когда транспозиция w_{ij} сама является фундаментальной. Пусть $j - i \geq 2$, причем для всех транспозиций с меньшей разностью $j - i$ утверждение уже доказано. Так как $j - i \geq 2$, то можно найти такое h, что $j < h < j$. Легко видеть, что $w_{ij} = w_{ih} w_{hj} w_{ih}$, причем по индукционному предположению w_{ih} и w_{hj} уже являются произведениями фундаментальных транспозиций. Вот явная формула для w_{ij}, которая получается на этом пути:

$$w_{ij} = s_i \ldots s_{j-2} s_{j-1} s_{j-2} \ldots s_i.$$

Теорема полностью доказана.

Задача. Докажите, что группа S_n порождается $n - 1$ транспозицией (12), (13), $\ldots$, $(1n)$.

Задача. Докажите, что группу S_n невозможно породить менее, чем $n - 1$ транспозицией.

Задача. Докажите, что группа S_n порождается транспозицией (12) и длинным циклом $(123 \ldots n)$.

Задача. Верно ли, что группа S_n порождается длинным циклом $(123 \ldots n)$ и *любой* транспозицией? Найдите необходимое и достаточное условие для того, чтобы S_n порождалось длинным циклом $(123 \ldots n)$ и транспозицией $(1m)$.

Решение. Так как группа $H = \langle (123 \ldots n), (1m) \rangle$ содержит все транспозиции $(i, i + m - 1)$, то она содержит и все транспозиции вида $(i, i + j(m-1))$, где второй индекс понимается по модулю n. В случае, когда $d = \gcd(n, m-1) = 1$ можно выбрать j такое, что $j(m-1) \equiv 1 \pmod{n}$. Тем самым, в этом случае H содержит (12) и мы оказываемся в условиях предыдущей задачи. Если же $d \geq 2$, то разобьем $\underline{n}$ на d блоков $\{1, 1+d, \ldots, n-d+1\}$, $\{2, 2+d, \ldots, n-d+2\}$, $\ldots$, $\{d, 2d, \ldots, n\}$. Ясно, что как $(123 \ldots n)$, так и $(1m)$ переставляет блоки, так что никакое их произведение не может отобразить 1 в 2, оставив при этом $1+d$ на месте. Тем самым, H собственная подгруппа в S_n. В действительности можно доказать [219], что порядок H равен $d((n/d)!)^d$. Минимальный

пример, когда $d \geq 2$ – это группа $\langle (1234), (13) \rangle \leq S_4$ порядок которой равен 8.

Задача. Докажите, что группа S_n порождается транспозицией (12) и циклом $(23 \dots n)$.

§ 9♢. Знак перестановки, 1st instalment: декремент

В этом параграфе мы построим гомоморфизм $\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$.

1. Знак перестановки. Обозначим через $m = |\underline{n}/\sigma|$ число орбит перестановки $\sigma \in S_n$. По определению $m = r + s$, где r — количество истинных циклов перестановки σ, а $s = |\operatorname{Fix}(\sigma)|$. Разность $\operatorname{decr}(\sigma) = n - m$ называется **декрементом*** перестановки σ.

Определение. Знаком перестановки $\sigma \in S_n$ *называется*

$$\operatorname{sgn}(\sigma) = (-1)^{\operatorname{decr}(\sigma)} = (-1)^{n-m} = \prod_{i=1}^{m} (-1)^{|X_i|-1},$$

где произведение берется по **всем** *орбитам* $X_1, \dots, X_m$ *перестановки* σ.

Достоинством этого определения (см., например, [**120**], упр. 9 на с. 70) является то, что, с одной стороны, легко доказать его совпадение с обычным определением в терминах транспозиций (к которому мы вернемся в § 11), а с другой стороны, так как знак определен в терминах самой перестановки σ, вопроса о корректности при этом не возникает. В следующих параграфах мы дадим еще два определения знака, но проверить их корректность и совпадение друг с другом заметно сложнее. В некоторых старых книгах знак перестановки назывался ее **сигнатурой**, в связи чем в `Mathematica` знак перестановки x вычисляется посредством `Signature[`x`]`.

Теорема. *Пусть* $\tau_1, \dots, \tau_l$ — *транспозиции. Тогда* $\operatorname{sgn}(\tau_1 \dots \tau_l) = (-1)^l$.

---

*`Декремент` — уменьшение, убывание или понижение; **`инкремент`** — увеличение, возрастание, приращение. Эти понятия широко используются в языках программирования. Например, и в `C++` и в `Mathematica` через `x++` и `x--` обозначаются постфиксные инкремент и декремент (увеличение/уменьшение текущего значения x на 1 *после* выполнения вычисления), а через `++x` и `--x` — префиксные инкремент и декремент (увеличение/уменьшение текущего значения x на 1 *перед* выполнением вычисления).

Доказательство. Индукция по l. Случай $l \leq 1$ очевиден. Для индукционного перехода достаточно показать, что знаки $\tau_2 \dots \tau_l$ и $\tau_1 \dots \tau_l$ **различны**. Мы покажем, что если π — любая перестановка, а τ – транспозиция, то $\operatorname{sgn}(\tau\pi) = -\operatorname{sgn}(\pi)$. Достаточно показать, что число орбит изменяется на 1. Пусть $\tau = (pq)$. Орбиты π, не содержащие ни p, ни q, продолжают оставаться орбитами $\tau\pi$. Поэтому нам нужно рассмотреть следующие два случая: p, q лежат в различных орбитах, p, q лежат в одной орбите.

Если p, q лежат в различных орбитах, то

$$(pq)(pi_2 \dots i_r)(qj_2 \dots j_s) = (pi_2 \dots i_r qj_2 \dots j_s)$$

так что в этом случае две орбиты сливаются в одну.

Если p, q лежат в одной орбите, то

$$(pq)(pi_2 \dots i_r qj_2 \dots j_s) = (pi_2 \dots i_r)(qj_2 \dots j_s),$$

так что в этом случае одна орбита распадается на две.

Проанализировав это доказательство, внимательный читатель может заметить, что оно позволяет установить *значительно* более точное утверждение.

Задача. Пусть $d = \operatorname{decr}(\sigma)$. Докажите, что σ можно представить как произведение d транспозиций, причем d наименьшее число, обладающее этим свойством.

Таким образом, декремент перестановки σ есть *в точности* длина этой перестановки по отношению к множеству транспозиций, т. е. *наименьшее* число $d \in \mathbb{N}_0$ такое, что σ можно представить в виде произведения d транспозиций. Поскольку $m \geq 1$, декремент принимает наибольшее значение на множестве длинных циклов: длинные циклы и только они требуют для своего выражения $n - 1$ транспозиции.

§ 10◇. Знакопеременная группа

Знак позволяет нам определить важнейшую подгруппу в S_n.

1. Знакопеременная группа. Теперь мы в состоянии высказать самое **витальное**, что можно высказать об отображении групп.

Теорема. *Отображение* $\operatorname{sgn} : S_n \longrightarrow \{\pm 1\}$ *является гомоморфизмом.*

Доказательство. Если перестановку π можно представить как произведение l транспозиций, а перестановку σ — как произведения m

транспозиций, то, конкатенируя эти представления, мы выразим $\pi\sigma$ как произведение $l+m$ транспозиций. Таким образом,

$$\operatorname{sgn}(\pi\sigma) = (-1)^{l+m} = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma).$$

Назовем перестановку σ **четной**, если $\operatorname{sgn}(\sigma) = 1$, и **нечетной**, если $\operatorname{sgn}(\sigma) = -1$. Например, l-цикл требует для своего выражения $l-1$ транспозиции и, тем самым, цикл четной длины *нечетен*, а цикл нечетной длины *четен*. Ядро sgn называется **знакопеременной группой** и обозначается A_n (от первой буквы слова `alternating`). Этот термин был предложен Жорданом в 1870-х годах [210]. По определению A_n состоит из всех четных перестановок. Множество $S_n \setminus A_n$ всех нечетных перестановок образует смежный класс S_n по A_n в качестве представителя которого можно выбрать, например, любую транспозицию:

$$S_n = A_n \sqcup (S_n \setminus A_n) = A_n \sqcup A_n(12).$$

Для любого $n \geq 2$ группа A_n является подгруппой индекса 2 в S_n и, значит $A_n \trianglelefteq S_n$. Порядок группы A_n равен $n!/2$.

Задача. Постройте вложение S_n в A_{n+2}. Покажите, что S_n нельзя вложить в A_{n+1}.

2. Порождение A_n. По определению группа A_n порождается всевозможными произведениями двух различных транспозиций $(ij)(hk)$. Однако обычно удобнее пользоваться другой системой образующих.

Теорема. *При любом $n \geq 3$ группа A_n порождается 3-циклами.*

Доказательство. Для доказательства теоремы нам нужно выразить произведение двух транспозиций $(ij)(hk)$ как произведение 3-циклов. Если $|\{i,j,h,k\}| = 3$, то это произведение само является 3-циклом. С другой стороны, если $|\{i,j,h,k\}| = 4$, то $(ij)(hk) = (ij)(ih)(ih)(hk)$ является произведением двух 3-циклов.

Задача. Докажите, что группа A_n порождается 3-циклами (123), (124), $\ldots$, $(12n)$.

Задача. Докажите, что группа A_n порождается 3-циклами (123), (234), $\ldots$, $(n-2, n-1, n)$.

Указание. Группа A_n порождается подгруппой A_{n-1}, стабилизирующей n, и одним (любым) циклом, перемещающим n.

Задача. Пусть n нечетно, верно ли, что группа A_n порождается 3-циклами (123), (145), $\ldots$, $(1, n-1, n)$?

Задача. Докажите, что группа A_n порождается 3-циклом (123), и либо длинным циклом $(12\dots n)$ при нечетном n, либо циклом $(23\dots n)$ при четном n.

Задача. Покажите, что при $n \geq 4$ центр группы A_n тривиален.

Решение. Для любого $\pi \neq \mathrm{id}$ найдется i такое, что $\pi(i) \neq i$. Так как $n \geq 4$, то найдутся j, h такие, что все четыре индекса $i, \pi(i), j, h$ различны. Тогда $\pi(ijh)\pi^{-1} = (\pi(i), \pi(j), \pi(h)) \neq (i, j, h)$.

Задача. Докажите, что при $n \geq 5$ все 3-циклы в A_n сопряжены. Верно ли это для $n = 4$?

Решение. Мы уже знаем, что 3-циклы сопряжены в S_n. Пусть (ijh) и (klm) — два любых 3-цикла, а $\pi \in S_n$ – перестановка такая, что $\pi(ijh)\pi^{-1} = (klm)$. Если перестановка π четна, мы достигли своей цели. Если перестановка π нечетна, но $n \geq 5$, то найдутся такие r, s, что все 5 индексов i, j, h, r, s различны. Тогда (rs) коммутирует с (ijh) и, тем самым, $\pi(rs)(ijh)(\pi(rs))^{-1} = (klm)$, причем $\pi(rs)$ четна. С другой стороны, централизатор 3-цикла содержит по крайней мере 3 элемента, поэтому в A_4 имеется не более $12/3 = 4$ циклов, сопряженных с данным. Это значит, что 3-циклы в A_4 разбиваются на два класса сопряженности.

§ 11♢. Знак перестановки, 2^{nd} instalment: транспозиции

> Мне, конечно, легче сойти с ума, чем им. Я, например, увижу на карте Пакистана: там, где должен быть Исламабад — там оказалось Равалпинди, а там, где прежде было Равалпинди, увижу Исламабад — и все, я сбрендил. А они все даже не заметят.
>
> Венедикт Ерофеев. *Из записных книжек*

Забудем про определение из § 9 и дадим другое определение знака.

Определение. *Положим* $\mathrm{sgn}(\sigma) = (-1)^l$, *если* σ *можно представить как произведение* l *транспозиций* $\sigma = \tau_1 \dots \tau_l$.

Как мы знаем, это определение эквивалентно нашему основному определению через декремент.

1. Корректность определения знака. Однако, из нашего нового определения совершенно неясно, почему знак определен **корректно**, т. е. почему перестановку σ нельзя представить в виде

$$\sigma = \tau_1 \dots \tau_l = \rho_1 \dots \rho_m,$$

где l и m имеют разную четность? Чтобы проиллюстрировать метод совместной индукции, сейчас мы проведем *еще одно* доказательство корректности, не зависящее от результатов § 9.

Теорема. *Знак перестановки $\sigma \in S_n$ определен корректно. Иными словами, если σ можно представить в виде произведения l транспозиций и m транспозиций, то $l \equiv m \pmod 2$.*

Доказательство. В самом деле, пусть $\sigma = \tau_1 \dots \tau_l = \rho_1 \dots \rho_m$. Так как транспозиции имеют порядок 2, то $\rho^{-1} = \rho$ для любой транспозиции и, следовательно, $\sigma^{-1} = \rho_m \dots \rho_1$. Таким образом,

$$e = \sigma\sigma^{-1} = \tau_1 \dots \tau_l \rho_m \dots \rho_1,$$

есть произведение $l + m \equiv l - m \pmod 2$ транспозиций. Поэтому достаточно показать, что если тождественная перестановка e есть произведение m транспозиций $e = \tau_1 \dots \tau_m$, то m четно.

Для доказательства этого мы проведем совместную индукцию по n, m и еще одному параметру, который появится позднее. **База индукции по n:** в случаях $n = 1, 2$ утверждение очевидно. Для $n = 1$ транспозиций нет вообще, так что длина каждого представления тождественной перестановки в виде произведения транспозиций равна 0. Для $n = 2$ имеется одна транспозиция, $\tau = (12)$, четные степени которой совпадают с e, а нечетные — с τ.

Шаг индукции по n: предположим, что для группы S_{n-1} теорема уже доказана. Если символ n не входит ни в одну из транспозиций $\tau_1, \dots, \tau_n$, то все эти транспозиции живут в подгруппе $S_{n-1} \leq S_n$, стабилизирующей символ n и можно применить индукционное предположение. Таким образом, какая-то транспозиция τ_l имеет вид (pn) для некоторого $p \neq n$. Рассмотрим самую правую среди таких транспозиций, т. е. транспозицию с **наибольшим** номером l. Сейчас мы покажем, что либо m, либо l можно уменьшить — это вариант совместной индукции, называемый **методом бесконечного спуска**.

Спуск по l, m: пусть теперь $m \geq 2$ и пусть $\tau_l = (pn)$, $\tau_{l-1} = (rs) = (sr)$. Рассмотрим три случая, в зависимости от порядка пересечения $t = |\{p, n\} \cap \{r, s\}|$, который может принимать значения 0,1,2.

Случай $t = 0$. Транспозиции τ_l и τ_{l-1} *независимы*. Тем самым, $\tau_{l-1}\tau_l = \tau_l\tau_{l-1}$ и, значит, в произведении $\tau_1 \dots \tau_m$ можно переставить множители τ_{l-1} и τ_l, при этом самый правый множитель, перемещающий n, будет иметь номер $l - 1$.

Случай $t = 1$. С точностью до перестановки r и s можно считать, что $\tau_{l-1} = (ns)$ или $\tau_{l-1} = (ps)$ для некоторого $s \neq p, n$. Однако в этих случаях произведение $\tau_{l-1}\tau_l$ можно переписать в виде $(ns)(np) = (np)(ps)$ и $(ps)(np) = (ns)(ps)$ (эти тождества легко проверяются в группе S_3 перестановок символов s, p, n). Таким образом, в каждом из этих случаев снова можно переписать произведение $\tau_1 \dots \tau_n$ так, чтобы самый правый множитель, перемещающий n, имел номер $l - 1$.

Случай $t = 2$. При этом $\tau_l = \tau_{l-1}$ так что $\tau_{l-1}\tau_l$ в произведении $\tau_1 \dots \tau_m$ можно сократить, выразив при этом e в виде произведения $m - 2$ транспозиций.

Итак, для любого выражения e как произведения $m \geq 2$ транспозиций осуществима одна из этих редукций. Ясно, что случай $l = 1$ невозможен. В самом деле, тогда τ_1 является единственной среди транспозиций τ_i, перемещающей n, так что $\tau_1 \dots \tau_m(n) = p$ и, значит, это произведение не может равняться e. Поэтому на

каком-то шаге нам удастся уменьшить m на 2. Это значит, что проделав все редукции в исходном произведении, мы получим выражение для e как произведение 0 либо 1 транспозиций. Однако случай $m = 1$ невозможен так как e не является транспозицией. Тем самым, последовательно уменьшая m на 2 мы должны дойти до 0. Но это и значит, что m четно. Теорема полностью доказана.

2. Единственность знака. Сейчас мы покажем, что знак вполне характеризуется тем, что это гомоморфизм, переводящий транспозиции в -1.

Теорема. *Для любого $n \geq 2$ знак* sgn *является единственным нетривиальным гомоморфизмом $\varphi : S_n \longrightarrow \{\pm 1\}$.*

Доказательство. В самом деле, пусть (pq), (rs) – две транспозиции в S_n, а π — любая перестановка такая, что $\pi(p) = r$, $\pi(q) = s$. Тогда $\pi(pq)\pi^{-1} = (rs)$, так что при всех гомоморфизмах $\varphi : S_n \longrightarrow \{\pm 1\}$ в абелеву группу $\{\pm 1\}$ транспозиции принимают одно и то же значение. Если это значение равно 1, то гомоморфизм φ тривиален. Если же оно равно -1, то $\varphi = \mathrm{sgn}$.

Следствие. *При $n \geq 2$ знакопеременная группа A_n является единственной подгруппой индекса 2 в S_n.*

§ 12♢. Знак перестановки, 3rd instalment: инверсии

Здесь мы дадим третье определение знака перестановки, в терминах длины этой перестановки по отношению к множеству фундаментальных транспозиций.

1. Инверсии. Пара (i, j) образует **инверсию** (`inversion`, `Fehlstand`) для перестановки $\sigma \in S_n$, если $i < j$, но $\sigma(i) > \sigma(j)$. Обозначим через $\mathrm{inv}(\sigma)$ общее **число инверсий** перестановки σ, т. е. количество всех пар (i, j), $1 \leq i < j \leq n$, образующих инверсию для σ.

Комментарий. Многие авторы называют инверсией не саму пару (i, j), а ее образ $(\sigma(i), \sigma(j))$ под действием σ. Кнут [207] утверждает, что понятие инверсии ввел в 1750 году Крамер в книге *Introduction à l'analyse des lignes courbes algébriques*. В действительности, трудно себе представить, чтобы Секи Кова и фон Лейбниц не владели этим понятием лет за 70 до Крамера, когда они одновременно (и, насколько мы в состоянии судить, независимо) ввели понятие определителя. Однако в шпенглеровском смысле понятие инверсии гораздо старше и уже абсолютно отчетливо выступает в китайских текстах III в. до н.э.

Габриэль Крамер (Gabriel Cramer, 31 июля 1704, Женева — 4 января 1752, Баньоль) — выдающийся швейцарский математик. После обучения в университете Женевы он стал там профессором философии и математики и занимал высокие муниципальные должности. В его главном труде *Introduction à l'analyse des lignes courbes algébriques*, излагается, в частности, решение систем уравнений и теория определителей. В нашем курсе несколько раз упоминается формула Крамера для обратной матрицы над коммутативным кольцом.

Такакадзу Секи Кова (Takakazu Seki Kowa, 1642, Фудзиока — 24 октября 1708, Эдо, ныне Токио) — замечательный японский математик, основные интересы которого относились к алгебре и теории чисел (решение уравнений и систем уравнений, диофантовы уравнения, и т.д.). Одновременно с Лейбницем он изучал определители и одновременно с Бернулли — числа Бернулли. Однако, в условиях изоляции Японии ни его открытия не были известны в Европе, ни он не знал о работах европейских математиках.

Теорема. *Для любой перестановки* $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$

Первое доказательство теоремы. Каждая транспозиция есть произведение нечетного числа фундаментальных транспозиций. Умножение на фундаментальную транспозицию создает или убивает ровно одну инверсию.

В действительности, и в этом случае можно высказать гораздо более точное утверждение.

Задача. Пусть $d = \mathrm{inv}(\sigma)$. Докажите, что σ можно представить как произведение d фундаментальных транспозиций, причем d наименьшее число, обладающее этим свойством.

Теперь мы в состоянии дать еще одно определение знака перестановки – можно думать, что это определение является пародией, но в действительности, оно взято из учебника "высшей алгебры" Куроша:

$$\mathrm{sgn}(\sigma) = \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j}.$$

При всей своей неестественности[♮] это определение обладает одним

[♮]Эпитет **неестественность** относится не к выражению $(-1)^{\mathrm{inv}(\sigma)}$ как таковому, **наоборот**, с точки зрения теории групп Вейля $\mathrm{inv}(\sigma)$ совпадает с $n(\sigma)$, числом положительных корней, которые становятся отрицательными под действием σ и, тем самым, с $l(\sigma)$ — длиной σ в Коксетеровских образующих. Нет ничего естественнее **этого** определения! Однако выражать $(-1)^{\mathrm{inv}(\sigma)}$ как дурацкое произведение!!! Такое определение было бы уместно в учебнике математического анализа, как часть общей перверсивно-декадентской парадигмы. Но цель курса алгебры прямо противоположна — культивировать радость, силу, вкус и привычку к естественности!

Готтфрид фон Лейбниц (Gottfried Wilhelm von Leibniz, 1 июля 1646, Лейпциг — 14 ноября 1716, Ганновер) — ключевая фигура в развитии математики и всей Европейской культуры. Кроме математики он занимался лингвистикой, историей, философией, геологией, был юристом, дипломатом и архивистом Ганноверской фамилии. Непосредственными учениками Лейбница были братья Бернулли, в свою очередь Леонард Эйлер был непосредственным учеником Иоганна Бернулли. Таким образом, вся Петербургская математика восходит к школе Лейбница.

Каждый, кто хоть раз в жизни открывал [какие-то из] 90 томов сочинений фон Лейбница, понимает, насколько бессмысленно пытаться в нескольких словах охарактеризовать его научную продукцию — или вообще высказывать какие-либо суждения о его **океанической** деятельности. В том, что касается конкретно математики, к нему восходят даже не десятки, а *сотни* понятий, терминов и обозначений в университетских курсах, в том числе вещественное число, функция, перестановка, определитель, дифференцирование кольца, производная, интеграл, дифференциальные уравнения, алгоритм, координаты, алгебраическое versus трансцендентного, мультиномиальные коэффициенты, булевы операции, круги Эйлера, пустое множество, знаки суммы и произведения, кванторы, законы де Моргана, etc., etc., etc. Только очень немногочисленные из этих понятий и результатов официально носят его имя: формула Лейбница, формула Ньютона—Лейбница, признак Лейбница ...

Наиболее известным широкой публике достижением Лейбница является создание им в 1663–1676 годах дифференциального и интегрального исчисления. Интегрирование было известно уже Архимеду, а дифференцирование изобретено Ферма, однако никто до Ньютона и Лейбница не замечал связи между этими операциями. Каждому, кто заглядывал в их тексты, ясно, что они пришли к этим идеям абсолютно разными путями: Ньютон из механических аналогий, а Лейбниц посредством чистого умозрения и прямого контакта с миром идей в форме откровения. Именно в этот момент математика окончательно отделилась от физики и начала свое независимое существование. Физики пошли за Ньютоном, математики за Лейбницем. Именно Лейбниц ввел обозначения $\int$ и dx, которыми мы пользуемся и сегодня.

В 1679 в связи с поисками "универсального метода", который должен свести рассуждения к вычислениям, и под влиянием увлечения китайской философией, в частности школой **инь-янг** и непосредственно *И Цзин*, Лейбниц развил двоичную арифметику. Провозглашенный им лозунг заменить идеи вычислениями, как и сформулированный Дирихле антитезис заменить вычисления идеями, в наше время окончательно совместились в слогане соединить идеи с вычислениями. Для меня совершенно очевидно, что именно Лейбниц своим необузданным, но компетентным и дисциплинированным визионерством создал ту математику, которую мы знаем сегодня. Ту математику, которая изучает не *числа и фигуры*, а все в области чистого умозрения, что поддается точному определению.

Из других замечательных документов, полностью сохранивших свою актуальность и сегодня, можно упомянуть написанную им для Петра I памятную записку на тему *Как нам обустроить Россию*, в которой он выделяет две самых важных для благополучия России задачи, повышение уровня образования и рост народонаселения.

техническим преимуществом, а именно, для этого определения очевидно, что sgn является гомоморфизмом. Для этого нужно лишь заметить, что в действительности произведение в этой формуле берется по $\{i,j\} \in \bigwedge^2(\underline{n})$. В частности, для любой перестановки π имеем

$$\prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = \prod_{1\le \pi(i)<\pi(j)\le n} \frac{\sigma(i)-\sigma(j)}{i-j}$$

Это значит, что следующее свойство получается даром.

Лемма. *Отображение* $(-1)^{\mathrm{inv}} : S_n \longrightarrow \{\pm 1\}$, $\pi \mapsto (-1)^{\mathrm{inv}(\pi)}$, *является гомоморфизмом.*

Доказательство. В самом деле,

$$(-1)^{\mathrm{inv}(\pi\sigma)} = \prod_{1\le i<j\le n} \frac{\pi\sigma(i)-\pi\sigma(j)}{i-j} =$$
$$= \prod_{1\le i<j\le n} \frac{\pi\sigma(i)-\pi\sigma(j)}{\sigma(i)-\sigma(j)} \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{\mathrm{inv}(\pi)}(-1)^{\mathrm{inv}(\sigma)}.$$

Второе доказательство теоремы. Как мы только что показали, отображение $(-1)^{\mathrm{inv}}$ является гомоморфизмом $S_n \longrightarrow \{\pm 1\}$. Этот гомоморфизм нетривиален, так как, например, у транспозиции $\tau = (1,2)$ всего одна инверсия, и, следовательно, $(-1)^{\mathrm{inv}(\tau)} = -1$. В силу единственности знака гомоморфизм $(-1)^{\mathrm{inv}}$ *обязан* совпадать с sgn.

§ 13♢. Знак перестановки, 4th instalment: определитель

Традиционно знак перестановки используется для того, чтобы написать знакопеременную формулу для определителя матрицы $x = (x_{ij})$:

$$\det(x) = \sum_{\pi\in S_n} \mathrm{sgn}(\pi) x_{1,\pi(1)} x_{2,\pi(2)} \dots x_{n,\pi(n)}.$$

Однако, известны десятки других способов ввести определитель матриц, которые не опираются на понятие знака перестановки (по Лапласу, по Грассману, по Вейерштрассу, по Дьедонне, и т. д.) В настоящем параграфе мы покажем, что знак перестановки является частным случаем определителя.

1. Матрицы перестановки. В книге IV, посвященной линейной алгебре, нам встречаются `элементарные преобразования третьего типа`, которые переставляют две строки или два столбца матрицы x. Такие преобразования реализуются умножением на матрицы вида

$$w_{ij} = e - e_{ii} - e_{jj} + e_{ij} + e_{ji},$$

где $1 \leq i \neq j \leq n$. Подгруппа в G, порожденная всеми w_{ij}, обозначается через $W = W_n$ и называется группой **матриц перестановки** (или, все же, **матриц-перестановок**? — английский оригинал, `permutation matrices`, прямолинеен и лишен `эк[в]ивоков` = `equivoco`). Она состоит из всех матриц, у которых в точности один ненулевой коэффициент в каждой строке и каждом столбце, причем этот ненулевой коэффициент равен 1. Эта группа естественно изоморфна симметрической группе S_n. А именно, для перестановки $\pi \in S_n$ обозначим через (π) матрицу перестановки, элемент которой в позиции (i, j) равен $\delta_{i,\pi(j)}$.

Задача. Докажите, что отображение $S_n \longrightarrow W_n$, $\pi \mapsto (\pi)$ является изоморфизмом. Выведите отсюда, что для матрицы перестановки обратная совпадает с транспонированной.

2. Знак перестановки. Теперь совершенно ясно, как определить знак перестановки. Матрица w_{ij} — это в точности образ транспозиции (i, j) и ее определитель равен -1. Таким образом, для любого поля характеристики $\neq 2$ мы можем определить сквозной гомоморфизм $S_n \longrightarrow \mathrm{GL}(n, K) \longrightarrow K^*$, $\pi \mapsto (\pi) \mapsto \det(\pi)$.

Задача. Докажите, что $\mathrm{sgn}(\pi) = \det(\pi)$.

Решение. Композиция двух гомоморфизмов — гомоморфизм. Так как W_n порождается w_{ij}, а $\det(w_{ij}) = -1$, то это гомоморфизм в $\{\pm 1\}$, причем нетривиальный. Но из § 11 мы уже знаем, что sgn является *единственным* нетривиальным гомоморфизмом из S_n в $\{\pm 1\}$.

В действительности, описанная реализация перестановок матрицами позволяет *естественно* истолковать и все остальные понятия. Более того, это и есть правильный подход к комбинаторике S_n, хотя и чуть витиевато сформулированный. Введем следующее обозначения:

$$\Phi^+ = \{(i, j) \mid 1 \leq i < j \leq n\}, \qquad \Phi^- = \{(i, j) \mid 1 \leq j < i \leq n\}.$$

Группа S_n естественно действует на множестве $\Phi = \Phi^+ \sqcup \Phi^-$ — по причинам, которые станут нам ясны в книге IIB, это множество называется **системой корней** типа A_{n-1}. А именно, $\pi(i, j) = (\pi(i), \pi(j))$. Теперь мы можем выразить число инверсий как $\mathrm{inv}(\pi) = |\pi(\Phi^+) \cap \Phi^-|$.

§ 14♡. Игра в 15

В начале 1870-х годов американский изобретатель головоломок Сэм Лойд предложил пермутационную игру известную как **игра в 15**. Эта игра оставалось чрезвычайно популярной до 1950-х годов, а в последние годы снова возродилась в некоторых марках мобильных телефонов. Игра состоит в следующем. В квадратной коробочке размера 4×4 размещены 15 квадратных фишек 1×1 с номерами $1, 2, 3, \ldots, 15$, а одно место остается свободным. Последовательно сдвигая фишки на свободное место, требуется расставить их в **стандартном порядке**:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	$*$

где через $*$ обозначено свободное место. Пусть теперь

i_1	i_2	i_3	i_4
i_5	i_6	i_7	i_8
i_9	i_{10}	i_{11}	i_{12}
i_{13}	i_{14}	i_{15}	$*$

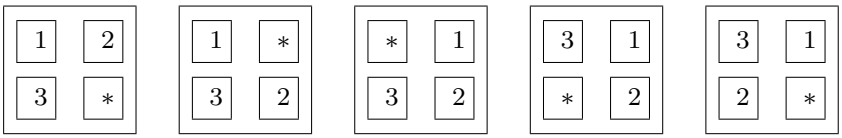
какая-то другая расстановка фишек, при которой свободное место расположено в правом нижнем углу. Такая расстановка отвечает перестановке $\pi \in S_{15}$ такой, что $\pi(j) = i_j$. Требуется узнать, является ли эта расстановка фишек **допустимой**, т. е. можно ли от нее легальными ходами перейти к стандартной расстановке. В частности, Лойд предложил награду в \$1000 тому, кто сможет решить **трудный случай** головоломки, т. е. привести к стандартному виду расстановку

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	$*$

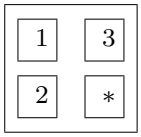
В 1879 году Джонсон и Стори опубликовали математическую теорию этой игры, из которой, в частности, следует, что поставленная Лойдом задача неразрешима, см.,

например [220], ?? . Так как мы можем выполнить любую композицию легальных ходов и обратных к ним, то допустимые перестановки образуют подгруппу в S_{15} и мы хотим найти эту подгруппу.

Из методических соображений и так как это понадобится нам в доказательстве, начнем с анализа **игры в 3**, которая отличается от игры в 15 тем, что в коробочке 2×2 расположены **три** фишки размера 1×1. Ясно, что следующие перестановки фишек



образуют последовательность легальных ходов. Применяя ту же последовательность ходов еще раз, мы убеждаемся, что оба цикла $(1, 2, 3)$ и $(1, 3, 2)$ являются допустимыми перестановками, так что от любой перестановки можно перейти к такой, для которой $\pi(1) = 1$. С другой стороны, перейти легальными ходами от перестановки



к единичной перестановке невозможно. Это наводит нас на мысль, что скорее всего справедлив следующий результат.

Теорема. *Расстановка фишек в том и только том случае является допустимой, когда перестановка π четная.*

Набросок доказательства. **Необходимость.** С точки зрения группы S_{16}, действующей на множестве $\{1, 2, 3, \ldots, 15, *\}$, любой легальный ход является транспозицией. Однако не каждая транспозиция отвечает легальному ходу. Будем нумеровать позиции в коробочке парами (i, j), где $i, j = 1, \ldots, 4$ суть, соответственно, номера строки и столбца. При каждой легальной транспозиции сумма номеров строка и столбца, в которых расположена $*$ меняется на 1. Так как нас интересуют только такие расстановки, у которых $*$ расположена в позиции $(4, 4)$, для перехода от одной такой расстановки к другой требуется четное число транспозиций.

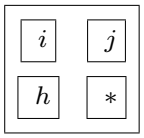
Достаточность. Так, как каждый из циклов

- $(1, 2, 6, 10, 11, 7, 3, 4, 8, 12, *, 15, 14, 13, 9, 5)$,
- $(2, 3, 4, 8, 12, *, 15, 14, 10, 6)$,
- $(3, 4, 8, 12, *, 15, 11, 7)$,
- $(5, 6, 7, 8, 12, *, 15, 14, 13, 9)$,
- $(9, 10, 11, 12, *, 15, 14, 13)$

получается последовательностью легальных ходов, то применяя какую-то их комбинацию, мы можем считать, что наша расстановка отвечает перестановке, в которой $\pi(1) = i$, $\pi(2) = j$, $\pi(5) = h$. Применив теперь какое-то произведение циклов

- $(6, 7, 8, 12, *, 15, 14, 10)$,
- $(11, 12, *, 13)$,

мы можем считать, что, кроме того, $\pi(6) = *$. Таким образом, мы приходим к расстановке, в которой левый верхний угол выглядит так



Как мы уже знаем, из такой конфигурации ходами в левом верхнем углу мы можем получить 3-цикл (i, j, h). Проделывая теперь те же ходы, которые понадобились нам, чтобы поставить $i, j, h, *$ в левый верхний угол, в обратном порядке, мы видим, что наша группа допустимых расстановок содержит 3-цикл (i, j, h), для любых трех попарно различных индексов $i, j, h = 1, \ldots, 15$. Но ведь 3-циклы порождают знакопеременную группу A_{15}.

Задача. Восстановите все детали в предшествующем рассуждении.

Задача (ibid., задача 6 на стр.104). Предположим, что на фишках для игры в 15 вместо чисел написаны буквы **и,г,р,а,в,п,я,т,н,а,д,ц,а,т,ь**. Покажите, что от любой расстановки фишек можно легальными ходами перейти к такой расстановке, чтобы при этом получался текст **игра в пятнадцать**[♮].

Задача (ibid., задачи 9,10 на стр.104). Проведите аналогичный анализ игры в 8, игры в 24, игры в 35, ...

§ 15◇. Транзитивность

В настоящем параграфе мы совсем коротко обсудим свойства транзитивности групп перестановок. На русском языке дальнейшие детали и ссылки можно найти, например, в статье [221].

1. Транзитивность. Пусть $G \leq S_n$ — группа перестановок множества $X = \underline{n}$. Говорят, что группа G **транзитивна**, если для любых $x, y \in X$ существует перестановка $\pi \in G$ такая, что $\pi(x) = y$. В противном случае группа G называется **интранзитивной**.

Задача. Докажите, что степень транзитивной группы перестановок $G \leq S_n$ делит ее порядок.

Решение. Пусть $H = G_n$ — стабилизатор точки $n \in \underline{n}$. Тогда $|G : H| = n$.

Задача. Докажите, что транзитивная группа всегда содержит перестановку без неподвижных точек.

Решение. Пусть, как и в предыдущей задаче, G_i — стабилизатор точки $i \in \underline{n}$. Так как все группы G_i сопряжены, то их порядки равны,

[♮]Как и при чтении китайского текста, пробелы здесь являются позднейшей интерполяцией, между фишками в коробочке никаких пробелов нет.

обозначим их общий порядок через m. Как мы убедились в предыдущей задаче, $|G| = mn$. Но $|G_1 \cup \ldots \cup G_n| \leq n(m-1)+1 < |G|$, так как 1 принадлежит всем группам G_i. Это значит, что найдется перестановка $\pi \in G$, которая не принадлежит ни одной группе G_i.

Задача. Докажите, что если $G \leq S_n$ — транзитивная группа перестановок, порожденная транспозициями, то $H = S_n$.

Задача. Покажите, что если $G \leq S_n$ — транзитивная группа перестановок, а $H \trianglelefteq G$, то любые две орбиты группы H содержат одно и то же количество элементов.

Задача. В условиях предыдущей задачи покажите, что если $n = p$ — простое число, а $H \neq e$, то группа H тоже транзитивна.

2. Подгруппы индекса n в S_n. Группа S_5 вкладывается в S_6 как стабилизатор точки 6, однако это действие не является транзитивным. Оказывается, у группы S_5 есть еще одно вложение в S_6, не сопряженное с этим вложением.

Задача. Построить транзитивное действие S_5 на 6 символах.

Решение 1. Любая подгруппа порядка 5 в S_5 состоит из тождественной перестановки и четырех 5-циклов. Так как две различные подгруппы порядка 5 пересекаются по тождественной перестановке, а общее количество 5-циклов в S_5 равно $4! = 24$, всего в S_5 имеется 6 таких подгрупп. Мы уже знаем, что действие S_5 сопряжениями на множестве таких подгрупп (и даже на множестве их образующих!) транзитивно.

Решение 2. В связи с анализом группы Рубика нам будет полезно доказать, что группа, порожденная $(1,2,3,4)$ и $(1,2,5,6)$, изоморфна S_5.

Заметим, что при $n \geq 5$ это *единственное* исключение. Как мы уже знаем, A_n является единственной подгруппой в S_n индекса 2. Оказывается, как правило, в S_n ровно 2 подгруппы индекса $\leq n$ с точностью до сопряженности.

Теорема Бертрана. *При $n \geq 5$ группа S_n не содержит никаких подгрупп H таких, что $2 < |S_n : H| < n$. Единственная с точностью до сопряженности подгруппа индекса n в $G = S_n$ есть $G_n = S_{n-1}$, за исключением случая $n = 6$.*

Доказательство самого Бертрана [222] основывалось на следующем предположении, которое он проверил для всех $n < 1500000$, но доказательством которого в общем случае он не владел.

Жозеф Бертран (Joseph Louis François Bertrand, 11 марта 1822, Париж — 3 апреля 1900, ibid.) — известный французский математик, основные работы которого относятся к теории вероятностей и дифференциальной геометрии. Его книга *Calcul des probabilités* содержит первую формулировку того, что сегодня известно как **парадокс Бертрана**.

Постулат Бертрана. *При $n > 7$ между $n/2$ и $n-2$ всегда содержится хотя бы одно простое число.*

Доказательство постулата Бертрана было получено в 1852 году П. Л. Чебышевым [223].

Пафнутий Львович Чебышёв (16 мая 1821, село Окатово под Калугой — 8 декабря 1894, Санкт-Петербург) — великий русский математик, один из основателей Петербургской математической школы. Основные работы Чебышева относятся к алгебре и теории чисел, анализу, теории аппроксимации, теории вероятностей, прикладной математике и механике. После окончания Московского университета и защиты в 1846 году магистерской диссертации на тему *Опыт элементарного анализа теории вероятностей* он получает позицию в Санкт-Петербургском университете, с которым и связана вся его дальнейшая карьера. В 1849 году он получает докторскую степень за свою замечательную книгу *Теория сравнений*. Именно к этому периоду относятся его знаменитые работы по теории чисел: только что упомянутое доказательство постулата Бертрана, результаты по асимптотическому распределению простых и т.д. В середине 1850-х годов он начинает интересоваться задачами аппроксимации (многочлены Чебышева, чебышевские системы, ...) Важнейшие результаты принадлежат ему и в теории вероятностей (неравенство Чебышева, закон больших чисел, метод моментов, ...) Кстати, именно в процессе работы над задачами теории вероятностей он ввел ключевое понятие алгебры — свертку.

Чебышев может с полным правом считаться основателем российской алгебры и теории чисел. Непосредственными учениками Чебышева были замечательные теоретико-числовики Коркин, Золотарев, Марков, Вороной, от которых и есть пошла Петербургская школа алгебры и теории чисел, а также Ляпунов, Стеклов и другие Петербургские математики. Так Граве был учеником Коркина и Золотарева, а учениками Граве в Киеве были Делоне, Шмидт, Чеботарев и Островский. Делоне вернулся в Петербург, где его учеником стал Дмитрий Константинович Фаддеев, все работающие сегодня алгебраисты в Петербурге его дети, внуки и правнуки. С другой стороны, Шмидт уехал в Москву, где основал алгебраическую школу в Московском университете.

Сегодня постулат Бертрана обычно формулируется в чуть более слабой форме, как существование простого p между n и $2n$, причем обычно воспроизводится доказательство Эрдёша [224]. Однако, тем временем Серре нашел доказательство теоремы Бертрана, не опирающееся на постулат Бертрана [225].

Жозеф Серре (`Joseph Alfred Serret`, 30 августа 1819, Париж — 2 марта 1885, Версаль) — знаменитый французский математик, основные работы которого относятся к дифференциальной геометрии (формулы Френе—Серре), механике, анализу, группам перестановок и теории чисел. Репутация Серре связана главным образом с его учебником *Cours d'algèbre supérieur*, который в течение полувека (до появления учебника Вебера *Lehrbuch der Algebra*) оставался de facto *стандартным* учебником алгебры. Первое издание этой замечательной книги появилось в 1849 году и насчитывало всего 400 страниц, к моменту публикации пятого издания в 1885 году объем книги вырос в три раза. Именно Серре ввел изучение групп перестановок в университетский курс алгебры. Еще один грандиозный осуществленный им проект — публикация работ Лагранжа в 14 томах.

§ 16♡. Кратная транзитивность

1. Кратная транзитивность. Более общо, пусть $1 \leq m \leq n$. Группа G называется **m-транзитивной**, если ее действие на множестве списков из m попарно различных точек транзитивно. Иными словами, для любых попарно различных $x_1, \dots, x_m \in X$ и любых попарно различных $y_1, \dots, y_m \in X$ существует $\pi \in G$ такое, что $\pi(x_i) = y_i$ для всех $i = 1, \dots, m$. Группа $G \leq S_n$ называется **кратно транзитивной**, если она m-транзитивна для какого-то $m \geq 2$.

Лемма. *Группа A_n является $(n-2)$-транзитивной.*

Доказательство. В самом деле, из двух перестановок

$$\begin{pmatrix} x_1 & \dots & x_{n-2} & x_{n-1} & x_n \\ y_1 & \dots & y_{n-2} & y_{n-1} & y_n \end{pmatrix}$$

$$\begin{pmatrix} x_1 & \dots & x_{n-2} & x_{n-1} & x_n \\ y_1 & \dots & y_{n-2} & y_n & y_{n-1} \end{pmatrix}$$

одна является четной.

Задача. Докажите, что порядок m-транзитивной группы перестановок $G \leq S_n$ делится на $n(n-1)\dots(n-m+1)$.

2. Группы Матье. В 1861 году Эмиль Матье открыл пять совершенно удивительных групп M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, обладающих высокой степенью транзитивности. А именно, группы M_{12} и M_{24} 5-кратно транзитивны, группы M_{11} и M_{23} 4-кратно транзитивны, а M_{22} 3-кратно транзитивна.

Эмиль Матье (Emile Leonard Mathieu, 15 мая 1835, Метц — 19 октября 1890, Нанси) — замечательный французский математик. Всего за 18 месяцев Матье заканчивает полный курс Ecole Polytechnique и в 1859 году получает докторскую степень за свою работу о свойствах симметрии функций, которая и привела к открытию групп Матье — первых пяти спорадических простых конечных групп. К сожалению, в течение 10 лет Матье не мог получить университетской позиции и работал как частный репетитор, только в 1869 году он получает кафедру в Безансоне, откуда через пять лет переезжает в Нанси, где и остается до конца жизни. В это время научные интересы Матье смещаются в сторону математической физики, в первую очередь явного решения дифференциальных уравнений, возникающих в теории потенциала, теории колебаний, теории упругости, теплопроводности, при изучении капиллярных сил, магнетизма и в задаче трех тел. Кроме групп Матье самым известным достижением, связанным с его именем, являются функции Матье, которые он открыл, исследуя задачи гидродинамики.

В действительности, M_{12} и M_{24} это *единственные* 5-кратно транзитивные группы, кроме S_n и A_n.

$$\begin{aligned}
M_{11} &\qquad 2^4\cdot 3^2\cdot 5\cdot 11 = 7920,\\
M_{12} &\qquad 2^6\cdot 3^3\cdot 5\cdot 11 = 95040,\\
M_{22} &\qquad 2^7\cdot 3^2\cdot 5\cdot 7\cdot 11 = 443520,\\
M_{23} &\qquad 2^7\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 23 = 10200960,\\
M_{24} &\qquad 2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23 = 244823040.
\end{aligned}$$

Группа M_{12} уже была описана нами в § 6 главы 2, в следуюшем параграфе мы опишем все пять групп Матье, а в § 16 приведем еще две совершенно удивительные конструкции группы M_{12}, открытые Джоном Конвеем.

3. Кратная однородность. Подгруппа $G \le S_n$ называется **m-однородной**, если она транзитивна на множестве $\bigwedge^m(\underline{n})$ всех m-элементных подмножеств в $\underline{n}$. Ясно, что m-транзитивная группа автоматически является $(m-1)$-транзитивной. Для m-однородных групп это уже отнюдь не столь очевидно, следующая теорема является одним из основных результатов статьи [226].

Теорема Ливингстона—Вагнера. *Если подгруппа $G \le S_n$ является m-однородной для некоторого $m \le n/2$, то она является и $(m-1)$-однородной.*

§ 17♣. Системы Штейнера и группы Матье

В этом параграфе мы изложим простую единообразную конструкцию групп Матье, предложенную Эрнстом Виттом [227] и в дальнейшем детально исследованную многими авторами [228], [229].

Эрнст Витт (`Ernst Witt`, 26 июня 1911, Алзен, ныне Алс, Дания — 03 июля 1991, Гамбург) — гениальный немецкий алгебраист. Его основные работы относятся к теории квадратичных форм, алгебраической геометрии, алгебраической теории чисел, теории алгебр Ли и теории групп. Витт провел детство в Китае, а его студенческие годы прошли во Фрайбурге и Геттингене, где его непосредственным руководителем была Эмми Нетер. В 1937 году, когда Эмиль Артин вынужден был покинуть Германию, Витт был назначен на его позицию в Гамбургском университете, где и оставался до ухода на пенсию в 1979 году. В нашем курсе встречаются *десятки* введенных им понятий, теорем Витта и придуманных им доказательств, в особенности относящихся к геометрической алгебре и теории алгебр Ли: индекс Витта, базис Витта, разложение Витта, кольцо Витта, векторы Витта, алгебры Витта, теоремы Витта о продолжении изометрии и сокращении, тождество Холла—Витта и т. д.

Витт был активным нацистом и после войны долгое время подвергался остракизму со стороны западных коллег и вел довольно замкнутую жизнь. Единственная известная мне мемориальная статья [230] написана Иной Керстен, которая была его ученицей в Гамбурге.

Рассмотрим пару (X, Ω), где X есть n-элементное множество, а $\Omega \subseteq \bigwedge^m(X)$ — множество, состоящее из m-элементных подмножеств множества X, называемых **блоками**. Такая пара называется **системой Штейнера** с параметрами (k, m, n), если любое k-элементное подмножество $Z \in \bigwedge^k(X)$ содержится в единственном блоке $Y \in \Omega$. Система Штейнера с параметрами (k, m, n) обозначается $S(k, m, n)$, это обозначение особенно часто используется в том случае, когда система с такими параметрами единственна с точностью до изоморфизма.

Вот три очевидных примера систем Штейнера.

• Очевидно, что $(X, \bigwedge^m(X))$ является системой Штейнера с параметрами (m, m, n), такая система называется **тривиальной**. В дальнейшем мы интересуемся только нетривиальными системами, для которых $k < m$.

• Пусть X — проективная плоскость над полем из q элементов. Возьмем в качестве Ω множество всех прямых в X. Так как через любые две точки проходит единственная прямая, то (X, Ω) представляет собой Штейнерову систему с параметрами $(2, q+1, q^2+q+1)$

• Пусть $S = (X, \Omega)$ система Штейнера с параметрами (k, m, n). Для любой точки $x \in X$ пара, состоящая из множества $X_x = X \setminus \{x\}$ и множества Ω_x его $(m-1)$-элементных подмножеств Y таких, что $Y \cup \{x\} \in \Omega$, является системой Штейнера с параметрами $(k-1, m-1, n-1)$, называемой **одноточечным ограничением** (`one-point restriction`) системы S

Якоб Штейнер (Jakob Steiner, 18 марта 1796, Утценсторф — 1 апреля 1863, Берн) — замечательный швейцарский геометр, прославившийся своими работами в области проективной геометрии, теории геометрических конфигураций и изопериметрических задач.

Биография Штейнера в высшей степени колоритна. Будучи сыном пастуха он только в 14 лет научился читать и в 18 лет пошел в школу. Под влиянием своего учителя Песталоцци он увлекся педагогикой и решил — вопреки воле семьи!! — продолжить образование. После обучения в Гейдельберге в 1818–1821 годах он переезжает в Берлин, где работает школьным учителем, а в 1835 году становится **экстраординарным** профессором Берлинского университета.

В Берлине он очень близко сошелся с Карлом Якоби. Трудно представить себе более живописную пару. Болезнено чувствительный, утонченный и язвительный интеллектуал Якоби, происходивший из богатейшей еврейской банкирской семьи, написавший свои первые математические работы примерно в том возрасте, в котором Штейнер научился читать, и крестившийся в 21 год, чтобы получить университетскую позицию. И крестьянский сын Штейнер, человек *невыносимой врожденной грубости* ?? не скрывавший своего антисемитизма. Несмотря на все это, и на разницу в возрасте они стали ближайшими друзьями — и источником десятков анекдотов.

Вот небольшая зарисовка для Владимира Соловьева. Как-то они крепко поругались и Штейнер вызвал Якоби на дуэль. Якоби ответил в своей обычной издевательской манере: “Wenn Du des Lebens überdrüssig bist, so kaufe Dir Pistolen und schiesse Dir eine Kugel in den Kopf; mich hast Du dazu nicht nötig.” — “Если Тебе наскучила жизнь, то купи пистолет и застрелись; я Тебе для этого совершенно не нужен.” Штейнер был полностью удовлетворен: “Damit ist die Sache erledigt!”

Группа автоморфизмов $\mathrm{Aut}(X,\Omega)$ штейнеровой системы (X,Ω) состоит из таких перестановок $\pi\in S_n$, что образ блока под действие π снова является блоком: $Y\in\Omega\Longrightarrow\pi(Y)\in\Omega$. Например, группа автоморфизмов конечной проективной плоскости — это обычная группа коллинеаций.

В цитированной работе Витт доказал существование единственных систем Штейнера $S(4,5,11)$, $S(5,6,12)$, $S(4,7,23)$ и $S(5,8,24)$.

Теорема Витта. *Имеют место изоморфизмы*

$$\mathrm{Aut}(S(4,5,11))\cong M_{11},\qquad \mathrm{Aut}(S(5,6,12))\cong M_{12},$$
$$\mathrm{Aut}(S(4,7,23))\cong M_{23},\qquad \mathrm{Aut}(S(5,8,24))\cong M_{24}.$$

Группа M_{22} является подгруппой индекса 2 в $\mathrm{Aut}(S(3,6,22))$.

§ 18♣. Игра в 12 и закрутки икосаэдра

В этом параграфе мы опишем еще две естественные конструкции группы Матье M_{12}. Своими словами содержание этого параграфа можно пересказать так: каждый раз, когда мы пытаемся *естественным образом* построить *какую-то* группу перестановок 12 символов, получается M_{12}.

1. Игра в 12. Игра в 12 аналогична игре в 15, но играют в нее на проективной плоскости над полем из трех элементов. Напомним, что на проективной плоскости над полем из q элементов q^2+q+1 точка, которые лежат на q^2+q+1 прямых, по $q+1$ точке на каждой. В частности, на проективной плоскости над полем из трех элементов 13 точек на 13 прямых, по 4 точки на каждой прямой. Поставим в 12 точек по фишке, занумерованной от 1 до 12, при этом одна точка остается свободной. То, что это точка свободна, будет обозначаться размещением там дырки $*$. Легальный ход игры в 12 можно описать следующим образом. Через любую точку, содержащую фишку, и ту точку, в которой находится $*$, проходит *единственная* прямая. На этой прямой расположены еще две точки. Легальный ход состоит в том, что мы перемещаем фишку в свободную точку и при этом переставляем две другие фишки, расположенные на той же прямой. Все возможные расстановки фишек, к которым можно прийти из данной при помощи последовательности легальных ходов, образуют группоид M_{13}, при этом расстановки с фиксированной позицией свободной точки соответствуют элементам группы M_{12}.

2. Закрутки икосаэдра. Рассмотрим **икосаэдр Рубика**, в котором можно осуществить поворот половины икосаэдра вокруг оси, соединяющей две противоположные вершины, на угол $2\pi/5$. Пусть x и y суть две противоположные вершины. Поворот половины икосаэдра содержащей x вокруг оси xy, осуществленный в отрицательном направлении (по часовой стрелке), называется **закруткой** вокруг вершины x и обозначается τ_x, а вращение τ_x^{-1} в положительном направлении (против часовой стрелки) — **раскруткой** вокруг вершины x. Группа, порожденная произведениями $\tau_x\tau_y^{-1}$, где x и y суть две *произвольные* вершины икосаэдра, изоморфна группе Матье M_{12}, доказательство этого факта намечено в статье Дж. Конвея *Коды Голея и группы Матье*, на русском языке эта статья опубликована как глава 11 в книге [231].

Замечание. Произведение закрутки вокруг вершины x и раскрутки вокруг *противоположной* вершины y есть вращение икосаэдра на угол $2\pi/5$ как целого. Таким образом, M_{12} содержит собственную группу икосаэдра I^+.

В главе 1 нам встречался 24-вершинник в четырехмерном пространстве. Напрашивается мысль, что если изготовить из него **24-вершинник Рубика**, то подходящая группа его вращений будет изоморфна M_{24}. Однако, как сообщил автору Джон Конвей, построение такой реализации группы M_{24} представляет собой открытый вопрос!

§ 19♠. Примитивность

1. Примитивные группы. Группа $G \leq S_n$ называется **импримитивной**, если множество $X = \underline{n}$ можно представить в виде $X = X_1 \sqcup \ldots \sqcup X_t$, где $1 < t < n$, притом так, что каждый элемент $g \in G$ переставляет классы $X_1, \ldots, X_t$ между собой. Иными словами, для каждого $g \in G$ и каждого X_i, $1 \leq i \leq t$, существует такое j, $1 \leq j \leq t$, что $gX_i \leq X_j$. Условие $1 < t < n$ утверждает, что каждый класс X_i содержит по крайней мере 2 элемента, и, кроме того, имеется не менее, чем 2 класса. Набор классов $\{X_1, \ldots, X_t\}$ называется **системой импримитивности** группы G, а сами классы $X_1, \ldots, X_t$ — **блоками импримитивности**. В противном случае, когда такое разбиение невозможно, группа G называется **примитивной**. Таким образом, примитивная группа перестановок множества $X = \underline{n}$ стабилизирует лишь два отношения эквивалентности на множестве X, а именно равенство и тотальную эквивалентность.

Ясно, что примитивная группа транзитивна, а дважды транзитивная группа примитивна. Таким образом, условие примитивности является *промежуточным* между транзитивностью и кратной транзитивностью:

$$2\text{-транзитивность} \Longrightarrow \text{примитивность} \Longrightarrow \text{транзитивность}.$$

Группа G называется **унипримитивной**, если она примитивна, но не 2-транзитивна. Число 2-орбит группы G называется **(перестановочным) рангом** группы G. Группа G в том и только том случае 2-транзитивна, когда ее ранг ≤ 2. Тем самым, ранг унипримитивной группы ≥ 3. Это значит, что наиболее близкими к кратно транзитивным группам являются унипримитивные группы ранга 3. Такие группы были детально изучены Хигманом.

Следующая задача устанавливает теснейшую связь между примитивностью и описанием максимальных подгрупп.

Задача. Покажите, что транзитивная группа $G \leq S_n$ в том и только том случае примитивна, когда стабилизатор G_n точки n максимален в G.

Решение. Предположим, что G_n не максимальна в G и H, $G_n < H <$

G, — собственная промежуточная подгруппа. Тогда $H_n = G_n$, причем так как $H \neq G$, то индекс $|H : G_n|$ не делится на n. Поэтому группа H не может быть транзитивной. В то же время, так как $H \neq G_n$, то ее орбиты содержат больше одного элемента. Тем самым, орбиты группы H можно взять в качестве блоков импримитивности группы G.

Задача. Докажите, что если G — примитивная группа перестановок, $H \trianglelefteq G$, $H \neq 1$, то H транзитивна.

§ 20♠. Теорема Галуа о простоте A_n, $n \geq 5$

In five minutes you will say that it is all so absurdly simple.

Sir Arthur Conan Doyle. *The adventure of dancing men*

В настоящем параграфе мы докажем следующую теорему, установленную Галуа. Заметим, что именно оценка $n \geq 5$ в этой теореме объясняет, почему алгебраические уравнения степени $n \leq 4$ разрешимы в радикалах, а уравнения степени $n \geq 5$ — нет.

Теорема Галуа. *Знакопеременная группа A_n, $n \geq 5$, проста.*

Мы разобьем доказательство на последовательность лемм.

Лемма 1. *Если нормальная подгруппа H в A_n, $n \geq 4$, содержит 3-цикл, то она совпадает с A_n.*

Доказательство. Для $n \geq 5$ это сразу вытекает из результатов предыдущего параграфа. В самом деле, так как $n - 2 \geq 3$, то группа A_n 3-транзитивна. Тем самым, H содержит все 3-циклы и, следовательно, совпадает с A_n.

Однако в действительности лемма верна и для $n = 4$, как показывает следующее очевидное вычисление. Пусть $(ijh) \in H$ – некоторый 3-цикл и k — индекс, отличный от i, j, h. Тогда $(ijk)^{-1}(ijh)(ijk) = (ihk) \in H$. Переписывая (ijh) в виде $(ijh) = (jhi) = (hij)$ и сопрягая при помощи (jhk) и (hik), соответственно, точно так же убеждаемся, что $(jik), (hjk) \in H$, но это и значит, что H снова содержит все 3-циклы.

Следующая лемма представляет собой основной шаг доказательства.

Лемма 2. *Любая нормальная подгруппа $H \neq e$ в A_n, $n \geq 4$, содержит нетривиальное произведение двух 3-циклов.*

Доказательство. В самом деле, пусть $\tau \in H$, $\tau \neq e$. Так как A_n, $n \geq 4$, порождается 3-циклами, а ее центр равен e, то найдется такой 3-цикл σ, что $[\sigma, \tau] \neq e$. Но ведь $[\sigma, \tau] = \sigma(\tau\sigma^{-1}\tau^{-1}) \in H$ есть произведение двух 3-циклов.

Таким образом, в каждой нормальной подгруппе $H \neq e$ группы A_n, $n \geq 4$, есть *нетривиальное* произведение двух 3-циклов. Если нам удастся показать, что в действительности H содержит 3-цикл, то мы сможем воспользоваться леммой 1 и заключить, что $H = A_n$. Наличие 3-цикла в H вытекает из следующих лемм. Посмотрим, прежде всего, на цикленный тип произведения двух 3-циклов.

Лемма 3. *Произведение π двух 3-циклов является, в зависимости от того того, перемещает оно $3, 4, 5$ или 6 элементов, либо 3-циклом, либо произведением двух независимых транспозиций, либо 5-циклом, либо произведением двух независимых 3-циклов.*

Доказательство. Очевидно. В самом деле, произведение двух 3-циклов сидит в A_6, а в формулировке леммы перечислены все четные классы сопряженности в S_6, за исключением перестановок цикленного типа $(4, 2)$. Однако, если произведение двух 3-циклов перемещает 6 символов, то эти циклы должны быть независимы, так что этот случай не реализуется.

В случае, когда в H есть 3-цикл, мы достигли полного счастья, а случай, когда в H есть произведение двух независимых 3-циклов, сразу сводится к наличию в H 5-цикла.

Лемма 4. *Если в H есть произведение двух независимых 3-циклов, то в H есть 5-цикл.*

Доказательство. В самом деле, пусть $\pi = (ijh)(klm) \in H$ для 6 попарно различных индексов i, j, h, k, l, m. Тогда $[\pi, (ijk)] = (ikhlj) \in H$.

В двух других возникающих в лемме 3 случаях коммутатор элемента указанного типа с подходящим 3-циклом есть 3-цикл.

Лемма 5. *Если $n \geq 5$ и в H есть произведение двух независимых транспозиций, то в H есть 3-цикл.*

Доказательство. Пусть $\pi = (ij)(hk) \in H$ и l — индекс отличный от i, j, h, k. Тогда $[\pi, (hkl)] = (hkl) \in H$.

Лемма 6. *Если в H есть 5-цикл, то в H есть 3-цикл.*

Доказательство. В самом деле, пусть $\pi = (ijhkl) \in H$ — некоторый 5-цикл. Тогда $[\pi, (ijh)] = (ikj) \in H$.

Теорема полностью доказана. Интересно, что *единственное* место, в этом доказательстве, которое не работает при $n = 4$ — это лемма 5, где мы должны выбирать индекс l отличный от четырех фиксированных индексов i, j, h, k. Именно здесь и возникает исключение: знакопеременная группа A_4 не является простой. Дело в том, что в группе A_4 произведения двух независимых трансвекций образуют вместе с единичной перестановкой четверную группу

$$V = \{e, (12)(34), (13)(24), (14)(23)\},$$

которая нормальна не только в A_4, но даже в S_4.

Следствие. *При $n \geq 5$ подгруппа A_n является единственной нетривиальной собственной нормальной подгруппой в S_n.*

Доказательство. Так как $|S_n : A_n| = 2$, то $A_n \trianglelefteq S_n$. Обратно, пусть $H \trianglelefteq S_n$, $H \not\leq A_n$. Возьмем $\pi \in H \setminus A_n$. Так как центр S_n тривиален, то найдется такое $\sigma \in S_n$, что $[\pi, \sigma] \neq 1$. Так как $[\pi, \sigma] \in H \cap A_n \trianglelefteq A_n$, то по предыдущей теореме $H \cap A_n = A_n$, и, тем самым, $A_n < H \leq S_n$. Но это значит, что $H = S_n$.

Задача. Покажите, что в группе S_4 имеются две нетривиальных собственных нормальных подгруппы, а именно, A_4 и V.

Задача. Покажите, что при $n \leq 4$ (но не при $n \geq 5$) группа S_{n-1} является фактор-группой группы S_n.

§ 21♠. Автоморфизмы S_n

В этом параграфе мы полностью вычислим группу $\mathrm{Aut}(S_n)$.

1. Теорема Гельдера. Следующий результат был доказан О.Гельдером в 1895 году [232].

Теорема Гельдера. *При $n \neq 6$ каждый автоморфизм группы S_n является внутренним, т. е.* $\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n)$.

Следствие. *Для всех $n \neq 2, 6$ имеем* $\mathrm{Aut}(S_n) \cong S_n$.

Доказательство. Для всех $n \geq 3$ центр группы S_n тривиален.

Наметим доказательство теоремы Гельдера, так как при этом вводится ключевая идея, которая может быть использована (и десятки раз использовалась!) для

определения автоморфизмов других конкретных групп. Ясно, что любой автоморфизм φ группы G отображает класс сопряженных элементов снова в класс сопряженных элементов. В частности, любой класс инволюций переходит снова в класс инволюций. Любая инволюция в S_n является произведением d независимых транспозиций для некоторого $1 \leq d \leq l = \lfloor n/2 \rfloor$. Таким образом, инволюции в S_n разбиваются на l сопряженных классов $C_1, \ldots, C_l$, где в класс C_d входят произведения d независимых транспозиций. Легко видеть, что имеется $\binom{n}{2}$ различных транспозиций, $\frac{1}{2}\binom{n}{2}\binom{n-2}{2}$ различных произведений двух независимых транспозиций — мы произвольным образом выбираем первую транспозицию n символов, а потом вторую транспозицию оставшихся $n-2$ символов, но при этом каждое произведение оказалось посчитанным *дважды*, так как мы могли стартовать со второй транспозиции. По тем же причинам имеется $\frac{1}{6}\binom{n}{2}\binom{n-2}{2}\binom{n-4}{2}$ произведений трех независимых транспозиций и вообще

$$|C_d| = \frac{1}{d!}\binom{n-2}{2}\binom{n-2}{2}\ldots\binom{n-2d+2}{2} = 1 \cdot 3 \cdot \ldots \cdot (2d-1)\binom{n}{2d}$$

различных произведений d независимых транспозиций.

Задача. Покажите, что при $n \neq 6$ имеем $|C_d| \neq |C_1|$ для любого $d \geq 2$.

Для $n = 6$ это утверждение не имеет места! В самом деле, непосредственное вычисление показывает, что в этом случае $|C_1| = |C_3| = 15$, в то время как $|C_2| = 45$, что в сумме дает нам все 75 инволюций группы S_6 (в следующем параграфе мы скажем, что в этой группе 76 инволюций, это расхождение связано с тем, что `Mathematica` подобно большинству математиков-неспециалистов считает тождественную перестановку инволюцией). И действительно, в следующем пункте мы построим внешний автоморфизм группы S_6, переводящий C_1 в C_3.

Доказательство теоремы Гельдера. Пусть $\varphi \in \mathrm{Aut}(S_n)$. Так как S_n порождается фундаментальными транспозициями $s_1, \ldots, s_{n-1}$, то нам достаточно доказать существование такой перестановки $\pi \in S_n$, что

$$\varphi(s_1) = \pi s_1 \pi^{-1}, \ldots, \varphi(s_{n-1}) = \pi s_{n-1} \pi^{-1}.$$

В действительности, технически несколько удобнее доказывать существование такого $\pi \in S_n$, что $I_\pi\varphi(s_h) = s_h$ для всех $h = 1, \ldots, n-1$. Из предшествующей задачи мы знаем, что при $n \neq 6$ имеем $|C_d| \neq |C_1|$ при всех $d \geq 2$. Поэтому все $\varphi(s_h)$ обязаны быть транспозициями. Будем вести доказательство индукцией по количеству r фундаментальных транспозиций, образы которых удается вернуть на место сопряжением.

База индукции. Пусть, скажем, $\varphi(s_1) = (ij)$. Тогда полагая $\pi = (1i)(2j)$ мы можем считать, что $I_\pi\varphi(s_1) = s_1$.

Шаг индукции. Вообще предположим, что нам уже удалось построить такое $\pi \in S_n$, что $I_\pi\varphi(s_1) = s_1, \ldots, I_\pi\varphi(s_r) = s_r$ для некоторого $1 \leq r \leq n-2$, и будем вести доказательство индукцией по r. Посмотрим на образ s_{r+1} под действием $I_\pi\varphi$. Пусть, скажем, $I_\pi\varphi(s_{r+1}) = (ij)$.

Пусть вначале $r = 1$, так как порядок $(12)(ij)$ равен порядку $(12)(23)$ равен 3, то $\{1, 2\}$ и $\{i, j\}$ пересекаются ровно по одному элементу, а так как $(ij) = (ji)$, то

можно даже считать, что $i = 1$ или $i = 2$. Заменяя π на $(3j)\pi$, если $i = 2$, и на $(12)(3j)\pi$, если $i = 1$, можно считать, что $I_\pi\varphi(s_1) = s_1, I_\pi\varphi(s_2) = s_2$.

В случае $r \geq 2$ доказательство аналогично и даже чуть проще. Так как $I_\pi\varphi(s_{r+1}) = (ij)$ коммутирует со всеми $(12), \dots, (r-1, r)$, а порядок произведения $(r, r+1)(ij)$ равен 3, то $\{i, j\}$ не пересекается с $\{1, 2, \dots, r\}$, но $r+1 \in \{i, j\}$. Переименовывая i и j можно даже считать, что $i = r+1$ и тогда заменяя π на $(r+2, j)\pi$ мы получаем $I_\pi\varphi(s_1) = s_1, \dots, I_\pi\varphi(s_{r+1}) = s_{r+1}$.

2. Исключительный автоморфизм S_6. Начиная с 1895 года было дано несколько различных конструкций [233]–[237] внешнего автоморфизма порядка 2 группы S_6. Бендер задает S_6 образующими и соотношениями и предъявляет две несопряженных системы образующих, удовлетворяющих этим соотношениям. Очень эффектное доказательство Витта основано на следующем соображении. Он реализует S_6 как подгруппу в группе Матье M_{12} и явно указывает элемент $g \in M_{12}$, нормализующий S_6 и такой, что сопряжение при помощи него задает внешний автоморфизм S_6. Миллер следующим образом определяет образы внешнего автоморфизма группы S_6 на образующих:

$$(12) \mapsto (12)(35)(46),$$
$$(13) \mapsto (13)(24)(56),$$
$$(14) \mapsto (14)(25)(36),$$
$$(15) \mapsto (15)(26)(34),$$
$$(16) \mapsto (16)(23)(45)$$

и показывает, что действительно существует автоморфизм S_6 (по сравнению с работой [233] мы для большей симметрии переставили 5 и 6).

Упражнение. Вычислите, во что переходят при этом автоморфизме фундаментальные транспозиции.

Как известно, S_5 допускает два неэквивалентных представления на 6 буквах, интранзитивное и транзитивное. Януш и Ротман замечают, что так как $|S_6 : S_5| = 6$, то действие S_6 на смежных классах по транзитивной подгруппе S_5 определяет гомоморфизм $S_6 \longrightarrow S_6$, который как раз и является внешним автоморфизмом S_6. Кроме того, они упоминают, что Дж. Уолтер заметил, что уже группа коллинеаций $\mathrm{P\Gamma L}(2, 9)$ содержит S_6 и нормализующий S_6 элемент g, сопряжение при помощи которого реализует внешний автоморфизм S_6. Наконец, Фурнель приводит еще одно построение внешнего автоморфизма S_6 основанное на исключительном изоморфизме $O = S_3 \wr C_2 \cong S_4 \times C_2$. Таким образом, группа O допускает два представления в S_6 — транзитивное (это действие O на 6 гранях куба) и интранзитивное (это прямая сумма действия O на 4 диагоналях куба и действия на 2 точках, при котором собственные вращения и только они переходят в тождественную перестановку). Внешний автоморфизм S_6 как раз и является продолжением изоморфизма между $S_3 \wr C_2$ и $S_4 \times C_2$ на всю группу S_6. В работе [238] изучается строение группы $\mathrm{Aut}(S_6)$. В частности, там показано, что порядок любого элемента $\mathrm{Aut}(S_6) \setminus \mathrm{Inn}(S_6)$ равен 2,4,8 или 10.

3 ♣. Изоморфизм $S_6 \cong \mathrm{Sp}(4, 2)$. Для более продвинутого читателя приведем еще одно доказательство существования у S_6 внешнего автоморфизма. Для этого заметим, что существование исключительного автоморфизма у S_6 совершенно

очевидно, *если* знать исключительный изоморфизм $S_6 \cong \mathrm{Sp}(4,2)$ группы S_6 с симплектической группой степени 4 над полем из 2-х элементов, к которому мы вернемся в третьем семестре. Дело в том, что симплектические группы над полем K характеристики 2 допускают исключительный автоморфизм, меняющий длину корня. Этот автоморфизм переводит симплектическую матрицу

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} \in \mathrm{Sp}(4,K)$$

в симплектическую матрицу

$$\begin{pmatrix} a_{12}a_{21}+a_{11}a_{22} & a_{14}a_{21}+a_{11}a_{24} & a_{13}a_{22}+a_{12}a_{23} & a_{14}a_{23}+a_{13}a_{24} \\ a_{12}a_{41}+a_{11}a_{42} & a_{14}a_{41}+a_{11}a_{44} & a_{13}a_{42}+a_{12}a_{43} & a_{14}a_{43}+a_{13}a_{44} \\ a_{22}a_{31}+a_{21}a_{32} & a_{24}a_{31}+a_{21}a_{34} & a_{23}a_{32}+a_{22}a_{33} & a_{24}a_{33}+a_{23}a_{34} \\ a_{32}a_{41}+a_{31}a_{42} & a_{34}a_{41}+a_{31}a_{44} & a_{33}a_{42}+a_{32}a_{43} & a_{34}a_{43}+a_{33}a_{44} \end{pmatrix}.$$

Если взять здесь $K = \mathbb{F}_2$ и вернуться к S_6, мы как раз и получим внешний автоморфизм S_6, о котором шла речь выше.

Комментарий. На языке корней этот автоморфизм $\mathrm{Sp}(4,K)$ построен Римхаком Ри для объяснения конструкции групп Судзуки. Матричная формула записана Уореном Уонгом и опубликована в статье [239]. Наша формула слегка отличается от формулы, приведенной в книгах **[147]** и **[88]**, так как мы рассматриваем симплектическую группу по отношению к базису Витта, в котором $(e_1,e_4) = (e_2,e_3) = 1$, в то время как в цитированных книгах $(e_1,e_3) = (e_2,e_4) = 1$.

§ 22♠. Mathematica ПЕРЕСТАНОВОК

В системе `Mathematica` имплементировано несколько стандартных функций, связанных с перестановками. Кроме того, много дополнительных функций подгружаются командами

```
<<DiscreteMath‘Permutations‘
<<DiscreteMath‘Combinatorica‘
```

Перечислим некоторые наиболее полезные функции. `Permutations[`l`]` генерирует все перестановки списка l. Например,

```
Permutations[Range[n]]
```

генерирует все элементы симметрической группы S_n степени n в лексикографическом порядке, в сокращенной записи.

`Reverse` — перестановка $\begin{matrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{matrix}$.

`RotateLeft`, `RotateRight` — длинные циклы. Точнее, `RotateRight[`l`]` циклически сдвигает элементы списка l на одну позицию вправо, а `RotateLeft[`l`]` — на одну позицию влево. Аналогично, `RotateRight[`l,n`]` циклически сдвигает элементы списка l на n позиций вправо, а `RotateLeft[`l,n`]` — на n позиций влево.

`Permute[`x`,`y`]` переставляет список x в соответствии с перестановкой y. При этом получается сокращенная запись произведения xy, так что фактически это

и есть способ вычисления произведения перестановок. Совершенно удивительно, что эта функция не имплементирована в ядре. Однако поскольку в ядре есть умножение матриц, то нетрудно определить и умножение перестановок, для этого достаточно построить гомоморфизм $S_n \longrightarrow \mathrm{GL}(n, K)$

```
pi[x_]:=Table[If[i==x[[j]],1,0],{i,Length[x]},{j,Length[x]}]
```

Этот гомоморфизм устанавливает биекцию между S_n и множеством всех матриц перестановки, причем обратное отображение определяется посредством

```
ip[x_]:=Flatten[Table[Position[Transpose[x][[i]],1],{i,Length[x]}]]
```

Теперь мы можем вычислить произведение xy перестановок x и y при помощи переноса структуры `ip[pi[`x`].pi[`y`]]`.

`InversePermutation[`x`]` — перестановка обратная к x.

тест `PermutationGroupQ[`g`]` возвращает `True`, если список перестановок g образует группу.

`RandomPermutation[n]` порождает (псевдо)случайную перестановку длины n.

тест `PermutationQ[x]` возвращает `True`, если x является перестановкой, и `False` в противном случае.

`MinimumChangePermutations[`x`]` порождает все перестановки списка x таким образом, что любые два соседних элемента отличаются на одну транспозицию.

`RankPermutation[`x`]` показывает позицию перестановки $x \in S_n$ в лексикографическом списке всех перестановок n символов (заметим, что нумерация начинается с 1, так что, например, `RankPermutation[{4,3,2,1}]=23`.

`NextPermutation[`x`]` порождает перестановку, следующую за x в лексикографическом порядке.

тест `DerangementQ[`x`]` возвращает `True`, если перестановка является беспорядком. Напомним, что перестановка $\pi \in S_n$ называется **беспорядком**, если у нее нет неподвижных точек, т. е. если $\pi(i) \neq i$ для всех $i \in \underline{n}$.

`NumberOfDerangements[`n`]` вычисляет количество D_n беспорядков на n символах. Приведем для примера несколько первых значений D_n: $D_2 = 1$, $D_3 = 2$, $D_4 = 9$, $D_5 = 44$, $D_6 = 265$, $D_7 = 1854$, $D_8 = 14833$, $D_9 = 133496$, $D_{10} = 1334961$.

`NumberOfInvolutions[`n`]` вычисляет количество I_n инволюций на n символах (включая тождественную перестановку!). Приведем для примера несколько первых значений I_n: $I_1 = 1$, $I_2 = 2$, $I_3 = 4$, $I_4 = 10$, $I_5 = 26$, $I_6 = 76$, $I_7 = 232$, $I_8 = 764$, $I_9 = 2620$, $I_{10} = 9496$.

`NumberOfPermutationsByCycles[`n`,`s`]` вычисляет количество перестановок на n символах, у которых в точности s циклов.

В пакете `DiscreteMath‘Permutations‘` есть команды, которые позволяют переходить от полной записи к цикленной и от цикленной к полной:

`ToCycles[`x`]` дает разложение перестановки x в произведение независимых циклов;

`FromCycles[{`$x_1, \ldots, x_n$`}]` генерирует перестановку с данным разложением на циклы.

`Inversions[`x`]` возвращает число инверсий перестановки x.

`Signature[`x`]` возвращает знак перестановки x.

Глава 6. ДЕЙСТВИЯ ГРУПП

В настоящей главе мы детально проанализируем понятие действия, изучим основные конструкции над действиями групп, основные связанные с действиями понятия — орбиты, стабилизаторы, транзитивность, ... — и познакомимся с несколькими замечательными действиями. Собственно говоря, в приложениях группа G *всегда* появляется не сама по себе, а в каком-то **представлении**, т. е. вместе с действием на каком-то множестве X. Если при этом рассматриваются *произвольные* биекции множества X на себя, такие представления называются **пермутационными**. Однако очень часто это множество само снабжено какой-то алгебраической, геометрической и/или топологической структурой. Например, если $X = V$ является векторным пространством, говорят о **линейных представлениях**, если X является группой или кольцом — о **представлениях автоморфизмами** и т. д.

§ 1♢. Действие группы на множестве

В этом параграфе мы приведем основные определения, связанные с действиями групп. Специфика групповых действий состоит в том, что элементы группы осуществляют *обратимые* преобразования множества X.

1. Действие группы. Начнем с основного определения.

Определение. *Пусть G — группа, а X — множество. Говорят, что G* **действует на X слева**, *и пишут $G \curvearrowright X$, если задано отображение*

$$\mathrm{act} : G \times X \longrightarrow X, \qquad (g, x) \mapsto gx,$$

такое, что выполняются свойства

1) **внешняя ассоциативность**: $(gh)x = g(hx)$ *для всех* $g, h \in G$, $x \in X$;

2) **унитальность**: $ex = x$.

При этом X называется **G-множеством** *или, точнее,* **левым G-множеством**.

Про элемент gx говорят, что он получается из x **применением** элемента g или что он является **образом** x под действием g. Иногда для действия группы G на X используются и другие системы записи, например, образ x под действием g обозначается через $g+x$, $g\circ x$, $g\cdot x$, $g\bullet x$, $g(x)$, ${}^g x$ или как нибудь еще, но чаще всего мы будем использовать обычную мультипликативную запись.

Заметим, что для каждого элемента группы отображение $\theta_g : X \longrightarrow X$, $x \mapsto gx$, осуществляет *биекцию* множества X на себя. Из аксиом 1) и 2) сразу вытекает, что

3) $(\theta_g)^{-1} = \theta_{g^{-1}}$ для любого $g \in G$.

В самом деле, $\theta_g\theta_{g^{-1}} = \theta_{gg^{-1}} = \theta_1 = \mathrm{id}_X$.

Аналогично определяется **правое** действие $X \times G \longrightarrow X$ группы G на множестве X, которое обозначается $X \curvearrowleft G$. При этом внешняя ассоциативность приобретает вид $x(gh) = (xg)h$. Таким образом, различие состоит в том, что при левом действии первым действует *второй* множитель, а при правом действии первым действует *первый* множитель. Результат применения g к x при правом действии часто записывается еще как x^g, при этом внешняя ассоциативность выражается обычной формулой $x^{gh} = \left(x^g\right)^h$.

Для любой группы G и любого множества X отображение $G\times X \longrightarrow X$, $(g, x) \mapsto x$ определяет действие G на X, которое называется **тривиальным**.

2. Связь правых и левых действий. Обратимость всех элементов позволяет установить более простую связь правых и левых действий в случае групп, чем это имело место в случае моноидов. Дело в том, что отображение $\mathrm{inv} : G \longrightarrow G$, $g \mapsto g^{-1}$, является **антиавтоморфизмом** группы G на себя, т. е. для любых элементов $f, g \in G$ выполняется равенство $(fg)^{-1} = g^{-1}f^{-1}$. Тем самым любое *правое* G-множество X естественно превращается в *левое* G-множество посредством формулы $gx = xg^{-1}$. Аналогично, каждое левое G-множество превращается в правое G-множество посредством формулы $xg = g^{-1}x$. Таким образом, в дальнейшем мы можем не теряя общности говорить лишь о левых G-множествах имея в виду, что при помощи этой конструкции все определения и результаты автоматически переносятся и на правые действия.

3. Действия групп с дополнительной структурой. В случае, когда G и X несут одну и ту же дополнительную структуру, обычно требуют, чтобы действие было морфизмом этой структуры. Вот несколько типичных примеров.

• **Непрерывное действие**: G — топологическая группа, X — топологическое пространство, act — непрерывное отображение.

• **Гладкое действие**: G — группа Ли, X — бесконечно дифференцируемое многообразие, act — бесконечно дифференцируемое отображение.

• **Аналитическое действие**: G — аналитическая группа, X — аналитическое многообразие, act — аналитическое отображение.

• **Регулярное действие**: G — алгебраическая группа, X — алгебраическое многообразие, act — регулярное отображение.

• **Рациональное действие**: G — алгебраическая группа, X — алгебраическое многообразие, act — рациональное отображение.

§ 2♢. Эквивариантные отображения, ♠ категория G-множеств

Каждый раз, как только вводится новый класс математических объектов, нужно сразу же определить допустимый класс отображений между этими объектами.

1. Морфизмы G-множеств. Морфизмом одного G-множества в другое называется отображение, согласованное с действием элементов группы G.

Определение. *Пусть X и Y суть два G-множества. Тогда отображение $\psi : X \longrightarrow Y$ называется* **морфизмом** *G-множеств или* **G-эквивариантным** *отображением, если для любого $g \in G$ и любого $x \in X$ имеет место равенство $\psi(gx) = g\psi(x)$.*

В обозначениях предыдущего пункта эквивариантность означает, что для каждого $g \in G$ следующий квадрат отображений

$$\begin{array}{ccc} X & \xrightarrow{\theta_g^X} & X \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ Y & \xrightarrow[\theta_g^Y]{} & Y \end{array}$$

коммутативен, т. е. $\psi\theta_g^X = \theta_g^Y\psi$.

Множество всех G-эквивариантных отображений из X в Y будет обозначаться через $\mathrm{Map}_G(X, Y)$. Биективное эквивариантное отображение называется **изоморфизмом** G-множеств или **G-изоморфизмом**. Два G-множества X и Y называются **G-изоморфными**, если существует изоморфизм $\psi : X \longrightarrow Y$. Одной из наших первых основных целей является классификация G-множеств с точностью до G-изоморфизма.

§ 3♢. Естественное действие S_n

1. Естественное действие моноида эндоморфизмов. В книге I мы уже встречали универсальный пример действия моноидов. А именно, пусть $M = \mathrm{End}(X) = \mathrm{Map}(X, X)$ — моноид **эндоморфизмов** множества X, т. е. всех отображений X в себя.

Предостережение. В тех случаях, когда обозначение $\mathrm{End}(X)$ сопряжено с двусмысленностью (например, если множество X несет дополнительную структуру и эндоморфизмами называются лишь отображения X в себя, сохраняющие эту структуру), вместо $\mathrm{End}(X)$ используется обозначение $\mathrm{Map}(X, X)$ или X^X.

По самому определению M действует на X слева посредством $fx = f(x)$. В самом деле, операция в M *определяется* так, чтобы выполнялась внешняя ассоциативность. Действительно, умножение в M — это *композиция* отображений, для которой $(fg)(x) = f(g(x))$, но это и есть просто другая запись внешней ассоциативности. В свою очередь, унитальность это просто определение *тождественного отображения* $e = \mathrm{id}_X$. Это действие $\mathrm{End}(X)$ на X называется **естественным** действием $\mathrm{End}(X)$ на X. Сейчас мы увидим, что произвольное действие на множестве X выражается в терминах естественного действия $\mathrm{End}(X)$.

2. Естественное действие симметрической группы. Ограничивая описанное в предыдущем пункте действие $\mathrm{End}(X)$ на группу $S_X = \mathrm{Bij}(X, X)$, мы получим универсальный пример, групповых действий. А именно, группа S_X действует на множестве X обычным образом, как $\pi x = \pi(x)$ для любого $\pi \in S_X$ и любого $x \in X$. По самому определению

3. Перестановочные представления. Пусть X есть левое G-множество. В соответствии с общей теорией отображение $g \mapsto \theta_g$ представляет собой гомоморфизм *моноидов* $G \longrightarrow \mathrm{End}(X)$. Однако, как замечено в пункте 1, в действительности все эндоморфизмы θ_g, $g \in G$, биективны.

Теорема. *Таким образом, сопоставление $g \mapsto \theta_g$ можно рассматривать как гомоморфизм $G \longrightarrow S_G$ в симметрическую группу.*

В действительности этим устанавливается взаимно однозначное соответствие между всеми *левыми* действиями G на X и всеми *гомоморфизмами* G в S_X.

• Аналогично, правые действия G на X взаимно однозначно соответствуют *антигомоморфизмам* G в S_X.

Гомоморфизм G в симметрическую группу S_X часто называется также **перестановочным представлением** группы G на множестве X.

Действие G на X называется **точным**, если соответствующий гомоморфизм $G \longrightarrow S_X$, $g \mapsto \theta_g$, инъективен. Иными словами, для точного действия e является единственным элементом $g \in G$ таким, что $gx = x$ для всех x. В общем случае ядро гомоморфизма $G \longrightarrow S_X$ называется ядром действия G на X.

Действие G на X нахывается **тривиальным**, если $gx = x$ для всех $g \in G$ и $x \in X$.

§ 4♠. Категория групп перестановок

1. Группы перестановок. Пусть X есть G-множество. Ядро отображения $\theta : G \longrightarrow S_X$ называется также **ядром** действия G на X. Действие называется **точным**, если его ядро совпадает с 1. Иными словами, точность действия означает, что для для любого $g \in G$, $g \neq 1$, найдется $x \in X$ такое, что $gx \neq x$. Если группа G действует на X точно, то она называется еще **группой перестановок** множества X. Отображение θ позволяет отождествить группу перестановок множества X с подгруппой симметрической группы S_X.

$$\begin{array}{ccc} H \times X & \xrightarrow{\mathrm{act}_X} & X \\ {\scriptstyle \varphi\times\psi}\downarrow & & \downarrow{\scriptstyle \psi} \\ G \times Y & \xrightarrow[\mathrm{act}_Y]{} & Y \end{array}$$

Произведение групп перестановок (H, X), (G, Y),
$(H \times G) \times (X \times Y) \longrightarrow X \times Y$, $(h, g)(x, y) = (hx, gy)$.

§ 5♢. Естественное линейное действие $\mathrm{GL}(n,R)$

1. Полная линейная группа. Пусть R — ассоциативное, но, вообще говоря, не обязательно коммутативное кольцо с 1. Мультипликативная группа полного матричного кольца $M(n,R)^*$ обозначается через $G = \mathrm{GL}(n,R)$ и называется **полной линейной группой** степени n над R. Обозначение GL как раз и является сокращением от английского `General Lienar Group`. Таким образом, по определению группа $\mathrm{GL}(n,R)$ состоит из всех *двусторонне* обратимых квадратных

матриц степени n с коэффициентами из R. Как и в главах, посвященных линейной алгебре, мы обозначаем матрицу, обратную к матрице $g = (g_{ij}) \in G$, через $g^{-1} = (g'_{ij})$.

В наиболее важном частном случае, когда кольцо R коммутативно, определен мультипликативный гомоморфизм $\det : M(n, R) \longrightarrow R$. При этом матрица $g \in M(n, R)$ в том и только том случае обратима, когда ее определитель $\det(x)$ обратим в кольце R. В этом случае полную линейную группу можно определить следующим образом:

$$\mathrm{GL}(n, R) = \{x \in M(n, R) \mid \det(x) \in R^*\}.$$

В частности, отсюда вытекает, что над коммутативным кольцом односторонняя обратимость матриц совпадает с двусторонней обратимостью.

2. Полная линейная группа модуля. Вообще, пусть V — любой R-модуль. Группа $\mathrm{GL}(V) = \mathrm{End}(V)^*$ (двусторонне) обратимых линейных операторов на V называется полной линейной группой модуля V. С этой точки зрения группу $\mathrm{GL}(n, R)$ становится изоморфной группе автоморфизмов свободного модуля ранга n, после того, как мы выберем в этом модуле базис.

А именно, $\mathrm{GL}(n, R)$ можно отождествить с группой $\mathrm{GL}(R^n)$ автоморфизмов свободного *правого* R-модуля R^n. А именно, $g \in \mathrm{GL}(n, R)$ действует на R^n умножением *слева*: $u \mapsto gu$. Это действие является **линейным** в том смысле, что

$$g(u + v) = gu + gv, \qquad g(\lambda u) = \lambda g(u).$$

При этом обратимость g гарантирует, что умножение на g является автоморфизмом, а не просто эндоморфизмом модуля R^n.

Точно так же группа $\mathrm{GL}(n, R)$ действует *справа* на свободном *левом* R-модуле ${}^nR$ как группа автоморфизмов $\mathrm{GL}({}^nR)$ посредством $v \mapsto vg$ для $g \in \mathrm{GL}(n, R)$ и $v \in {}^nR$.

§ 6♢. Действие группы на себе трансляциями

§ 7♢. Теорема Кэли

В этом параграфе мы покажем, что *каждая* группа может рассматриваться как подгруппа группы перестановок.

1. Теорема Кэли. В главе 1 мы рассматривали таблицу Кэли конечной квазигруппы G. В 1854 году Кэли заметил, что все строки этой

таблицы получаются перестановкой G, и, таким образом, G *отображается* в некоторое подмножество группы S_G. В действительности, для квазигруппы все строки таблицы Кэли различны, так что G *вкладывается* в S_G. Если G не является группой, это вложение, конечно, не может быть *гомоморфизмом*, т. е. не сохраняет произведения. Однако, **как доказал Жордан**, если G — группа, это действительно так, причем не обязательно даже предполагать, что G конечна. Сопоставим каждому элементу $g \in G$ **левую трансляцию** $L_g : G \longrightarrow G$, заданную *левым* умножением на g, $L_g(x) = gx$ (исторически от немецкого `linke`, но сейчас, конечно, все думают, что от английского `left`).

Теорема Кэли. *Отображение $L : G \longrightarrow S_G$, $g \mapsto L_g$, является мономорфизмом G в симметрическую группу S_G.*

Доказательство. Покажем, прежде всего, что $L_g \in S_G$. В самом деле, L_g — инъекция: $L_g(x) = L_g(y)$ означает, что $gx = gy$ и, значит, сокращая на g слева, $x = y$. С другой стороны, L_g сюръекция, так как, для любого $y \in G$ уравнение $gx = L_g(x) = y$ имеет в G решение $x = g^{-1}y$.

Проверим теперь, что, $L : g \mapsto L_g$ осуществляет *инъекцию* G в $S_G \cong S_n$. В самом деле, пусть $L_h = L_g$ для каких-то $h, g \in G$. Тогда, в частности, $h = L_h(e) = L_g(e) = g$.

Нам остается лишь убедиться в том, что это отображение является гомоморфизмом. То, что это действительно так, демонстрируется следующей выкладкой:

$$L_{gh}(x) = (gh)(x) = g(hx) = L_g(L_h(x)) = (L_g \circ L_h)(x),$$

где $g, h, x \in G$. Заметим, что *именно* здесь использована ассоциативность умножения в G.

2. Левое регулярное представление. Построенное в теореме Кэли отображение $L : G \longrightarrow S_G$, $g \mapsto L_g$, называется **левым регулярным представлением** группы G. Вообще **пермутационным представлением** (alias, **представлением перестановками**) группы G называется любой гомоморфизм G в симметрическую группу S_X перестановок некоторого множества X. Пермутационное представление $\pi : G \longrightarrow S_X$ называется **точным**, если ого является мономорфизмом, т. е. если $\mathrm{Ker}(\pi) = 1$. В этой терминологии теорема Кэли утверждает, что $g \mapsto L_g$ задает точное пермутационное представление G.

Следствие. *Любая конечная группа G порядка n изоморфно вкладывается в симметрическую группу S_n.*

Задача. Покажите, что группа кватернионов не вкладывается в группу S_7, постройте ее вложение в группу S_8.

Замечание. Многие авторы называют *сдвигами* то, что мы называем трансляциями, однако мы, по принятой в теории алгебраических групп и групп Ли традиции, *тщательно различаем* трансляции и сдвиги. А именно, **трансляция** (`translation`) — это преобразование самой группы, а **сдвиг** (`shift`) — это индуцированное трансляцией преобразование *функций* на группе. Ясно, что это совсем не одно и то же. Куда сдвигается график функции $x \mapsto f(x)$, если заменить x на $x+1$?

3. Правое регулярное представление. Возникает искушение определить *правое* регулярное представление группы G, сопоставив каждому $g \in G$ соответствующую **правую трансляцию** $R_g : G \longrightarrow G$, заданную *правым* умножением на g, $R_g(x) = xg$ (от немецкого `recht`, но при большом желании можно считать, что от английского `right`).

Точно так же, как в теореме Кэли мы можем доказать, что отображение $R : G \longrightarrow S_G$, $g \mapsto R_g$, будет вложением. Но будет ли оно гомоморфизмом, т. е. верно, ли, что $R_{gh} = R_g R_h$? Посмотрим, чему равно $R_{gh}(x)$:

$$R_{gh}(x) = x(gh) = (xg)h = R_h(xg) = R_h(R_g(x)) = (R_h \circ R_g)(x).$$

Таким образом, $R_{gh} = R_h R_g$, т. е. R является **антигомоморфизмом** (см. $\tilde{?}$, пример 2.2). Но ведь мы знаем, как изготовить из антигомоморфизма гомоморфизм: каждая группа антиизоморфна самой себе при помощи $\mathrm{inv} : g \mapsto g^{-1}$, а композиция двух антигомоморфизмов является гомоморфизмом. Это подсказывает следующее определение.

Назовем **правым регулярным представлением** группы G мономорфизм $R^- : G \longrightarrow S_G$, $g \mapsto R_{g^{-1}}$.

4. Конечные группы с циклическими силовскими 2-подгруппами. Вот одно из типичных применений теоремы Кэли.

Задача. Пусть G — конечная группа порядка $n = 2^l m$, где $l \geq 1$, $m \geq 3$ нечетно. Предположим, что в G есть элемент порядка 2^l. Тогда G не может быть простой.

Решение. Рассмотрим гомоморфизм $\varphi : G \longrightarrow S_G \longrightarrow \{\pm 1\}$, где $\varphi = \mathrm{sgn} \circ L$. Положим $H = \mathrm{Ker}(\varphi) \trianglelefteq G$. Пусть $o(x) = 2^l$. Тогда $L_x \in S_G$ состоит из m циклов длины 2^l и, поэтому, $\mathrm{sgn}(L_x) = -1$. Тем самым, $x \notin H$ и, значит, $H \neq G$. С другой стороны, все элементы нечетного порядка лежат в H, так что $H \neq 1$.

Знаменитая теорема Томпсона-Фейта утверждает, что порядок неабелевой конечной простой группы делится на 2.

Задача. Докажите, что порядок неабелевой конечной простой группы делится на 4.

§ 6♢. Действие подгруппы трансляциями

$H \times G \longrightarrow G$, $(h, g) \mapsto hg$. При этом орбиты H — это в точности смежные классы G по H.

Аналогично,

§ 8♠. Голоморф

Сейчас для любой группы G мы построим такую группу, в которой все автоморфизмы группы G становятся внутренними. Подгруппа

$$\mathrm{Hol}(G) = \langle L(G), \mathrm{Aut}(G)\rangle$$

симметрической группы S_G, порожденная множеством $L(G) = \{L_g \mid g \in G\}$ левых сдвигов и всеми автоморфизмами группы G, называется **голоморфом** группы G. Изучим строение голоморфа.

Задача. Докажите, что

$$\mathrm{Hol}(G) = \langle R(G), \mathrm{Aut}(G)\rangle,$$

где $R(G) = \{R_g \mid g \in G\}$ — множество правых сдвигов.

Задача. Покажите, что $L(G) \trianglelefteq \mathrm{Hol}(G)$ и $L(G) \cap \mathrm{Aut}(G) = 1$. Таким образом, $\mathrm{Hol}(G) = \mathrm{Aut}(G) \leftthreetimes L(G)$, где $\mathrm{Aut}(G)$ действует на $L(G)$ по формуле $\varphi L_g \varphi^{-1} = L_{\varphi(g)}$, для любых $\varphi \in \mathrm{Aut}(G)$, $g \in G$.

Задача. Покажите, что $\mathrm{Hol}(G) = \mathrm{Aut}(G) \leftthreetimes R(G)$. Каким образом $\mathrm{Aut}(G)$ действует на $R(G)$?

Задача. Покажите, что в голоморфе выполняется двойное централизаторное условие:

$$C_{\mathrm{Hol}(G)}(L(G)) = R(G), \qquad C_{\mathrm{Hol}(G)}(R(G)) = L(G).$$

§ 9♢. Действие на смежных классах, ♠ обобщенная теорема Кэли

Группа G действует слева на множестве G/H смежных классов G по $H \leq G$. Сейчас мы обобщим теорему Кэли на этот случай. Напомним, что **сердцевиной** группы H называется группа $H_G = \cap gHg^{-1}$, $g \in G$. Группа H_G это в точности наибольший нормальный делитель группы G, содержащийся в H.

Теорема. *Ядро действия G на G/H равно H_G. При этом G/H_G изоморфна подгруппе симметрической группы $S_{G/H}$.*

Доказательство. Если $gH = H$ для какого-то $g \in G$, то $g \in H$. Поэтому стабилизатор класса $H \in G/H$ в G равен $H \leq G$. Так как G действует на G/H транзитивно, то все стабилизаторы сопряжены со стабилизатором точки $H \in G/H$, точнее, стабилизатор точки $gH \in G/H$ имеет вид gHg^{-1}. Ядро действия — это в точности пересечение стабилизаторов всех точек, ясно, что это нормальная подгруппа. Обратно, если N — какая-то нормальная подгруппа группы G, содержащаяся в H, то для любого $g \in G$ имеем $N = gNg^{-1} \leq gHg^{-1}$. Таким образом, $N \leq H_G$. Так как действие G на G/H является *точным* действием G/H_G на G/H, то $G/H_G \leq S_{G/H}$.

Следствие 1. *Если $|G : H| = n$, то $|G : H_G| | n!$.*

В частности, мы получаем еще одно доказательство теоремы Пуанкаре, которую мы видели в главе 3.

Следствие 2. *Если $|G : H| < \infty$, то $|G : H_G| < \infty$.*

Следствие 3. *Если G конечна и $|G : H| = p$, где p — наименьшее простое, делящее $|G|$, то $H \trianglelefteq G$.*

Доказательство. В самом деле, по теореме $|G : H_G|$ делит $p!$. Так как никакое простое меньшее, чем p не делит $|G|$, то $|G : H_G| = 1$ или $|G : H_G| = p$, но ведь $H_G \leq H$, так что первая возможность исключена. Но это значит, что $H_G = H$.

Задача. Докажите, что если G *простая* группа с подгруппой индекса n, то она изоморфна подгруппе в S_n.

Задача. Пусть G — конечная простая группа, $|G| = p^r m$, где $p \perp m$. Докажите что $p^r | m$.

Задача. Докажите, что в конечной простой группе порядка > 60 не существует собственных подгрупп индекса ≤ 5.

Задача. Пусть G — конечная простая группа с элементом порядка 21. Докажите, что тогда индекс любой собственной подгруппы ≥ 10.

Задача. Пусть $H \leq G$ — подгруппа конечной простой группы G такая, что $|G : H| = p$. Покажите, что p должно быть наибольшим простым делящим порядок группы G.

Задача. Пусть G — конечная простая группа, $p^2 || |G|$. Докажите, что тогда в G нет подгрупп индекса p.

Задача. Пусть G — конечная группа, силовская 2-подгруппа которой циклична. Докажите, что тогда в G есть *нормальная* подгруппа $H \trianglelefteq G$ нечетного порядка такая, что $|G : H| = 2^m$.

Следствие. *В бесконечной простой группе не существует подгрупп конечного индекса.*

Упражнение. Докажите, что в бесконечной простой группе любой класс $C \neq 1$ сопряженных элементов бесконечен.

Упражнение. Докажите, что в бесконечной простой группе у любой подгруппы $1 < H < G$ бесконечное число сопряженных.

Задача. Если $H \leq G$ — подгруппа конечного индекса такая, что G совпадает с объединением сопряженных с H, то $H = G$.

Указание. Можно считать, что $|G| < \infty$.

Задача. Доказать, что в конечно порожденной группе имеется лишь конечное число подгрупп индекса n.

Решение. А сколько у конечно-порожденной группы гомоморфизмов в S_n?

§ 10♢. Действие группы на себе сопряжениями

1. Действие $G \times G$. При помощи регулярных представлений можно строить и более интересные пермутационные представления. Для начала заметим, что асоциативность произведения в G эквивалентна тому, что все левые трансляции коммутируют со всеми правыми трансляциями: $L_g R_h = R_h L_g$ для всех $h, g \in G$. В самом деле, $(L_g R_h)(x) = g(xh) = (gx)h = (R_h L_g)(x)$.

Таким образом, в действительности, комбинируя левое и правое регулярное представления G, мы получаем представление $G \times G$ прямого произведения *двух копий* группы G в S_G, а именно, $G \times G \longrightarrow S_G$, $(h, g) \mapsto L_h R_{g^{-1}}$. Конечно, в общем случае это представление не является точным, так как, если $h = g \in C(G)$ — центральный элемент, то $L_g R_{g^{-1}} = \mathrm{id}_G$

2. Действие левыми сопряжениями. Особый интерес представляет композиция диагонального вложения

$$\Delta : G \longrightarrow G \times G, \qquad g \mapsto (g, g),$$

с этим представлением. По определению при этом $g \in G$ переходит в $I_g = L_g R_{g^{-1}}$. Композиция двух гомоморфизмов — гомоморфизм.

Проведем еще раз вычисление в этом случае, чтобы посмотреть, как в нем используется тот факт, что L_g и R_h коммутируют:

$$I_{hg} = L_{hg}R_{(hg)^{-1}} = L_hL_gR_{g^{-1}h^{-1}} = \\ L_hL_gR_{h^{-1}}R_{g^{-1}} = L_hR_{h^{-1}}L_gR_{g^{-1}} = I_hI_g.$$

Таким образом, отображение $I : G \longrightarrow S_G$, $g \mapsto I_g$, является перестановочным представлением группы G. При этом представлении $g \in G$ сопоставляется перестановка $I_g : G \longrightarrow G$, $x \mapsto gxg^{-1}$, т. е. **внутренний автоморфизм** группы G, отвечающий $G \in G$. Это представление обычно называется **представлением G сопряжениями** на себе. Значительная часть теории групп связана с изучением этого представления — например, все учение о канонической форме операторов ('спектральная теория') есть, по существу, изучение этого представления в специальном случае, когда G является группой автоморфизмов векторного пространства.

3. Действие правыми сопряжениями. Образ элемента x под действием I_g часто обозначается также ${}^gx$, иными словами, ${}^gx = I_g(x) = gxg^{-1}$. При этом ${}^{gh}x = {}^g({}^hx)$. Однако не все привыкли записывать показатель степени слева. Тем не менее, мы не можем просто обозначить ${}^gx$ через x^g, потому что при этом получилась бы весьма странно выглядящая формула $x^{gh} = (x^h)^g$. В предыдущем пункте мы уже разобрались, как бороться с этой проблемой: нужно перейти к обратным. Поэтому для $x, g \in G$ обычно полагают $x^g = {}^{g^{-1}}x = g^{-1}xg$. При этом выполняется обычная формула $x^{gh} = (x^g)^h$. Однако следует иметь в виду, что отображение $g \mapsto I_{g^{-1}} = (x \mapsto x^g)$ *не является* представлением группы G перестановками, так как оно задает гомоморфизм G не в симметрическую группу S_G, а в *противоположную* группу, в которой умножение перестановок осуществляется не справа налево, как обычно, а слева направо (что соответствует случаю, когда функция пишется **справа** от аргумента, $(x)\sin$).

Задача. Докажите, что если $H \trianglelefteq G$ — нормальная подгруппа порядка 3, не содержащаяся в центре G, то в G есть подгруппа индекса 2.

§ 11♢. Орбиты и стабилизаторы

Пусть $G \curvearrowright X$. Сейчас мы свяжем с каждым элементом $x \in X$ подмножество Gx в G и подгруппу G_x в G.

Орбитой элемента $x \in X$ называется множество

$$Gx = \{gx \mid g \in G\} \subseteq X.$$

$X = X_1 \sqcup \ldots \sqcup X_s$ — разложение на орбиты.

Говорят, что действие G на X **транзитивное**, если X состоит из одной орбиты. В этом случае для любых $x, y \in X$ существует $g \in G$ такое, что $gx = y$. Само X в этом случае называется **G-однородным множеством** или, как принято говорить в геометрии и анализе, **однородным пространством** группы G.

Стабилизатором элемента $x \in X$ называется подгруппа

$$G_x = \{g \in G \mid gx = x\} \leq G.$$

Многие авторы пользуются для G_x обозначением $C_G(x)$ и называют G_x **централизатором** или **подгруппой изотропии** x в G.

Теорема. $Gx \leftrightarrow G/G_x$

Лемма. *Стабилизаторы двух точек $x, y \in X$ лежащих в одной орбите сопряжены в G.*

Доказательство. В самом деле, если $gx = y$ для некоторого $g \in G$, то для любого $h \in G_y$ имеем $(g^{-1}hg)x = g^{-1}hy = g^{-1}y = x$. Таким образом, $g^{-1}G_y g \leq G_x$ или, что то же самое, $G_y \leq gG_x g^{-1}$. С другой стороны, так как $g^{-1}x = y$, то $gG_x g^{-1} \leq G_y$. Но это и значит, что $G_y = gG_x g^{-1}$.

Пусть $Y \subseteq X$. Подгруппа, состоящая из всех $g \in G$ таких, что $gx = x$ для всех $x \in Y$, называется **поэлементным стабилизатором** (`element-wise stabiliser`) подмножества Y и обозначается через $C_G(Y)$. Легко видеть, что $C_G(Y) = \cap G_x$, где пересечение берется по всем $x \in Y$.

Пример. Пусть группа G действует на себе сопряжениями. Тогда

§ 12♡. Главные однородные пространства

1. Главные однородные пространства. Действие группы G на множестве X называется **свободным**, если $\mathrm{Stab}_G(x) = 1$ для любого $x \in X$. Действие группы G на множестве X называется **просто транзитивным**, если для любых $x, y \in X$ существет *единственное* $g \in G$ такое, что $gx = y$.

Задача. Докажите, что действие G на X в том и только том случае просто транзитивно, когда оно транзитивное и свободное.

Задача. Если G абелева, то ее действие на X в том и только том случае просто транзитивно, когда оно транзитивное и точное.

Условие, что G абелева, убрать нельзя. Симметрическая группа S_X действует на X точно и транзитивно, но при $n \geq 3$ это действие не является просто транзитивным.

Задача. Действие группы G на себе левыми/правыми трансляциями просто транзитивно.

Множество X на котором группа G действует просто транзитивно, называется **главным однородным пространством** для группы G. Как G-множество оно изоморфно самой группе G относительно действия G на себе трансляциями, но изоморфизм этот, вообще говоря, не является каноническим! Для установления изоморфизма нужно зафиксировать точку $x \in X$. Тогда $G \longrightarrow X$, $g \mapsto gx$, и будет искомым изоморфизмом.

2. Аффинные пространства. Первый пример главных однородных пространств, встречающийся каждому еще в школьной математике, это аффинные пространства. Сейчас, наконец, мы можем объяснить начинающему одну из главных загадок школьной геометрии: а именно, мы проясним различие между точками, свободными векторами и связанными векторами. С позиции линейной алгебры векторы — это *свободные* векторы. Да, но что такое тогда точки? Векторы можно складывать, но точки складывать нельзя, их можно только вычитать, причем разность двух точек является вектором.

Ситуация здесь такова. Пусть K^n — векторное пространство размерности n над полем K. Чтобы связать это со школьной геометрией, возьмите здесь $K = \mathbb{R}$ и вообразите случай $n = 2$ или $n = 3$. Это все еще не будет тем, что в школьной геометрии обычно называется эвклидовой плоскостью или эвклидовым пространством. Дело в том, что в пространстве K^n есть выделенная точка 0, в то время как в эвклидовом пространстве элементарной геометрии такой точки нет! Аксиоматика Германа Вейля состояла ровно в том, что в ней n-мерное эвклидово пространство определяется в терминах векторного пространства $\mathbb{R}^n$ с дополнительной структурой в виде скалярного произведения. Отвлекаясь пока от метрических свойств пространства E, а также от вещественной координатизации, рассмотрим *аффинные* пространства над произвольным полем.

С чисто алгебраической точки зрения $E = E^n$ представляет собой *главное однородное пространство* над K^n. Чтобы отличать его элементы от элементов K^n, называемых **векторами**, элементы E^n называются **точками**. При этом считается, что задано действие $K^n \times E^n \longrightarrow E^n$, $(u, x) \mapsto x + u$, превращающее E^n в главное однородное пространство над K^n. Иными словами, каждой точке x и каждому

вектору u сопоставляется точка $x+u$. При этом как всегда предполагается, что для любой точки x и любых двух векторов u, v имеет место равенство $x+(u+v)=(x+u)+v$ и, кроме того, $x+0=x$. Кроме того, требуется, чтобы для любых двух точек x, y существовал *единственный* вектор x такой, что $u+x=v$. Как всегда, аффинное пространство становится изоморфным векторному пространству *после того*, как в нем выбрано начало координат — но вся фишка в том, что в E^n как раз не выбрано никакого начала координат.

Разность $y-x$ двух точек x, y интерпретируется как тот *единственный* вектор u такой, что $x+u=y$. В свою очередь связанный векторы истолковывается как дупель $(u,x)\in K^n\times E^n$, состоящий из вектора и точки. При этом на множестве $K^n\times E^n$ вводится частичная операция, а именно, $(u,x)+(v,y)$ определено только если $y=x+u$, и в этом случае равно $(u+v,x)$.

§ 13♡. Классификация однородных пространства

Классификация транзитивных G-множеств

Задача (аргумент Фраттини). Пусть X — конечное G-множество, $H\le G$ транзитивно действует на X. Тогда $G=HG_x$ для любого $x\in X$.

Задача. Пусть X — транзитивное G-множество, $x\in X$, $H=G_x$ — стабилизатор точки x. Покажите, что H-орбиты на X находятся в биективном соответствии с $H\backslash G/H$.

Теорема. *Любое левое однородное G-множество изоморфно множеству G/H правых смежных классов по какой-то подгруппе $H\le G$.*

Два множества G/F и G/H в том и только том случае изоморфны, когда F и H сопряжены в G.

Доказательство. В самом деле,

§ 13♠. Бернсайдовское кольцо конечной группы

Пусть G — конечная группа. Рассмотрим $\mathbb{Z}$-модуль с базисом, состоящим из X, где X пробегает множество классов изоморфизма левых однородных G-множеств. Иными словами, можно сказать, что в качестве базиса $A(G)$ выступают классы G/H, где H пробегает представители классов сопряженности подгрупп в G. Умножение в $A(G)$ описывает разложение $G/F\times G/H$ на орбиты.

§ 14♠. Лемма [не] Бернсайда, раскраски куба

На русском языке эта теория изложена, например, в книгах [**93**], ?? , [240], [241]. Следующее элементарное соображение представляет собой еще одну аватару изменения порядка суммирования (метод подсчета двумя способами). Долгое время оно было известно под кодовым названием **лемма Бернсайда**, хотя в последнее время более распространено название **лемма не Бернсайда** (`not Burnside lemma`). Эта лемма была доказана Фробениусом в 1887 году и неоднократно использовалась Шуром, но, как считается, была впервые опубликована в 1911 году Бернсайдом в его книге *Theory of groups of finite order*. Впрочем, возможны и другие точки зрения, например, Питер Нойман [242] утверждает, что *идею* доказательства этой леммы можно найти в работе Коши 1845 года и предложил переименовать ее в **лемму Коши—Фробениуса**. Джозеф Ротман называет ее **теоремой Коши—Фробениуса**. Киевская школа придерживается **нулевого варианта** и называет ее **леммой Коши—Фробениуса—Бернсайда**.

Мы уже неоднократно сталкивались с тем, что не следует недооценивать мощь элементарных соображений. Элементарное соображение, которые мы сейчас сформулируем, лежит в основе **теории перечисления Редфилда—Пойа** и уже через пару страниц читатель поймет, что ее способность производить вычисления, связанные с конечными вероятностями и перечислительными задачами комбинаторики, возросла в *десятки* раз. Для разминки попробуйте ответить на следующий вопрос: сколькими существенно различными способами можно раскрасить грани икосаэдра в 7 цветов?

Лемма не Бернсайда. *Пусть конечная группа G действует на конечном множестве X и $X_1, \dots, X_s$ орбиты этого действия. Тогда*

$$\frac{1}{|G|}\sum_{g\in G} |\operatorname{Fix}_X(g)| = s.$$

Доказательство. Подсчет двумя способами. Рассмотрим график отношения изотропии $gx = x \iff x$ фиксируется $g \iff g$ стабилизирует x:

$$R = \{(g,x) \mid g\in G, x\in X, gx = g\} \subseteq G\times X.$$

Просуммировав вначале по x, а потом по g, получим

$$|R| = \sum_{g\in G} |\operatorname{Fix}_X(g)|.$$

Просуммируем теперь вначале по g, а потом по x. Для этого выберем какой-то представитель x_i орбиты X_i и воспользуемся тем, что в действительности $|G_x|$ зависит не от самого x, а только от его орбиты $Gx = X_i = Gx_i$. Так как G_x и G_{x_i} сопряжены, то их порядки совпадают. Поэтому

$$|R| = \sum_{x\in X} |G_x| = \sum_{i=1}^{s} \left(\sum_{x\in X_i} |G_{x_i}| \right) =$$

$$\sum_{i=1}^{s} (|X_i||G_{x_i}|) = \sum_{i=1}^{s} (|G : G_{x_i}||G_{x_i}|) =$$

$$\sum_{i=1}^{s} |G| = s|G|$$

Сравнивая два эти выражения для $|R|$ получаем результат.

Следующие миленькие примеры взяты из дополнения к книге [243] (после исправления нескольких опечаток).

Пример 1. Группа S_n транзитивно действует на $X = \{q, \dots, n\}$. Поэтому

$$\frac{1}{n!} \sum_{\pi\in S_n} |\operatorname{Fix}_X(\pi)| = 1.$$

Это значит, что *в среднем* каждая перестановка фиксирует провно один символ.

Пример 2. Группа S_n 2-транзитивна на X. Это значит, что у действия $\pi(x, y) = (\pi x, \pi y)$ группы G на $X \times X$ ровно две орбиты: **диагональ** $\Delta = \{(x, x) \mid x \in X\}$ и **все остальное** $X \times X \setminus \Delta$. Легко видеть, что $\operatorname{Fix}_{X\times X}(\pi) = \operatorname{Fix}_X(\pi) \times \operatorname{Fix}_X(\pi)$. Поэтому

$$\frac{1}{n!} \sum_{\pi\in S_n} |\operatorname{Fix}_X(\pi)|^2 = 2.$$

Это значит, что среднее значение *квадрата* порядка неподвижных точек перестановки на n буквах равно 2.

Задача. Каково среднее значение *куба* порядка неподвижных точек перестановки на n буквах?

Пример 3. Сколько существует существенно различных раскрасок куба с использованием n цветов? Под существенно различными раскрасками мы подразумеваем такие, которые не переводятся друг в

друга вращением куба. В случае $n = 1$ такая раскраска, очевидно, ровно одна. В случае $n = 2$ все раскраски тоже несложно перечислить. Пусть, например, два цвета это R — `red` и B — `blue`. Очевидно, что каждому из случаев $6R$, $6B$, $5R + B$, $R + 5B$ отвечает единственная раскраска. В случае $4R + 2B$ имеется две раскраски, в зависимости от того, являются две синих грани противоположными или смежными. То же относится, разумеется к случаю $2R+4B$, с заменой B на R. Наконец, случаю $3R+3B$ тоже отвечает две раскраски, в зависимости от того, есть ли среди красных граней две противоположные, или они все три сходятся в одном углу. Однако перечислить в стиле устного счета все раскраски граней куба в *три* цвета R, B и G — `green`, не пропустив при этом чего-нибудь, представляется уже *малореальным* — в действительности, как мы сейчас увидим, таких раскрасок 57.

Итак, пусть C — множество цветов. Вспомним (см. § ? главы I), как устроены все 24 вращения куба и рассмотрим их действие на множестве Y, состоящем из 6 и на множестве $X = C^Y$ раскрасок граней (каждой грани сопоставляется цвет). Итого — это общий вклад в формулу Бернсайда

∘ 1 тождественное вращение, сохраняющее все 6 граней и все n^6 раскрасок. Итого n^6.

∘ 8 вращений на углы $2\pi/3$, $4\pi/3$ вокруг главных диагоналей куба, имеющих по 2 орбиты на гранях (порядков 3 и 3) и, соответственно, по n^2 орбит на раскрасках. Итого $8n^2$.

∘ 6 вращений на угол π вокруг прямых, соединяющих середины противоположных ребер, имеющих по 3 орбиты на гранях (порядков 2,2,2) и, соответственно, по n^3 орбит на раскрасках. Итого $6n^3$.

∘ 6 вращений на углы $\pi/2$, $3\pi/2$ вокруг прямых, соединяющих центры противоположных граней, имеющих по 3 орбиты на гранях (порядков 4,1,1) и, соответственно, по n^3 орбит на раскрасках. Итого $6n^3$.

∘ 3 вращения на угол π, вокруг прямых, соединяющих центры противоположных граней, имеющих по 4 орбиты на гранях (порядков 2,2,1,1) и, соответственно, по n^4 орбит на раскрасках. Итого $3n^4$.

Таким образом, по лемме Бернсайда общее число орбит на X равно, которые мы назвали существенно различными раскрасками, равно

$$s = \frac{n^6 + 3n^4 + 12n^3 + 8n^2}{24}.$$

Имея под рукой карманный калькулятор, теперь каждый при желании может посчитать, что имеется 240 раскрасок на 4 цвета, 800 раскрасок

на 5 цветов, 2226 раскрасок на 6 цветов, 5390 раскрасок на 7 цветов, 11712 раскрасок на 8 цветов, 23355 раскрасок на 9 цветов и 43450 раскрасок на 10 цветов. Ну и, скажем, 106906070700 раскрасок на 117 цветов.

Задача. Сколько существует существенно различных раскрасок ребер куба на n цветов?

Задача. А вершин?

Задача. Сколько существует существенно различных раскрасок граней полого куба на 2 цвета, если мы хотим покрасить грани как снаружи, так и изнутри?

Ну а теперь Вы вполне созрели, чтобы вернуться к задаче, над которой Вы безуспешно думали в начале параграфа, вспомнив предварительно, как устроена группа вращений икосаэдра (см. § ? главы 1).

Задача. Сколькими существенно различными способами можно раскрасить грани икосаэдра в n цветов?

§ 15♠. Основные конструкции над G-множествами

1. Ограничение действия. Пусть X есть G-множество. Подмножество $Y \subseteq X$ называется **устойчивым** относительно действия G, если $GY \subseteq Y$, т. е., иными словами, $gy \in Y$ для любого $g \in G$, $y \in Y$. Любое устойчивое подмножество $Y \subseteq X$ можно рассматривать как G-множество посредством $G \times Y \longrightarrow Y$, $(g, y) \mapsto gy$. Это действие называется **ограничением** действия G на X.

2. Множество неподвижных точек. Отметим тривиальный, но важный случай ограничения действия. Обозначим через X^G множество **неподвижных точек** действия G на X, т. е. множество таких $x \in X$, что $gx = x$ для всех $g \in G$. По определению $X^G = \cap \mathrm{Fix}_g(X)$, где пересечение берется по всем $g \in G$. Тогда X^G является наибольшим подмножеством в X, на котором G действует тривиально.

3. Индуцированные действия. Пусть X есть G-множество. Отношение эквивалентности $\sim$ на X называется **согласованным** с действием G или **конгруэнцией**, если из того, что $x \sim y$ для любого $g \in G$ вытекает, что $gx \sim gy$. Обозначим через $\overline{x}$ класс элемента x относительно $\sim$. Для конгруэнции $\sim$ на X фактор-множество $X/\sim$ можно превратить в G-множество, полагая $g\overline{x} = \overline{gx}$ для всех $g \in G$, $x \in X$. *Корректность* этого определения, т. е. независимость $g\overline{x}$ от выбора представителя $x \in \overline{x}$ сразу вытекает из того, что $\sim$ конгруэнция.

4. Множество орбит. Снова отметим тривиальный, но важный случай индуцированного действия. А именно, пусть $\sim = \sim_G$ представляет собой отношение G-сопряженности. Тогда, очевидно, $\sim$ представляет собой конгруэнцию (в самом деле, если $x \sim y$, то $gx \sim x \sim y \sim gy$). Фактор-множество $X/\sim_G$ обозначается обычно через X/G и называется множеством орбит для действия G на X. Множество X/G является наибольшим фактор-множеством множества X, на котором G действует тривиально.

5. Действие подгруппы. Пусть X есть G-множество, а $H \leq G$ — подгруппа в G. Тогда очевидно X можно рассматривать как H-множество. При этом если $\mathrm{act} : G \times X \longrightarrow X$ есть действие G на X, то действие H на X является ограничением act на $H \times X$. В дальнейшем мы будем использовать эту конструкцию без всяких специальных ссылок.

6. Связь между орбитами группы и подгруппы. Пусть, как и выше, X есть G-множество, а $H \leq G$ — подгруппа в G. Тогда для каждого $x \in X$ выполняется включение $Hx \subseteq Gx$. Таким образом, каждая орбита группы G на X является объединением орбит группы H, иными словами $x \sim_H y$ влечет $x \sim_G y$. Обратное, вообще говоря, неверно, т. е. элементы $x, y \in X$ могут быть сопряжены относительно G, но не относительно H. Если орбита Gx точки $x \in X$ является объединением более, чем одной орбиты группы G, то говорят, что она **распадается** при ограничении действия на H. По отношению же к орбитам группы H используется следующая терминология. Если Hx и Hy суть две различные H-орбиты, которые содержатся в одной и той же G-орбите, т. е. $Gx = Gy$, то говорят, что они **сливаются** под действием G, а сам этот феномен называется **слиянием** (fusion).

?. Действие на булеане. Пусть X есть G-множество. Тогда действие G на 2^X задается следующим образом. Для $g \in G$ и $Y \subseteq X$ положим $gY = \{gy \mid y \in Y\}$. Легко видеть, что этим действительно задается действие G на 2^X.

?. Внешняя степень действия. Действие G на 2^X не может быть транзитивным. В самом деле, если $|gY| = |Y|$. Таким образом, орбиты группы G при действии на 2^X заведомо содержатся в подмножествах булеана, состоящих из множеств фиксированной мощности. Особенно большой интерес представляет действие G на конечных подмножествах.

§ 16♠. Произведение, копроизведение и расслоенное произведение G-множеств

1. Копроизведение G-множеств. Пусть X, Y — два G-множества. Тогда G действует на их теоретико-множественном копроизведении $X \sqcup Y$. А именно, для любых $g \in G$ и $z \in X \sqcup Y$ положим $gz = \mathrm{act}_X(g, z)$, если $z \in X$ и $gz = \mathrm{act}_Y(g, z)$, если $z \in Y$.

2. Прямое произведение G-множеств. Если X, Y — два G-множества, безразлично, левых или правых, то на их теоретико-множественном прямом произведении естественно определяется левое и правое действие G. Например, если X, Y — два левых G-множества то G действует на $X \times Y$ слева посредством $g(x, y) = (gx, gy)$. Точно так же, если X — правое, а Y — левое, то G действует на $X \times Y$ слева посредством $g(x, y) = (xg^{-1}, gy)$. Читатель при желании без труда напишет и все оставшиеся шесть вариантов.

3. Действие на m-ках.

4. Расслоенное произведение G-множеств. Пусть X и Y — два G-множества. Фактор-пространство $X \times Y$ по отношению эквивалентности связанному с действием G называется расслоенным произведением X и Y и обозначается $X \times_G Y$.

Пусть, например, $F, H \leq G$. Положим $X = F\backslash G$, $Y = G/H$. Тогда множество $X \times_G Y$ изоморфно $F\backslash G/H$.

§ 17♠. Действие на отображениях G-множеств

Пусть теперь X и Y суть два G-множества и $\mathrm{Map}(X, Y)$ — множество всех отображений из X в Y. Сейчас мы обсудим вопрос о том, как действие G на X и/или Y переносится на $\mathrm{Map}(X, Y)$. Оказывается, по отношению к X и Y действие G на $\mathrm{Map}(X, Y)$ выглядит совершенно по разному.

1. Действие на значениях. Пусть вначале G действует на Y слева. Определим действие G на $\mathrm{Map}(X, Y)$ следующим образом. Для $g \in G$ и $\varphi \in \mathrm{Map}(X, Y)$ определим $g\varphi$ как отображение $g\varphi : X \longrightarrow Y$, получающееся из φ действием g на значения, т. е. $(g\varphi)(x) = g\varphi(x)$ для любого $x \in X$. Легко убедиться, что этим на $\mathrm{Map}(X, Y)$ определяется структура левого G-множества. Тем самым левое действие G на Y индуцирует левое действие G на $\mathrm{Map}(X, Y)$. Ясно, что точно так же правое действие G на Y индуцирует правое действие G на $\mathrm{Map}(X, Y)$.

2. Действие на аргументах. Пусть теперь G действует на X слева. Попытаемся определить действие G на $\mathrm{Map}(X, Y)$ слева по аналогии

с тем, как мы делали это в предыдущем пункте, а именно, определим для $g \in G$ и $\varphi \in \mathrm{Map}(X, Y)$ образ φ под действием g посредством $(g\varphi)(x) = \varphi(gx)$. Действительно ли эта формула определит левое действие G на $\mathrm{Map}(X, Y)$? Унитальность очевидным образом выполнена, но вот как обстоит дело с внешней ассоциативностью? Возьмем два элемента $g, h \in G$ и вычислим $(gh)\varphi$. Для любого $x \in X$ имеем

$$((gh)\varphi)(x) = \varphi((gh)x) = \varphi(g(hx)) = (g\varphi)(hx) = (h(g\varphi))(x).$$

Это значит, что в действительности формула $(g\varphi)(x) = \varphi(gx)$ определяет не левое, а правое действие G на $\mathrm{Map}(X, Y)$, так что было бы правильнее писать $(\varphi g)(x) = \varphi(gx)$.

Таким образом, мы пришли к заключению, что левое действие G на X естественно приводит к правому действию G на $\mathrm{Map}(X, Y)$. Это подсказывает, что для того, чтобы определить левое действие на $\mathrm{Map}(X, Y)$, группа G должна действовать на X справа. Итак, предположим, что X есть правое G-множество и зададим для $g \in G$ и $\varphi \in \mathrm{Map}(X, Y)$ отображение $g\varphi$ формулой $(g\varphi)(x) = \varphi(xg)$. Вот теперь мы действительно получим левое действие, как показывает следующая выкладка

$$((gh)\varphi)(x) = \varphi(x(gh)) = \varphi((xg)h) = (h\varphi)(xg) = (g(h\varphi))(x).$$

Вывод, к которому мы пришли не должен удивлять. Хорошо известно, что множество отображений $\mathrm{Map}(X, Y)$ ведет себя контравариантно по отношению к первому аргументу, а это как раз и значит, что направление всех отображений меняется на противоположное, так что, в частности, левые и правые множества должны меняться местами.

3. Действие на аргументах: вариация. Предположим, что G действует на X слева, а мы все же хотим задать на $\mathrm{Map}(X, Y)$ левое действие. Для этого, в соответствии с предыдущим пунктом мы должны прежде всего превратить X в правое G-множество. Как мы знаем из § 2, имеется канонический способ сделать это. А именно, пусть $g \in G$, $\varphi \in \mathrm{Map}(X, Y)$. Определим отображение $g\varphi$ следующим образом: положим $(g\varphi)(x) = \varphi(g^{-1}x)$. Тогда, как мы знаем из предыдущего пункта, этим задается левое действие G на $\mathrm{Map}(X, Y)$. Проведем еще раз соответствующее вычисление:

$$\begin{aligned}((gh)\varphi)(x) = \varphi((gh)^{-1}x) =& \varphi((h^{-1}g^{-1})x) = \\ =& \varphi(h^{-1}(g^{-1}x)) = (h\varphi)(g^{-1}x) = (g(h\varphi))(x).\end{aligned}$$

Совершенно ясно, что точно так же можно превратить $\mathrm{Map}(X,Y)$ в правое G-множество отправляясь от правого действия G на X, при помощи формулы $(\varphi g)(x) = \varphi(xg^{-1})$.

4. Действие на отображениях. Предположим, что

5. Множество эквивариантных отображений.
$\mathrm{Map}(X,Y)^G = \mathrm{Map}_G(X,Y)$.

§ 18♡. Несколько замечательных действий, возникающих в геометрии

Как мы уже знаем, группа Мебиуса $\mathrm{PSL}(2,\mathbb{C})$ действует на расширенной сфере Римана $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ посредством

$$\begin{matrix} a & b \\ c & d \end{matrix} \ : \ z \mapsto \frac{az+b}{cz+d}.$$

Следующие два примера имеют ключевое значение в геометрии, теории чисел и комплексном анализе.

1. Действие $\mathrm{PSL}(2,\mathbb{R})$ на плоскости Лобачевского. Обозначим через H верхнюю полуплоскость $\{z \in \mathbb{C} \mid \mathrm{im}(z) > 0\}$. Хорошо известно♮, что H можно мыслить себе как модель **плоскости Лобачевского***. При этом прямыми являются дуги окружностей, ортогональных вещественной оси (в том числе, конечно, и дуги окружностей бесконечного радиуса, т. е. направленные в верхнюю полуплоскость лучи ортогональные к вещественной оси). Эта интерпретация геометрии Лобачевского называется **моделью Пуанкаре♮**. Легко проверить (проделайте это!), что группа $\mathrm{PSL}(2,\mathbb{R})$ действует на H, иными словами, если $\mathrm{im}(z) > 0$, а $a,b,c,d \in \mathbb{R}$, то $\mathrm{im}\ \dfrac{az+b}{cz+d} > 0$.

2. Действие $\mathrm{PSL}(2,\mathbb{C})$ на трехмерном пространстве Лобачевского. Построить действие в этом случае чуть сложнее. А именно, рассмотрим следующую модель трехмерного пространства Лобачевского. Вложим поле комплексных чисел $\mathbb{C} = \mathbb{R}1 \oplus \mathbb{R}i$ в тело кватернионов $\mathbb{H} = \mathbb{R}1 \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ и обозначим через H следующее множество кватернионов $H = \{u+vi+wj \mid u,v,w \in \mathbb{R}, w > 0\}$. Определим следующее действие следующей формулой:

$$\begin{matrix} a & b \\ c & d \end{matrix} \ : \ u+vi+wj \mapsto \frac{(a(u+vi)+b)\overline{(c(u+vi)+d)} + a\bar{c}w^2 + wj}{|c(u+vi)+d|^2 + |c|^2t^2}.$$

Задача. Проверьте, что приведенная формула действительно определяет действие $\mathrm{PSL}(2,\mathbb{C})$ на H.

♮Например, из рисунков Мориса Эшера.

*Буква `H` является первой буквой слова `hyperbolic` — гиперболический, в англоязычной литературе геометрию Лобачевского принято называть гиперболической геометрией.

♮Часто моделью Пуанкаре называют конформно эквивалентную модель, при которой плоскость Лобачевского изображается внутренностью единичного круга, а прямыми являются дуги окружностей ортогональных к границе этого круга. Эти модели переводятся друг в друга преобразованием Кэли.

§ 19♣. Два замечательных действия S_3 и S_6

Пусть $K^\sharp = K \setminus \{0,1\}$. Следующее действие S_3 *реально* возникает при приведении уравнения **эллиптической кривой** к каноническому виду $y^2 = x(x-1)(x-\lambda)$ (см., например, [На], с.403–406).

1. Действие S_3. Заставим группу S_3 действовать на $K^\sharp$ следующим образом. Для заданного $\lambda \neq 0,1$ элемент $\pi \in S_3$ обычным образом переставляет $0,1,\lambda$, после чего к полученным элементам применяется аффинное преобразование, переводящее их в $0,1,\mu$. Элемент μ и провозглашается $f_\pi(\lambda)$.

Задача. Докажите, что это действие. Найдите орбиты группы S_3 в этом действии.

Указание. Посмотрите вначале на массовый случай $\mathrm{char}(K) \neq 2,3$, потом выясните, что происходит в исключительных характеристиках.

Решение. Аффинное преобразование f, переводящее a,b, $a \neq b$, в $0,1$ имеет вид $x \mapsto (x-a)/(b-a)$. Таким образом, если $f_{\mathrm{id}}(\lambda) = \lambda) = \mathrm{id}$, $f_{(12)}(\lambda) = 1-\lambda$, $f_{(13)}(\lambda) = \lambda/(1-\lambda)$, $f_{(23)}(\lambda) = 1/\lambda$, $f_{(123)}(\lambda) = 1/(1-\lambda)$ и, наконец, $f_{(132)}(\lambda) = (1-\lambda)/\lambda$. В задаче ? уже предлагалось проверить, что эти преобразования образуют группу относительно композиции. Таким образом, **все** орбиты шестиэлементные, вида

$$\{\lambda, 1-\lambda, \lambda/(1-\lambda), 1/\lambda, 1/(1-\lambda), (1-\lambda)/\lambda,$$

за исключением трехэлементной орбиты $\{-1,2,1/2\}$ и, *возможно*, двухэлементой орбиты $\{1+\omega, 1+\overline{\omega}\}$, где $\omega = \sqrt[3]{1}$, которая возникает, если $\omega \in K$. Таким образом, двухэлементная орбита состоит из первообразных корней 6-й степени из 1, если они лежат в поле K. Трехэлементная орбита появляется, когда λ стабилизируется транспозицией, скажем, $\lambda = 1/\lambda$, а двухэлементная орбита — когда λ стабилизируется 3-циклом, скажем, $\lambda = 1/(1-\lambda)$. Это последнее условие сводится к уравнению $\Phi_6(\lambda) = \lambda^2 - \lambda + 1 = 0$.

В исключительных характеристиках возможны следующие отклонения от этой стройной картины:

• Если $\mathrm{char}(K) = 2$, то орбиты $\{-1,2,1/2\}$ нет.

• Если $\mathrm{char}(K) = 2$, то уравнение $\lambda^2 - \lambda + 1 = 0$ принимает вид $\lambda^2 + \lambda + 1 = 0$, так что двухэлементная орбита состоит из первообразных корней степени 3, если они оежат в поле K.

• Если $\mathrm{char}(K) = 3$, то $-1 = 2 = 1/2$, так что трехэлементная орбита становится одноэлементной!

• Если $\mathrm{char}(K) = 3$, то $\lambda^2 - \lambda + 1 = 0$ принимает вид $\lambda^2 + \lambda + 1 = 0$, так что двухэлементная орбита не возникает.

Начинающему полезно осознать, что все это конкретно означает для небольших конечных полей таких как $\mathbb{F}_{25}$, $\mathbb{F}_{27}$, $\mathbb{F}_{32}$ и $\mathbb{F}_{49}$.

2. Действие S_6. В классификации кривых рода 2 возникает следующее обобщение этого примера (см. [На], упражнение 2.2 на стр. 385–386). Как мы узнаем в книге IV, если x,y,z три попарно различные точки из $\overline{K} = K \cup \{\infty\}$, то существует единственное **дробно-линейное преобразование** $\varphi : t \mapsto (at+b)/(ct+d)$ такое, что $\varphi(x) = 0$, $\varphi(y) = 1$, $\varphi(z) = \infty$. Определим действие S_6 на *тройках попарно различных точек* из $K^\sharp$ следующим образом. Для заданного $x,y,z \neq 0,1,\infty$ элемент

$\pi \in S_6$ обычным образом переставляет $0, 1, \infty, x, y, z$, после чего к полученным элементам применяется дробно-линейное преобразование φ, переводящее первые три из них в $0, 1, \infty$. Тройка $(\varphi(\pi(x)), \varphi(\pi(x)), \varphi(\pi(x)))$ и называется образом (x, y, z) под действием π.

Обобщение на это действие предыдущей задачи в полном объеме представляет собой достаточно суровое занятие (используйте `Mathematica` или `Maple`!). Ограничимся поэтому одним особенно интересным случаем.

Задача. Найти орбиты троек (x, y, z) под действием 5-цикла $(12345) \in S_6$.

Ответ. Несложное вычисление показывает, что этот цикл действует посредством

$$(x, y, z) \mapsto \quad \frac{y-1}{y-x}, \frac{1}{x}, \frac{z-1}{z-x} \quad .$$

Одноэлементные орбиты возникают в золотом сечении и корнях 5-й степени из 1.

§ 20♡. Каскады и потоки

Действие аддитивной группы $\mathbb{Z}$ на множестве X называется **каскадом** на X.

Действие аддитивной группы $\mathbb{R}$ на множестве X называется **потоком** на X. Пусть $I \subseteq \mathbb{R}$ — открытый интервал, содержащий 0. Действие I на X, задавыаемое отображением $I \times X \longrightarrow X$ называется **локальным потоком**, если

LF1. $(a + b)x = a(bx)$ каждый раз, когда $a, b \in I$ таковы, что $a + b \in I$

LF2. $0x = x$ для любого $x \in X$.

Часто удобнее считать, что задано отображение $\theta : I \longrightarrow S_X$, $a \mapsto \theta_a$, сопоставляющее каждому $a \in I$ преобразование θ_a множества X. Тогда локальный поток задается посредством $ax = \theta_a(x)$, а условия на действие запишутся в виде $\theta_{a+b} = \theta_a\theta_b$ и $\theta_0 = \mathrm{id}_X$.

Показать, что любой локальный поток на X единственным образом продолжается до потока на X. — ПРОРАБОТАТЬ!!

Соображение такое: пусть $I \subseteq \mathbb{R}$. Отображение $\varphi : I \longrightarrow G$ называется **локальным гомоморфизмом**, если $\varphi(a + b) = \varphi(a)\varphi(b)$ для всех $a, b \in I$ таких, что $a + b \in I$. Показать, что любой локальный гомоморфизм единственным образом продолжается до гомоморфизма $\mathbb{R} \longrightarrow G$.

Указание: для любого $x \in \mathbb{R}$ существует $n \in \mathbb{N}$ такое, что $x/n \in I$.

Коан. Как это согласуется с неединственностью решений дифференциальных уравнений?

Ответ: особые точки, там время заканчивается и начинается снова.

Аппендикс 1: Set[']s cradle

Ниже мы совсем коротко напоминаем некоторые обозначения, определяемые *где-то* в книге 1 Не совсем наивная теория множеств. Все эти обозначения совершенно стандартны и читатель может познакомиться с ними по любой книге по теории множеств. Тем, у кого нет доступа к электронному тексту моей книги, можно порекомендовать, например, замечательный недавний учебник [244].

§ 1. Логические символы

1. Логические связки. Мы будем пользоваться обычными символами исчисления высказываний:

$\vee$ — дизъюнкция* (**или**, or, vel);

$\wedge$ (а также &) — конъюнкция* (**и**, and, et);

$\neg$ — негация (alias отрицание, **не**, not, non);

$\Longrightarrow$ — импликация (**тогда**, **если** ..., **то** ..., **из** ... **следует** ..., ... **влечет** ...);

$\Longleftrightarrow$ — эквиваленция и/или логическая эквивалентность (**тогда и только тогда**, if and only if, se e solo se).

2. Кванторы. Единственными другими систематически используемыми нами логическими символами будут кванторы — три обычных квантора:

$\forall$ — квантор всеобщности* (for All, **для всех**);

$\exists$ — квантор сушествования* (Exists, **существует**);

---

*Символ $\vee$ представляет собой стилизованную букву V — первую букву слова vel — или.

*Символ $\wedge$ представляет собой перевернутый символ $\vee$, и его использование указывает на двойственность между $\wedge$ и $\vee$. В свою очередь, **амперсанд** & является сокращением латинского et, использовавшимся в рукописных текстах начиная со средних веков.

*Символ $\forall$ представляет собой перевернутую букву A — первую букву слова Allgemeinheit = общность, всеобщность.

*Символ $\exists$ представляет собой перевернутую букву E — первую букву слова Existenz = существование.

$\exists!$ — существует единственный.

Существует много других чрезвычайно полезных кванторов (`существует не более конечного числа`, `существует бесконечное множество`, `для всех`, `кроме конечного числа`, и т.д.), но, к сожалению, они не имеют общепринятых обозначений.

3. Значения истинности. В дальнейшем `True` и `False` обозначают, соответственно, истину и ложь[♮]. Некоторые авторы используют не сами эти слова, а лишь их первые буквы: `T` (`trivial`) и `F` (`falsch`), или первые буквы соответствующих латинских/итальянских слов `V` (`vero`) и `F` (`falso`) или приписывают истине булево значение 1, а лжи — значение 0. Однако большая часть наших высказываний в математике носит условный характер. Поэтому математикам (в отличие от логиков!) настолько редко приходится обращаться к абсолютной истине и лжи самим по себе, что получающаяся при использовании сокращений экономия бумаги не оправдывает потери ясности.

§ 2. Элементы и подмножества, булевы операции

Напомним теперь основные символы, касающиеся элементов и подмножеств.

$\in$ — знак принадлежности[♮], $a \in A$, a **принадлежит** A, a **является элементом** A;

$\ni$ — то же, $A \ni a$, A **содержит** a **в качестве элемента**;

$\subseteq$ — знак включения, $A \subseteq B$, A **является подмножеством** B;

$\supseteq$ — то же, $B \supseteq A$, B **является надмножеством** A, B **содержит** A **в качестве подмножества**;

$\subset$ — знак строгого включения, $A \subset B$, A **является собственным подмножеством** B, т. е. $A \subseteq B$ и $A \neq B$;

$\supset$ — то же, $B \supset A$, B **является собственным надмножеством** A, B **собственно содержит** A;

[♮]Понятия `true/vero` и `false/falso` относятся к **истинности** *высказываний* в формальной системе и не имеют **никакого** отношения к понятиям `right/giusto` и `wrong/sbagliato`, оценивающими **правильность** наших *идей*! *Правильное* высказывание может быть *ложным* и, тем самым, нет ничего необычного в том, чтобы *истинное* высказывание оказалось *ошибочным*.

[♮]Этот знак, введенный Пеано, является стилизованной буквой ϵ, первой буквой греческого слова $\epsilon\sigma\tau\iota$ — быть.

$\varnothing$ — пустое множество, т. е. множество, не содержащее ни одного элемента[♮].

Для отрицания принадлежности или включения эти символы перечеркиваются. Например, $a \notin A$ означает, что a не является элементом множества A. Два множества равны, $A = B$, если они содержат одни и те же элементы, т. е. если $A \subseteq B$ и $B \subseteq A$ (**аксиома экстенсиональности**).

Мы предполагаем знакомство со следующими основными операциями над множествами (называемыми в дальнейшем **булевыми операциями**). Определения и свойства этих операций кратко напоминаются в § 3.

$\cup$ — **объединение**, $A \cup B = \{x \mid x \in A \vee x \in B\}$ — множество элементов принадлежащих по крайней мере одному из множеств A или B.

$\cap$ — **пересечение**, $A \cap B = \{x \mid x \in A \ \ \& \ \ x \in B\}$ — множество элементов принадлежащих обоим множествам A и B.

$\setminus$ — **разность**, $A \setminus B = \{x \mid x \in A \ \ \& \ \ x \notin B\}$ — множество элементов принадлежащих A, но не B. Если $A \supseteq B$, называется также **дополнением** к B в A.

$\triangle$ — **симметрическая разность**, $A \triangle B = (A \cup B) \setminus (B \cap A)$ — множество элементов принадлежащих ровно одному из множеств A или B. Легко видеть, что $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

В действительности можно определить объединение, пересечение и симметрическую разность любого (не обязательно конечного) семейства множеств. Пусть $\Omega = \{A_i, i \in I\}$ есть некоторое семейство множеств, где I — множество индексов. Тогда $\cup A_i$, $i \in I$, обозначает обьединение семейства Ω, и т.д.

Два множества A и B называются **дизъюнктными** (alias **непересекающимися**), если $\cap B = \varnothing$. В этом случае их объединение обозначается также $A \coprod B$ и называется **копроизведением**, **(прямой) суммой** или **свободным объединением**.

§ 3. Коллективизация

> Взять бы этого Лебега, да за такие `доказательства` года на три в Соловки!

[♮]Этот знак, введенный А.Вейлем, представляет собой стилизованную датскую и -норвежскую букву Ø (читается ö). В некоторых старых книгах для обозначения пустого множества используется символ Λ. Однако, сегодня Λ используется для обозначения не пустого множества, а **пустого массива**, скажем, слова, не содержащего ни одной буквы.

Михаил Булгаков. *Мастер и Маргарита*

Любая конечная совокупность объектов является множеством. В то же время, отнюдь не любая бесконечная совокупность объектов может рассматриваться как множество. Некоторые совокупности, называемые **классами**, слишком велики, чтобы быть множествами. К КЛАССАМ *нельзя* ПРИМЕНЯТЬ БОЛЬШУЮ ЧАСТЬ ОБЫЧНЫХ ТЕОРЕТИКО-МНОЖЕСТВЕННЫХ КОНСТРУКЦИЙ.

Через $\{a, b, c, \dots\}$ обозначается *класс* с элементами a, b, c, ... Большинство так называемых `доказательств` — и многие так называемые `теоремы`! — в элементарных учебниках математического анализа прямо **ошибочны**, потому, что их авторы считают, что написав $\{a, b, c, \dots\}$ они определили этим некоторое *множество*.

Например, знаменитое `доказательство` того, что каждое бесконечное подмножество X содержит счетное подмножество, выглядит примерно так. Множество X бесконечно и, значит, непусто, так что можно выбрать $x_1 \in X$. Множество $X \setminus \{x_1\}$ все еще бесконечно и, значит непусто, так что можно выбрать $x_2 \in X \setminus \{x_1\}$. Множество $X \setminus \{x_1, x_2\}$ все еще бесконечно .... Таким образом, X содержит счетное подмножество $\{x_1, x_2, x_3, \dots\}$.

Это замечательно простое `доказательство`, доступное пониманию не только студентов, но даже некоторых авторов учебников. ЕДИНСТВЕННЫЙ МЕЛКИЙ ДЕФЕКТ ЭТОГО `доказательства` СОСТОИТ В ТОМ, ЧТО ОНО НЕ ТОЛЬКО БЕЗНАДЕЖНО НЕПРАВИЛЬНО, НО И ГРУБО ОШИБОЧНО, А ДОКАЗЫВАЕМЫЙ ФАКТ ВООБЩЕ НЕ ИМЕЕТ МЕСТА в теории множеств без аксиомы выбора. Разумеется, ошибка состоит именно в том, что $\{x_1, x_2, x_3, \dots\}$ совершенно не обязано быть множеством — тот факт, что оно является множеством, как раз и эквивалентен одной из форм счетной аксиомы выбора **CC**. Таким образом, *с использованием* аксиомы выбора слегка извернувшись счетное подмножество *все-таки* удается построить. Конечно, правильная конструкция раз в пять длиннее, чем приведенное выше ошибочное `доказательство`.

В настоящей книге я стараюсь уклоняться от обсуждения подобных теоретико-множественных деталей, но, с другой стороны, стремлюсь избежать заведомого вранья. К счастью, *в отсутствие* аксиомы выбора **ZF8** мне *редко* приходится использовать ошеломительные утверждения вроде того, что объединение счетного множества счетных множеств счетно. С другой стороны, особо `персеверантный` читатель может проследить, что ни одно из сформулированных в основном тексте этой книги утверждений не зависит от аксиомы регулярности **ZF9**.

Часто подмножества данного множества выделяются при помощи **предикатов** (alias `условий` или `свойств`). Пусть P какой-то предикат, выражающий свойство элементов: $P(x)$, если x обладает требуемым свойством и $\neg P(x)$, в противном случае. Предположим, что A является множеством. Тогда $\{x \in A \mid P(x)\}$ обозначает **множество** тех элементов из A, которые обладают свойством P. Например, $\mathbb{N} = \{n \in \mathbb{Z} \mid n > 0\}$ есть множество натуральных чисел, а $2\mathbb{Z} = \{n \in \mathbb{Z} \mid 2|n\}$ есть множество всех четных целых чисел.

Предостережение. Некоторые беспринципные авторы используют слабоумное обозначение $\{x \mid P(x)\}$. Однако следует иметь в виду, что это обозначение относится к области журнализма, а не математики и не имеет никакого смысла, до тех пор, пока не доказано, что предикат P является **коллективизирующим**, т. е. действительно определяет некоторое множество. Например, предикат $P(x) = (x \in A \vee x \in B)$ является коллективизирующим по аксиоме **ZF4**, а предикат $P(x) = (x \subseteq A)$ является коллективизирующим по аксиоме **ZF7**, поэтому $\{x \mid x \in A \vee x \in B\}$ и $\{x \mid x \subseteq A\}$ определяют множества. С другой стороны известные парадоксы Кантора и Рассела утверждают, что $\{x \mid \texttt{True}\}$ и $\{x \mid x \notin x\}$ не определяют множеств — иными словами, предикаты $P(x) = \texttt{True}$ и $P(x) = (x \notin x)$ **не являются** коллективизирующими. В то же время, $\{x \mid \texttt{False}\}$ и $\{x \mid x \in x\}$ определяют пустое множество (по аксиоме **ZF9**). Начинающему, пока он не приобретет *полного автоматизма* в определении того, какие свойства являются коллективизирующими, а какие нет, следует вообще избегать запись $\{x \mid P(x)\}$.

§ 4. Группировка и скобки

Следует отличать фигурные скобки $\{,\}$ (braces) от круглых скобок $(,)$ (parenthesis), квадратных скобок $[,]$ (brackets), ломаных скобок $\langle,\rangle$ (angle brackets) и других видов скобок, двойных скобок, и т.д., которые используются в нескольких совершенно различных смыслах, определяемых из контекста.

Круглые скобки используются в первую очередь для **группировки**, т. е. для обозначения последовательности выполнения алгебраических операций: $(x + y) + z = x + (y + z)$. В отличие от школьной алгебры, мы **никогда** не используем для группировки квадратные и фигурные скобки. Для лучшей читаемости формул используются круглые скобки разных кеглей: $(,)$, $\big(,\big)$, $\Big(,\Big)$, ...

1. Множества, наборы, тупели. Другой важнейшей функци-

ей круглых скобок является обозначение **тупелей**♮. Так, например, (a,b,c) обозначает упорядоченную тройку с компонентами a,b,c. Напомним, что, в отличие от множеств, порядок и кратность компонент тупеля существенны! Так, $(a,b,c)\neq(c,a,b)$ и $(a,a,b)\neq(a,b)$, в то время, как $\{a,b,c\}=\{c,a,b\}$ и $\{a,a,b\}=\{a,b\}$. Кроме того, в алгебре широко используется понятие **набора**♮, промежуточное между множеством и тупелем: в наборе существенны кратности компонент, но не их порядок. Наборы обычно† обозначаются квадратными скобками, таким образом $[a,a,b]\neq[a,b,b]$, но $[a,a,b]=[b,a,a]$.

2. Другие функции скобок. Кроме группировки и записи тупелей **круглые скобки** иногда/обыкновенно/всегда используются для выражения многих других понятий, в частности, для обозначения

- аргумента/ов отображения: $f(x)$, $f(x,y)$,
- присоединения рациональных переменных: $K(x,y)$,
- идеала коммутативного кольца♭: $(x_1,\dots,x_m)$,
- скалярного произведения: (u,v),
- антикоммутатора♭: $(x,y)=(xy+yx)/2$,
- интервала частично упорядоченного множества:

$$(x,y)=\{z\in X\mid x<z<y\},$$

- наибольшего общего делителя♭: (m,n).

Квадратные скобки передают, в частности,

- присоединения полиномиальных переменных: $K[x,y]$,
- мультипликативный/групповой коммутатор: $[x,y]=xyx^{-1}y^{-1}$,
- скобку Ли или аддитивный/кольцевой коммутатор: $[x,y]=xy-yx$,
- отрезок частично упорядоченного множества: $[x,y]=\{z\in X\mid x\leq z\leq y\}$,

---

♮**Тупелем** называется упорядоченная n-ка с неопределенным n. В различных учебных и программистских книгах тупели называются также **списками**, **кортежами**, **массивами**, **векторами** и т.д.

♮Специалисты по комбинаторике обычно говорят о **мультимножествах**.

†В языке `Pascal` и книгах Вирта квадратные скобки используются для множеств, так как в фигурные скобки заключаются комментарии к программам. С другой стороны в языке `Maple` квадратные скобки используются для списков.

♭Мы предпочитаем писать $Rx_1+\ldots+Rx_n$.

♭В настоящей книге мы используем обозначение $x\circ y$.

♭В настоящей книге мы используем обозначение $\gcd(m,n)$.

• наименьшего общего кратного[♭]: $[m, n]$,

• целую часть числа[♭]: $[x]$.

Ломаные скобки передают, в частности,

• значение спаривания: $\langle x, y\rangle$ или $\langle x|y\rangle$,

• линейную оболочку векторов: $\langle u_1, \dots, u_n\rangle$,

• подгруппу, порожденную системой элементов: $\langle u_1, \dots, u_n\rangle$.

• присоединение некоммутирующих переменных: $K\langle x, y\rangle$,

§ 5. Произведение и копроизведение

Еще одним основным понятием теории множеств является понятие **упорядоченной n-ки** $(x_1, \dots, x_n)$. В тех случаях, когда мы не хотим явно упоминать длину n — например, при $n = k$ — упорядоченная n-ка называется **тупелем**. Основное свойство тупелей состоит в следующем:

Если $(x_1, \dots, x_m) = (y_1, \dots, y_n)$, то $m = n$ и $x_i = y_i$ для всех $i = 1, \dots, n$.

Это свойство можно либо вывести из аксиом теории **ZFC** (если проинтерпретировать тупели в терминах стандартной теории множеств, скажем, в духе Винера—Куратовского!), либо просто принять за аксиому, как это делают Бурбаки. В частности это свойство гарантирует, что длина тупеля определена однозначно. При $n = 0$ имеется ровно один тупель, а именно **упорядоченная нулька** (), часто обозначаемая также Λ. Заметим, что это не греческая буква `лямбда`, а просто перевернутая буква `V` — первая буква слова `vuoto`, `void`. Все тупели небольшой длины имеют общеупотребительные названия, греющие сердце энтузиастов греко-римской борьбы:

• так, упорядоченная пара (y, z) называется просто **дубль** или **дупель** (`double`, `duple`, `Doppel`),

• упорядоченная тройка (x, y, z) — **трипель** (`Tripel`, `triplo`, `triple`),

• упорядоченная четверка (w, x, y, z) — **квадрупель** (`Quadrupel`, `quadruplo`, `quadruple`),

• упорядоченная пятерка (v, w, x, y, z) — **квинтупель** (`Quintupel`, `quintuple`),

---

[♭]В настоящей книге мы используем обозначение $\mathrm{lcm}(m, n)$.

[♭]Это обозначение следует признать устаревшим, в современных текстах используется обозначение $\lfloor x\rfloor$.

• упорядоченная шестерка (u, v, w, x, y, z) — **секступель** (`Sechstupel`*, `sextuple`),

• упорядоченная семерка (t, u, v, w, x, y, z) — **септупель** (`septuple`),

• упорядоченная восьмерка (s, t, u, v, w, x, y, z) — **октупель** (`octuple`),

• упорядоченная девятка $(r, s, t, u, v, w, x, y, z)$ — **нонупель** (`nonuple`),

• упорядоченная десятка $(q, r, s, t, u, v, w, x, y, z)$ — **декупель** (`decuple`),

и т.д.

Пусть теперь A и B — любые множества. Тогда множества упорядоченных пар $A' = \{(x, 1) \mid x \in A\}$ и $B' = \{(y, 2) \mid y \in B\}$ дизъюнктны. Объединение $A' \cup B'$ по-прежнему называется **свободным объединением** alias **копроизведением** множеств A и B и обозначается $A \coprod B$. Эта конструкция легко обобщается на случай любого семейства $\Omega = \{A_i, i \in I\}$, в этом случае копроизведение обозначается обычно $\coprod A_i$, $i \in I$.

§ 6. Отображения

Отображение $f : X \longrightarrow Y$ сопоставляет каждому элементу x множества X единственный элемент y множества Y, обозначаемый обычно $f(x)$ и называемый **образом** элемента x под действием f. Равенство $y = f(x)$ записывается также в виде $f : x \mapsto y$ и читается, например, так: x **отображает** x **в** y или f **переводит** x **в** y.

Множество X называется **областью определения** отображения $f : X \longrightarrow Y$ и обозначается $D(f)$ (от английского `domain`), а множество Y называется **областью значений** отображения f и обозначается $R(f)$ (от английского `range`). В последнее время получает все большее распространение альтернативная терминология, пришедшая из теории категорий (см. § 14), когда $D(f)$ называется просто **областью** отображения f, а $R(f)$ **кообластью**. Говорят также, что f действует из X в Y. Напомним, что $D(f)$ и $R(f)$ входят в определение отображения f. Иными словами, два отображения f и g называются **равными**, если и только если

1) их области совпадают, $D(f) = D(g) = X$,

2) их кообласти совпадают, $R(f) = R(g) = Y$,

---

*Только наиболее стойкие латинисты используют альтернативную орфографию `Sextupel`. Но тогда, конечно, `reich durch Sechs`.

3) для любого $x \in X$ выполнено равенство $f(x) = g(x)$.

?. Образы и прообразы. Пусть $f : X \longrightarrow Y$ и $A \subseteq X$. Тогда $f(A) = \{f(x) \mid x \in A\}$ называется **образом** множества A относительно (или под действием) отображения f. Образ $f(X)$ области $X = D(f)$ под действием f обозначается обычно $\mathrm{Im}(f)$ (от английского `image`) и называется образом отображения f. Иными словами, $\mathrm{Im}(f)$ – это множество таких $y \in Y$, для которых существует такое $x \in X$, что $f(x) = y$. Вообще говоря, для $y \in \mathrm{Im}(f)$ может существовать много x с этим свойством. Любой $x \in X$ такой, что $f(x) = y$ называется **прообразом** y (alias **обратным образом** y, сравни определение обратной функции ниже и обратного отношения в § 3). Множество всех прообразов некоторого $y \in Y$ обозначается $f^{-1}(y)$ и называется **полным прообразом** элемента Y (а в геометрическом контексте **слоем** f над y или **множеством уровня** f, отвечающим значению y). Разумеется, если $y \notin \mathrm{Im}(f)$, то $f^{-1}(y) = \varnothing$. Вообще, для любого подмножества $B \subseteq Y$ его **полный прообраз** $f^{-1}(B)$ определяется как $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. Ясно, что $f^{-1}(B) = \cup f^{-1}(y)$, $y \in B$.

?. Функции нескольких переменных. Предположим, теперь, что $X \subseteq X_1 \times \ldots \times X_n$. В этом случае значение $f((x_1, \ldots, x_n))$ отображения а на n-ке $(x_1, \ldots, x_n)$ обычно обозначается просто $f(x_1, \ldots, x_n)$ и f рассматривается как `функция` n `аргументов` (или n `переменных`).

§ 7. Сюръекции, инъекции, биекции

?. Сюръекции и инъекции. Если $\mathrm{Im}(f) = Y$, то отображение $f : X \longrightarrow Y$ называется **сюръективным** В этом случае говорят также, что f отображение **на** (вместо обычного `в`). Если же полный прообраз $f^{-1}(y)$ каждой точки $y \in Y$ содержит не более одного элемента, то отображение f называется **инъективным**. Иными словами, отображение f инъективно, если для любых $x_1, x_2 \in X$ равенство $f(x_1) = f(x_2)$ влечет равенство $x_1 = x_2$. Слова **сюръекция** и **инъекция** латинского происхождения и означают, соответственно, `наложение` и `вложение`. Однако термин вложение обычно применяют только к ситуации, когда $X \subseteq Y$, причем отображение а переводит каждый x в себя. Вложение X в себя: $X \longrightarrow Y$, $x \mapsto x$, называется **тождественным** (alias единичным) отображением X в себя и обозначается $\mathrm{id} = \mathrm{id}_X$ (от английского `identical`) или просто 1_X. Иногда для обозначения того, что f сюръекция используется специальная стрелка $f : X \twoheadrightarrow Y$, а для обозначения того, что а инъекция — стрелка $f : X \rightarrowtail Y$.

?. Биекции и обратное отображение. Отображение, $f : X \longrightarrow Y$, которое как инъективно, так и сюръективно, называется **биективным** (alias **изоморфизмом**) или **взаимно однозначным**. Множества инъективных, сюръективных и биективных отображений из X в Y обозначаются через $\mathrm{Inj}(X, Y)$, $\mathrm{Surj}(X, Y)$ и $\mathrm{Bij}(X, Y)$ соответственно. Это означает, что для любого $y \in Y$ существует единственный $x \in X$ такой, что $f(x) = y$. Если существует биекция из X в Y, то говорят, что между элементами X и Y можно установить **взаимно-однозначное соответствие**. Биективное отображение X на себя называется обычно **перестановкой** множества X, этот термин особенно употребим в случае, когда X конечно. С точки же зрения теории категорий биективное отображение X на себя называется **автоморфизмом**.Множество всех биективных отображений X на себя часто обозначается $S(X)$ или S_X (подробнее об этом см. § 9). Самым важным свойством биективных отображений является то, что они обратимы. Иначе говоря, в этом случае сопоставление $y \mapsto f^{-1}(y)$ задает биективное отображение $f^{-1} : Y \longrightarrow X$, называемое отображением, **обратным** к f, см. ниже. При этом $(f^{-1})^{-1} = f$, так что в действительности f и f^{-1} совершенно равноправны. Для обозначения биекций иногда используется специальная стрелка, подчеркивающая симметрию X и Y: $X \longleftrightarrow Y$.

§ 8. Композиция отображений

Два отображения f и g такие, что $R(f) = D(g)$ можно **скомпонировать**. Точнее, пусть $f : X \longrightarrow Y$ и $g : Y \longrightarrow Z$ суть два отображения, область значений первого из которых совпадает с областью определения второго. Тогда их **композиция** $g \circ f : X \longrightarrow Z$ задается посредством равенства $(g \circ f)(x) = g(f(x))$, для любого $x \in X$ ($g \circ f$ читается как 'композиция f и g' или 'g кружочек f'). Обратите внимание на порядок факторов: отображение f, действующее первым, записывается вторым. Это связано с тем, что мы пишем функцию слева от аргумента, как $f(x)$. Разумеется, если бы мы использовали обозначение $(x)f$, то и композиция f и g записывалась бы как $f \circ g$, по формуле $(x)(f \circ g) = ((x)f)g$. Композиция двух отображений часто называется также их **суперпозицией** или **произведением**. Самым важным свойством композиции отображений является ее ассоциативность.

Лемма 1. *Если одно из выражений $(h \circ g) \circ f$ и $h \circ (g \circ f)$ определено, то определено и второе и при этом $(h \circ g) \circ f = h \circ (g \circ f)$.*

Доказательство. Пусть, например, определено первое из этих отоб-

ражений. По определению это означает, что $D(h) = R(g)$ и $D(g) = D(h \circ g) = R(f)$. Но тогда, конечно, определено и $g \circ f$ и, кроме того $R(g \circ f) = R(g) = D(h)$, так что второе отображение действительно определено. Равенство же этих отображений доказывается следующей выкладкой:

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = (h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x).$$

См. § 7 по поводу некоторых следствий из ассоциативности. Композиция отображений весьма далека от коммутативности, т. е. для двух отображений f и g, вообще говоря, $f \circ g \neq g \circ f$. Это ясно хотя бы из того, что одна из частей равенства $f \circ g = g \circ f$ может быть определена без того, чтобы была определена другая, т. е. из равенства $R(f) = D(g)$ отнюдь не следует, что $R(g) = D(f)$. Но даже если как $f \circ g$, так и $g \circ f$ обе определены, они могут быть совершенно различны. Например, если $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ задаются как $f(n) = n^2$ и $g(n) = n + 1$, то $(g \circ f)(n) = n^2 + 1$, в то время как $(f \circ g)(n) = (n + 1)^2$, так что для любого натурального n значения функций $f \circ g$ и $g \circ f$ различны.

Тождественные отображения действительно ведут себя как нейтральные элементы для композиции функций, но отсутствие коммутативности накладывает свой отпечаток. А именно, для отображений из $\mathrm{Map}(X, Y)$ тождественное отображение id_X выступает как **правая единица**, а id_Y — как **левая единица**. Иными словами, для любого $f \in \mathrm{Map}(X, Y)$ имеем $f \circ \mathrm{id}_X = f = \mathrm{id}_Y \circ f$. По отношению к отображениям X в себя id_X является уже **двусторонней единицей**.

Пусть теперь $f \in \mathrm{Map}(X, Y)$ — любое отображение. Тогда f называется **обратимым слева**, если существует такое $g \in \mathrm{Map}(Y, X)$, что $g \circ f = \mathrm{id}_X$ (любое такое g называется **левым обратным** к f). Аналогично, f называется **обратимым справа**, если существует такое $g \in \mathrm{Map}(Y, X)$, что $f \circ g = \mathrm{id}_Y$ (любое такое g называется **правым обратным** к f). Отображение f называется **обратимым** (иногда для полной определенности говорят **двусторонне обратимым**), если оно обратимо как слева, так и справа. Следующее утверждение очевидно.

Лемма 2. *Имеют место следующие эквивалентности:*
1) f инъективно $\Longleftrightarrow$ f обратимо слева,
2) f сюръективно $\Longleftrightarrow$ f обратимо справа,
3) f биективно $\Longleftrightarrow$ f двусторонне обратимо.

Легко видеть (подробнее об этом см. § 7), что если f двусторонне обратимо, то левый и правый обратный к нему определены однозначно

и совпадают между собой. Их общее значение обозначается f^{-1} и называется отображением обратным к f. Это в точности отображение, определенное выше посредством прообразов.

§ 9. Отношения

В понятие отображения область определения X и область значений Y входят неравноправно. При этом каждому элементу $x \in X$ соответствует ровно один элемент множества Y, но элемент $y \in Y$ может не соответствовать никакому x, либо соответствовать более, чем одному x. Понятие (бинарного) отношения восстанавливает симметрию между X и Y.

1. Бинарные отношения. Пусть, как и в предыдущем параграфе, X и Y — два множества.

Определение. Бинарным отношением *между X и Y называется любое подмножество $R \subseteq X \times Y$ их декартова произведения.*

Часто говорят также о **соответствии** между элементами X и Y, задаваемым отношением R. Для записи отношений обычно используется **инфиксная** запись, так что вместо $(x, y) \in R$ пишут просто xRy и говорят, что 'x соответствует y относительно R' или что 'x находится в отношении R к y'. Множество $2^{X\times Y}$ всех бинарных отношений между X и Y обозначается также $\mathrm{Rel}(X, Y)$ (от английского `relation`). В случае $X = Y$ говорят о **бинарных отношениях на** X — отношения такого типа обычно называются **внутренними**: при этом $\mathrm{Rel}(X, X)$ часто обозначается просто $\mathrm{Rel}(X)$.

§ 10. Отношения эквивалентности

Отношения эквивалентности.

Определение. Эквивалентностью *на множестве X называется рефлексивное симметричное транзитивное бинарное отношение R.*

Мы будем обозначать эквивалентность следующим образом: $xRy \iff x \sim y$ (читается x **эквивалентно** y), но часто потребляются и другие символы: $\cong$, $\equiv$, $=$, и так далее (названия эквивалентностей, которые будут нам встречаться и, соответственно, чтения этих символов будут определяться контекстом). По определению,

a) $x \sim x$ (рефлексивность),

b) $x \sim y \Longrightarrow y \in x$ (симметричность),

c) $x \sim y \ \ \& \ \ y \sim z \Longrightarrow x \sim z$ (транзитивность).

Для каждого элемента $x \in X$ через $\overline{x}$ обозначается соответствующий **класс эквивалентности**, определяемый как множество всех $y \in X$ эквивалентных x: $\overline{x} = \{y \in X \mid y \sim x\}$. При этом сам элемент x называется **представителем** класса $\overline{x}$. Так как по определени. $\overline{x} = \overline{y} \iff x \sim y$, то $\overline{x}$ однозначно определяется любым своим представителем. Условия a) — c) могут быть переформулированы теперь следующим образом:

a) $x \in \overline{x}$;

b) $y \in \overline{x} \Longrightarrow x \in \overline{y}$;

c) $y \in \overline{x}$ & $z \in \overline{y} \Longrightarrow z \in \overline{x}$.

Напомним, что **разбиением** множества X называется его представление как дизъюнктного объединения какого-то семейства подмножеств: $X = \coprod X_i$, $i \in I$ (см. § 1). Понятие разбиения по сути совпадает с понятием эквивалентности. А именно, каждому разбиению можно сопоставить отношение эквивалентности, для которого $x \sim y$ тогда и только тогда, когда $x, y \in X_i$ для некоторого i.

Обратно, следующее предложение показывает, что каждая эквивалентность на X задает разбиение X на попарно различные классы. Для этого выберем из каждого класса X_i по одному представителю x_i, где i пробегает некоторое множество индексов I, и назовем $\{x_i, i \in I\}$ **системой представителей** эквивалентности $\sim$ (или **трансверсалью** к этой эквивалентности).

Предложение. *Множество классов эквивалентности представляет собой разбиение X. Иными словами, X представляется в виде дизъюнктного обьединения $X = \coprod X_i$, $i \in I$, различных классов.*

Доказательство. Прежде всего, заметим, что $X = \cup X_i$, $i \in I$. В самом деле, так как мы выбрали по одному x_i из каждого класса, то для любого $x \in X$ найдется x_i такой, что $x \sim x_i$, но тогда по свойству a) имеем $x \in \overline{x} = \overline{x}_i$.

Осталось заметить, что два различных класса не могут пересекаться. В самом деле, если $\overline{x} \cap \overline{y} \neq \varnothing$, то найдется $z \in \overline{x} \cap \overline{y}$, но тогда по свойству b) также $y \in \overline{z}$ и теперь по свойству c) мы можем заключить, что $y \in \overline{x}$, так что, окончательно, $\overline{y} = \overline{x}$, что и требовалось доказать.

Различные аватары следующей конструкции будут сопровождать нас на протяжении всего курса.

Определение. *Множество $X/{\sim} = \{\overline{x} \mid x \in X\}$ классов эквивалентности $\sim$ на множестве X называется* **фактор-множеством** *X по*

отношению $\sim$*, а отображение* $\mathrm{pr} : X \longrightarrow X/\sim$, $x \mapsto \overline{x}$, *называется* **канонической проекцией** X *на* $X/\sim$.

Обычный способ задания разбиений множества X состоит в следующем. Пусть нам задано отображение $f : X \longrightarrow Y$ множества X в какое-то множество Y. Введем на X следующее отношение эквивалентности $\sim$: $x \sim y \iff f(x) = f(y)$. Классы этой эквивалентности (полные прообразы точек из Y относительно отображения f) называются **слоями** отображения f и, как мы знаем, X представляется как дизъюнктное обьединение слоев $f^{-1}(y)$, $y \in \mathrm{Im}(f)$. Пусть, как обычно, $X/\sim$ обозначает множество слоев (фактор-множество X по отношению эквивалентности $\sim$. Тогда можно определить отображение $\overline{f} : X/\sim \longrightarrow Y$ полагая $\overline{f}(\overline{x}) = f(x)$. Это определение корректно, т. е. не зависит от выбора представителя x из данного класса, так как отображение постоянно на своих слоях. Отображение f включается в следующий **коммутативный треугольник**:

triangle

'Коммутативность' в этом контексте означает, x то $f = \overline{f} \circ \mathrm{pr}$ (см. § ? по поводу общего определения коммутативных диаграмм). Резюмируем получившийся результат.

§ 11. Отношения порядка

Нам будут чрезвычайно часто встречаться отношения, обобщающие отношение неравенства '$<$' и отношение включения '$\subset$'.

?. Частично упорядоченные множества.

Определение. Порядком *на множестве* X *называется рефлексивное, антисимметричное транзитивное бинарное отношение* R.

Порядок обычно обозначается следующим образом: $xRy \iff x \leq y$ (читается 'меньше или равно', 'не больше', 'предшествует', 'минорирует'). По определению,

a) $x \leq x$ (рефлексивность),

b) $x \leq y \ \ \& \ \ y \leq x \Longrightarrow x = y$ (антисимметричность),

c) $x \leq y \ \ \& \ \ y \leq z \Longrightarrow x \leq z$ (транзитивность).

Отношение R^{-1}, обратное к R, обычно записывается $x \geq y$ (читается 'больше или равно', 'не меньше', 'следует', 'мажорирует'). Таким образом, $x \geq y \iff y \leq x$. Отношение $R \setminus \Delta$ записывается $x < y$

(читается 'меньше', 'строго меньше', 'строго предшествует', 'строго минорирует'). Иными словами, $x < y \iff x \leq y \ \& \ x \neq y$. Аналогичный смысл имеет $x > y$ ('больше', 'строго больше', 'строго следует', 'строго мажорирует').

?. Линейный порядок. Часто введенное выше понятие называется **частичным порядком**, чтобы подчеркнуть, что не любые два элемента множества X сравнимы относительно $<$. При этом два элемента X и Y называются **сравнимыми**, если $x < y \vee y < x$. В противном случае X и Y называют **несравнимыми**, и пишут $x \parallel y$. Само множество X, на котором задан частичный порядок называется **частично упорядоченным множеством** или, сокращенно, **чумом** (по аналогии с `poset` от `partially ordered set`).

Определение.. *Порядок R на X называется* **линейным**, *если $R \cup R^{-1} = X \times X$, т. е., если любые два элемента сравнимы.*

Множество X, на котором задан линейный порядок, называется **линейно упорядоченным множеством** или **цепью**.

§ 12. Алгебраические операции

Алгебраическая операция (если быть совсем точным, то **внутренняя бинарная операция**) или **закон композиции** на множестве X это отображение $f : X \times X \longrightarrow X$. Обычно для алгебраических операций используется **инфиксная запись**, т. е. вместо $z = f(x, y) = z$ пишут $z = xfy$. При этом элементы x, y называются **операндами** (или **факторами**), а z – **результатом** операции.

Две наиболее часто используемые системы записи — это мультипликативная нотация и аддитивная нотация. При **мультипликативной нотации**, операция называется **умножением** и обозначается точкой $\cdot$ (TEXническое название `\cdot`), которая часто опускается. Иными словами, в этом случае пишут $z = x \cdot y$ или просто $z = xy$. Элементы x, y называются **сомножителями**, а z — **произведением**. При **аддитивной нотации**, операция называется **сложением** и обозначается плюсом $+$. Иными словами, в этом случае пишут $z = x + y$, причем элементы x, y называются **слагаемыми**, а z — **суммой**.

Операция f называется **ассоциативной**, если

$$f(f(x, y), z) = f(x, f(y, z))$$

для всех $x, y, z \in X$. В мультипликативной и аддитивной записи это тождество принимает вид $(xy)z = x(yz)$ и $(x + y) + z = x + (y + z)$,

соответственно. В дальнейшем для краткости мы обычно пользуемся мультипликативной записью. **Обобщенная ассоциативность** (allgemeine Klammerregel) утверждает, что для ассоциативной операции произведение $x_1 \dots x_n$ не зависит от расстановки скобок.

Операция называется **коммутативной**, если $f(x, y) = f(y, x)$ для всех $x, y \in X$. В аддитивной и мультипликативной записи тождество коммутативности принимает вид, $xy = yx$ или $x + y = y + x$, соответственно. Следует иметь в виду, что аддитивная запись используется *как правило*[♮] только для коммутативных операций. **Обобщенная коммутативность** утверждает, что для коммутативной ассоциативной операции произведение $x_1 \dots x_n$ не зависит ни от расстановки скобок, ни от порядка сомножителей.

Элемент $e \in X$ называется **левым нейтральным**, если $ex = x$ для всех $x \in X$ и **правым нейтральным**, если $xe = x$ для всех $x \in X$. Элемент, который одновременно является как левым, так и правым нейтральным, называется **нейтральным** элементом (иногда, эмфатически **двусторонним нейтральным**). Нейтральный элемент по умножению называется **единицей** и обычно обозначается e или 1, а нейтральный элемент по сложению называется **нулем** и обозначается 0.

Множество с ассоциативной операцией называется **полугруппой**, в зависимости от типа записи говорят о мультипликативной или аддитивной полугруппе. **Моноид** — это полугруппа с нейтральным элементом. Если операция, кроме того, коммутативна, полугруппа или моноид называются коммутативными.

Пусть X — моноид с нейтральным элементом e. Элемент $x \in X$ называется **обратимым слева**, если существует элемент $y \in X$ такой, что $yx = e$. В этом случае элемент y называется **левым обратным** к x. Аналогично, x называется **обратимым справа**, если существует элемент $z \in X$ такой, что $xz = e$, В этом случае элемент z называется **правым обратным** к x. Вообще говоря, элемент x может иметь много левых обратных или много правых обратных, однако если элемент x обратим как справа, так и слева, то $y = ye = y(xz) = (yx)z = ez = z$. Обратите внимание, что в этом вычислении использована ассоциативность операции!

Иными словами, если у элемента x существуют левый обратный y и правый обратный z, то они совпадают. Это дает нам возможность ввести следующее определение. Элемент $x \in X$ называется **обратимым**

[♮]Имеется, впрочем, и исключения: сложение ординалов и некоторые экзотические примеры.

(или эмфатически **двусторонне обратимым**), если существует такое $y \in X$, что $xy = e = yx$. В этом случае y называется **обратным** к x и обозначается x^{-1}. При аддитивной записи обратный элемент обозначается $-x$ и называется **противоположным**.

Пусть X и Y — два множества с алгебраическими операциями. Отображение $f : X \longrightarrow Y$ называется **гомоморфизмом**, если $f(xy) = f(x)f(y)$ для любых $x, y \in X$. Биективный гомоморфизм называется **изоморфизмом**.

§ 13. Мощность

1. Мощность. Два множества A и B называются **равномощными** alias **эквивалентными** alias **изоморфными**, если между их элементами можно установить взаимно-однозначное соответствие. В этом случае мы пишем $A \sim B$. **Мощность** множества A будет обозначаться через $|A|$ или $\mathrm{Card}(A)$, американские авторы иногда используют символ $\#(A)$. Мощность A либо конечна и в этом случае является неотрицательным целым числом $n \in \mathbb{Z}$, $n \geq 0$, либо бесконечна. В случае, когда $|A| < \infty$, мощность A называется также **порядком** множества A.

Обнаружение иерархии бесконечностей — одно из самых замечательных открытий XIX века. Вычисления с мощностями, называемых также **кардиналами** или **кардинальными числами**, известны как **кардинальная арифметика**. Мы будем использовать лишь две бесконечные мощности.

• Множество A называется **счетным**, если оно равномощно $\mathbb{Z}$. В этом случае мы пишем $|A| = \aleph_0$, произносится `алеф-ноль`.

• Множество A называется **континуальным**, если оно равномощно $\mathbb{R}$. Мощность континуума будет обозначаться через $\mathfrak{c}$.

Континуум-гипотеза утверждает, что $\mathfrak{c} = \aleph_1 = 2^{\aleph_0}$. Иными словами, декларируется, что никаких мощностей, промежуточных между $\aleph_0$ и $\mathfrak{c}$, не существует. Континуум-гипотеза не зависит от обычных аксиом теории множеств; ни доказать, ни опровергнуть ее невозможно. Мы не будем нуждаться в этом предположении — или в каких-то других нелепых утверждениях про бесконечные мощности.

§ 14. Аксиома выбора и лемма Куратовского—Цорна

Лемма Куратовского—Цорна. *Если каждое линейно упорядоченное подмножество множества X имеет верхнюю грань, то в X существует максимальный элемент.*

Говорят, что множество X удовлетворяет **условию максимальности** (**минимальности**), если любое его непустое подмножество содержит максимальный (минимальный) элемент. Множества с условием максимальности называются еще **нетеровыми**, а множества с условием минимальности – **артиновыми**. Несложно убедиться, что условие максимальности эквивалентно следующему условию обрыва возрастающих цепей: если $x_1 \leq x_2 \leq \ldots \leq x_n \leq \ldots$, то существует такое m, что $x_n = x_m$ для всех $n \geq m$. Аналогично, условие минимальности эквивалентно двойственному условию обрыва убывающих цепей. Лемма Куратовского—Цорна и условие максимальности будут для нас основой многих индуктивных доказательств.

Линейно упорядоченное множество, удовлетворяющее условию минимальности называется **вполне упорядоченным**. В силу линейной упорядоченности минимальный элемент обязан быть наименьшим, поэтому вполне упорядоченное множество может быть определено еще как множество, в котором любое непустое подмножество содержит наименьший элемент. Следующие утверждения являются еще двумя известными переформулировками аксиомы выбора (иногда называемыми **аксиомой полной упорядоченности** и **принципом максимальности Хаусдорфа**, соответственно).

Аппендикс 2: АБЕЛЕВЫ ГРУППЫ

В настоящем приложении мы рассматриваем абелевы группы. В действительности теория абелевых групп относится скорее к линейной алгебре, чем собственно к теории групп. Об этом свидетельствует хотя бы сама используемая в теории абелевых групп аддитивная нотация. Тем не менее, некоторые простейшие результаты теории абелевых групп — в особенности классификация конечных абелевых групп — постоянно используются собственно в теории групп. Разумеется, теорема о строении конечных абелевых групп является частным случаем теоремы о строении конечно порожденных абелевых групп, которая, в свою очередь, является очень частным случаем теоремы о строении модулей над кольцом главных идеалов, которая, в свою очередь ... — и далее по тексту. Однако, нам хочется использовать эту теорему уже сейчас, до и независимо от общей теории.

Поэтому в настоящем приложении мы дадим непосредственное доказательство следующей теоремы, которая называется также **основной теоремой о конечно порожденных абелевых группах** или, коротко, `Fundamentalsatz`.

Теорема Фробениуса—Штикельбергера. *Конечно порожденная абелева группа G представляется в виде прямой суммы бесконечных циклических и примарных циклических групп. При этом типы слагаемых определены однозначно.*

Эта теорема была опубликована в 1879 году Фробениусом и Штикельбергером [245], причем их оригинальная статья занимала 46 страниц *большого формата*! Современные доказательства обычно несколько короче. Мы приведем два доказательства этой теоремы, первое из которых основано на отдельном рассмотрении конечных групп и групп без кручения, а второе — на изучении подгрупп свободной абелевой группы.

Кроме того, здесь мы обсудим класс делимых абелевых групп и, в частности, докажем теорему классификации делимых групп. Этот класс представляет большой интерес сам по себе, так как, во-первых, он двойственен классу свободных абелевых групп и, во-вторых, поз-

воляет строить много удивительных примеров. Но подлинной мотивировкой для нас является, конечно, то, что делимые абелевы группы постоянно возникают в приложениях. Основные результаты об этом классе многократно используются в книгах III и IV при обсуждении мультипликативных групп полей и векторных пространств над полями характеристики 0.

§ 1. Линейная независимость

Пусть $x_1, \ldots, x_n$ — элементы абелевой группы G. Рассмотрим отображение $\mathbb{Z}^n \longrightarrow G$, сопоставляющее набору $(m_1, \ldots, m_n)$ целых чисел **линейную комбинацию** $m_1x_1 + \ldots + m_nx_n \in G$ элементов $x_1, \ldots, x_n$ с коэффициентами $(m_1, \ldots, m_n)$. Линейная комбинация называется **тривиальной**, если $m_1 = \ldots = m_n = 0$. Понятие линейной комбинации легко обобщается и на случай бесконечного семейства элементов. Если $\{x_i\}$, $i \in I$, — такое семейство, то линейной комбинацией семейства $\{x_i\}$ называется любая сумма вида $\sum m_i x_i$, где $m_i \in \mathbb{Z}$, причем почти все m_i равны 0. Иными словами, линейная комбинация бесконечного семейства — это то же самое, что линейная комбинация какого-то его конечного подсемейства (**принцип компактности** для линейных комбинаций).

Элементы $x_1, \ldots, x_n$ называются **линейно независимыми**, если все нетривиальные линейные комбинации $x_1, \ldots, x_n$ отличны от 0, т. е. если $m_1x_1 + \ldots + m_nx_n = 0$ влечет $m_1 = \ldots = m_n = 0$. Иными словами, элементы $x_1, \ldots, x_n$ линейно независимы, если задаваемое ими отображение $\mathbb{Z}^n \longrightarrow G$ инъективно. В противном случае элементы $x_1, \ldots, x_n$ называются **линейно зависимыми**. Приведем простейшие примеры линейно независимых систем:

• Пустая система элементов линейно независима;

• Любая система, содержащая 0 линейно зависима;

• Система, состоящая из одного элемента $x \in G$, в том и только том случае линейно независима, когда x элемент бесконечного порядка;

• Элементы $(a, b), (c, d) \in \mathbb{Z}^2$ в том и только том случае линейно независимы, когда $\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$;

• *Любые* два элемента $x, y \in \mathbb{Q}$ линейно зависимы, а именно, если $x = k/l$, $y = m/n$, где $k, l, m, n \in \mathbb{Z}$, $l, n \neq 0$, то $mlx - kny = 0$;

• Более общо, два ненулевых элемента $x, y \in \mathbb{R}$ в том и только том случае линейно независимы, когда $x/y \notin \mathbb{Q}$.

Предостережение. Приведенное нами определение линейной независимости над $\mathbb{Z}$ является не единственным используемым в теории абелевых групп. Дело в том, что согласно этому определению в периодических группах любая непустая система векторов линейно зависима. Поэтому самые оголтелые адепты теории абелевых групп пользуются не приведенным выше определением, а определением, которое дал в 1950 году Селе [246]: элементы $x_1, \ldots, x_n$ называются **линейно независимыми в смысле Селе**, если из того, что $m_1x_1 + \ldots + m_nx_n \in G$ следует, что $m_1x_1 = \ldots = m_nx_n = 0$. Иными словами, элементы $x_1, \ldots, x_n$ в том и только том случае линейно независимы в смысле Селе, когда $\langle x_1, \ldots, x_n\rangle = \langle x_1\rangle \oplus \ldots \oplus \langle x_n\rangle$. В группах без кручения определение Селе совпадает с обычным, а в элементарных абелевых p-группах — с линейной независимостью над $\mathbb{F}_p$.

Понятие линейной независимости без труда обобщается на любое бесконечное семейство векторов $\{x_i\}$, $i \in I$. Для этого вспомним, что по определению линейная комбинация бесконечного семейства — это линейная комбинация какого-то его конечного подсемейства. Это значит, что если какая-то нетривиальная линейная комбинация семейства $\{x_i\}$ равна 0, то в $\{x_i\}$ найдется какое-то **конечное** подсемейство элементов $x_1, \ldots, x_n$ и его нетривиальная линейная комбинация, равная 0. Тем самым, в любом линейно зависимом семействе найдется конечное линейно зависимое подсемейство. Таким образом, мы можем сформулировать **принцип компактности линейной независимости**: семейство, **любое** конечное подсемейство которого линейно независимо, само будет линейно независимым.

§ 2. Свободные абелевы группы

Определение. *Абелева группа F называется* **свободной**, *если в ней существует линейно независимая система образующих.*

Линейно независимая система образующих группы F называется **базисом** этой группы. Таким образом, свободная группа это в точности абелева группа, в которой существует базис. Если $x_1, \ldots, x_n$ — базис группы F, то отображение $\mathbb{Z}^n \longrightarrow F$, $(m_1, \ldots, m_n) \mapsto m_1x_1 + \ldots + m_nx_n$, биективно. Обратно, элементы $e_1, \ldots, e_n$ образуют базис группы $\mathbb{Z}^n$. Таким образом, группы $\mathbb{Z}^n$ являются свободными абелевыми группами и обратно любая конечно порожденная свободная абелева группа изоморфна какой-то из групп $\mathbb{Z}^n$. Сформулированное в следующей теореме свойство обычно коротко называется **IBN = инвариантность базисного числа***.

*__Лингвистическое упражнение:__ напечатайте IBN по-русски. **Варианты ответа:** ИБЧ, ШИТ.

Теорема. *Любые два базиса свободной абелевой группы F содержат одинаковое количество элементов.*

Мы дадим два доказательства этой теоремы, вначале для групп конечного ранга, и чуть позже в общем случае.

Доказательство. В самом деле, если $x_1, \dots, x_n$ — базис группы F, а $y_1, \dots, y_m$ — любая система ее элементов, то каждый из элементов y_i может быть выражен как линейная комбинация $x_1, \dots, x_n$. Таким образом,

$$(y_1, \dots, y_m) = (x_1, \dots, x_n)a$$

для некоторой матрицы $a \in M(n, m, \mathbb{Z})$. Если $y_1, \dots, y_m$ в свою очередь является базисом группы F, то по той же причине

$$(x_1, \dots, x_n) = (y_1, \dots, y_m)b$$

для некоторой матрицы $b \in M(m, n, \mathbb{Z})$. Таким образом,

$$(x_1, \dots, x_n) = (x_1, \dots, x_n)ab, \qquad (y_1, \dots, y_m) = (y_1, \dots, y_m)ba.$$

Так как $x_1, \dots, x_n$ и $y_1, \dots, y_m$ базисы, то

$$ab = e \in \mathrm{GL}(n, \mathbb{Z}), \qquad ba = e \in \mathrm{GL}(m, \mathbb{Z}).$$

Однако над кольцом $\mathbb{Z}$ не существует неквадратных двусторонне обратимых матриц.

Количество элементов в базисе свободной группы называется ее **рангом**. Выше мы говорили только о свободных абелевых группах конечного ранга. Однако с учетом принципа компактности все эти определения легко обобщаются и на случай групп бесконечного ранга. Как и в случае конечного ранга семейство $\{x_i\}$, $i \in I$, называется базисом группы F если оно линейно независимо. Это значит, что группа каждый ненулевой элемент группы F *единственным образом* представляется в виде $g = m_{i_1}x_{i_1} + \ldots + m_{i_s}x_{i_s}$, где все m_i ненулевые, а все i_j попарно различны. Таким образом, свободная абелева группа с базисом $\{x_i\}$, $i \in I$, это в точности *прямая сумма* групп $\mathbb{Z}$ в количестве $|I|$ штук. Мы будем обозначать эту группу через $F = \mathbb{Z}^I$.

Еще одно доказательство. Итак, пусть $\mathbb{Z}^I$ и $\mathbb{Z}^J$ — две любых свободных абелевых группы. Мы хотим показать, что $F = \mathbb{Z}^I$ в том и только том случае изоморфна $\mathbb{Z}^J$, когда $|I| = |J|$. Для этого достаточно заметить, что для любого простого числа $p \in \mathbb{P}$ фактор-группа

$F/pF \cong (\mathbb{Z}/p\mathbb{Z})^I$ является векторным пространством размерности $|I|$ над полем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Иными словами, мы утверждаем, что если x_i, $i \in I$, базис F, то $x_i + pF$, $i \in I$, — базис F/pF. В самом деле, очевидно, что $x_i + pF$, $i \in I$, — система образующих, нам нужно только показать, что она линейной независима над $\mathbb{F}_p$. В самом деле, пусть $\sum m_i(x_i + pF) = 0$, где $0 \leq m_i < p$, — линейная зависимость над $\mathbb{F}_p$. Возвращаясь в F эту зависимость можно переписать в виде $\sum m_i x_i \in pF$, в силу линейной независимости x_i над $\mathbb{Z}$ это означает, что все m_i равны 0. Так как два векторных пространства над полем в том и только том случае изоморфны, когда они имеют одинаковую размерность, это и значит, что $|I| = |J|$.

Многие начинающие не особенно отчетливо понимают разницу между прямой суммой и прямым произведением. Для конечного количества сомножителей/слагаемых это действительно одно и то же. Но следующий простой результат [247], [248] должен развеять всякие неуместные иллюзии по поводу общего случая. Обратите внимание, что приводимое ниже доказательство самым существенным образом опирается на *второе* доказательство инвариантности базисного числа!

Теорема Бэра—Шпекера. *Прямое произведение P бесконечного семейства бесконечных циклических групп не является свободной группой.*

Доказательство. В простейшей форме теорема о подгруппах (Untergruppensatz) утверждает, что все подгруппы свободной группы свободны. Поэтому нам достаточно построить несвободную подгруппу в $P = \prod_{i\in\mathbb{N}} \langle g_i\rangle$. Зафиксируем простое число $p \in \mathbb{P}$ и рассмотрим подгруппу $G \leq P$, состоящую из всех элементов $(n_1 g_1, n_2 g_2, \dots)$ таких, что и любого $m \in \mathbb{N}$ все n_i, кроме конечного числа, делятся на p^m. Ясно, что G содержит $F = \bigoplus_{i\in\mathbb{N}} \langle g_i\rangle$ и имеет мощность континуума. Если бы G была свободна, то G/pG имела бы мощность континуума. Но так как всякий смежный класс G по pG содержит представитель из F, то G/pG счетна.

Заметим, впрочем, что из теоремы Понтрягина [128] вытекает, что все *счетные* подгруппы группы P свободны. С другой стороны, легко доказать, что сама группа P настолько далека от свободы, насколько это можно представить, в любом ее задании образующими и соотношениями множество соотношений несчетно.

§ 3. Универсальное свойство свободных абелевых групп

Свободные абелевы группы обладают в классе абелевых групп следующим универсальным свойством, которое в более продвинутых источниках принимается за *определение* свободных абелевых групп.

Универсальное свойство. *Если $x_1, \dots, x_n$ — базис свободной абелевой группы F, а $g_1, \dots, g_n$ — произвольная система элементов абелевой группы G. Тогда существует единственный гомоморфизм $\varphi : F \longrightarrow G$ такой, что $\varphi(x_i) = g_i$.*

Доказательство. Так как $x_1, \ldots, x_n$ — базис F, то любой элемент $x \in F$ можно *единственным образом* выразить в виде $x = m_1x_1 + \ldots + m_nx_n$ для подходящих $m_1, \ldots, m_n \in \mathbb{Z}$. Таким образом, формула $\varphi(x) = m_1g_1 + \ldots + m_ng_n$ корректно определяет отображение из F в G такое, что $\varphi(x_i) = g_i$. Из абелевости группы G сразу вытекает, что φ гомоморфизм, что доказывает существование. Для доказательства единственности заметим, что если $\psi : F \longrightarrow G$ — произвольный гомоморфизм такой, что $\psi(x_i) = g_i$, то

$$\begin{aligned}\psi(x) = \psi(m_1x_1 + \ldots + m_nx_n) = \\ = m_1\psi(x_1) + \ldots + m_n\psi(x_n) = m_1g_1 + \ldots + m_ng_n = \varphi(x).\end{aligned}$$

Дадим еще одну формулировку универсального свойства. В действительности именно получающийся при этом класс проективных модулей, а вовсе не класс свободных модулей является естественным субъектом линейной алгебры над кольцами!!! Разница здесь такая же, как между тривиальными и локально тривиальными векторными расслоениями в топологии. Однако для абелевых групп мы получаем просто еще одно определение свободных абелевых групп.

Назовем группу F **проективной**, если для любой группы G любой гомоморфизм $\varphi : F \longrightarrow H$ группы F на фактор-группу H группы G поднимается в G. Иными словами, существует такое $\psi : F \longrightarrow G$, что $\varphi = \pi \circ \psi$, где через $\pi : G \longrightarrow H$ обозначена каноническая проекция G на H:

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle \varphi} & & \\ G & \xrightarrow[\pi]{} & H & \longrightarrow & 0 \end{array}$$

Для произвольного кольца проективные модули определяются аналогично, при этом как будет видно из приводимого ниже доказательства, проективные модули — это в точности прямые слагаемые свободных. Легко привести примеры колец, над которыми не каждый проективный модуль свободен. Однако как мы докажем в следующем параграфе подгруппы свободных абелевых групп свободны, так что для абелевых групп никаких неожиданностей не возникает. Следующий результат был доказан Маклейном в 1950 году [249] в знаменитой статье, где он сформулировал двойственность между свободными и делимыми абелевыми группами.

Теорема Маклейна. *Абелева группа F в том и только том случае проективна, когда она свободна.*

Доказательство. То, что любая свободная абелева группа проективна сразу вытекает из универсального свойства. В самом деле, пусть x_i, $i \in I$, — базис F. Выберем в группе G какие-то прообразы g_i, $i \in I$, элементов $\varphi(x_i)$, так что $\pi(g_i) = \varphi(x_i)$. Универсальное свойство означает, что существует единственный гомоморфизм $\psi : F \longrightarrow G$, $x_i \mapsto g_i$. По построению $\pi(\psi(x_i)) = \pi(g_i) = \varphi(x_i)$, так что образы всех x_i под действием $\pi \circ \psi$ и φ совпадают.

Обратно, пусть F — проективная группа, а $\pi : G \longrightarrow F$ какой-то эпиморфизм свободной абелевой группы G на F. Пусть $\varphi = \mathrm{id}_F : F \longrightarrow F$ — тождественный гомоморфизм. По определению проективности существует гомоморфизм $\psi : F \longrightarrow G$ такой, что $\pi \circ \psi = \mathrm{id}_F$. Следовательно, ψ — изоморфизм F на прямое слагаемое в G, а по теореме о подгруппах каждая подгруппа свободной абелевой группы свободна.

§ 4. Подгруппы свободной абелевой группы, 1st installment: свободу подгруппам

Классификация конечно порожденных абелевых групп теснейшим образом связана с описанием подгрупп в свободных абелевых группах конечного ранга. Первое ключевое наблюдение состоит в том, что все такие подгруппы свободны. Начнем доказательство этого факта со следующего ключевого свойства свободных абелевых групп, которое представляет огромный самостоятельный интерес и будет использоваться в дальнейшем по нескольким разным поводам. Следующий результат сразу вытекает из того, что свободная группа проективна, но для удобства начинающего мы еще раз явно повторим *рассуждение*, фигурирующее в доказательстве проективности, тем более, что оно совсем короткое.

Теорема. *Если $\varphi : G \longrightarrow F$ эпиморфизм абелевой группы G на свободную абелеву группу F. Тогда $G \cong \mathrm{Ker}(\varphi) \oplus F$.*

Доказательство. Выберем базис $x_1, \ldots, x_n$ группы F и возьмем произвольные прообразы $g_1, \ldots, g_n$ этих элементов в G, $\varphi(g_i) = x_i$. Согласно универсальному свойству свободной абелевой группы существует единственный гомоморфизм $\psi : F \longrightarrow G$, переводящий x_i в g_i. Так как $(\varphi \circ \psi)(x_i) = x_i$ для всех $i = 1, \ldots, n$, то $\varphi \circ \psi = \mathrm{id}$. Тем самым, $H = \psi(F) \leq G$, является изоморфной F свободной абелевой подгруппой в G, с базисом $g_1, \ldots, g_n$. Так как $\varphi|_H$ сюръективно, то

для любого $g \in G$ найдется такое $h \in H$, что $\varphi(g) = \varphi(h)$. Тем самым, $\varphi(g-h) = 0$ и, значит, $G = \mathrm{Ker}(\varphi)+H$. С другой стороны, так как $\varphi|_H$ инъективно, то $\mathrm{Ker}(\varphi) \cap \psi(F) = 0$ и, окончательно, $G = \mathrm{Ker}(\varphi) + H$.

Теперь мы готовы доказать основной результат этого параграфа, известный как **теорема о подгруппах** или коротко `Untergruppensatz`.

Untergruppensatz. *Каждая подгруппа G свободной абелевой группы F является свободной абелевой группой ранга не превосходящего ранг F.*

Доказательство. Этот результат продолжает оставаться справедливым для свободных абелевых групп бесконечного ранга, но для наших целей достаточно доказать его только для групп конечного ранга. Будем вести доказательство индукцией по рангу n группы F. Для $n = 0$ утверждение очевидно, а для $n = 1$ равносильно тому, что $\mathbb{Z}$ является кольцом главных идеалов и уже обсуждалось в Главе 2. Пусть теперь F — свободная абелева группа ранга n, с базисом $x_1, \dots, x_n$. Рассмотрим подгруппу $H = \langle x_1, \dots, x_{n-1}\rangle$ в F. Тогда $F = H \oplus \langle x_n\rangle$, где $\langle x_n\rangle \cong \mathbb{Z}$ свободная абелева группа ранга 1 и мы можем рассмотреть проекцию $\pi : F \longrightarrow \langle x_n\rangle$ с ядром H. Тогда $\pi(G)$ является подгруппой в $\langle x_n\rangle$ и, значит, сама свободна в силу базы индукции. Воспользовавшись предыдущей теоремой, мы видим, что $G \cong \mathrm{Ker}(\pi|_G) \oplus \pi(G)$. Но ведь $\mathrm{Ker}(\pi|_G) \leq H$ является подгруппой в свободной абелевой группе H ранга $n-1$ и, значит, свободна по индукционному предположению.

§ 5. Подгруппа кручения

Пусть G — абелева группа. Обозначим через $T(G)$ множество всех элементов конечного порядка. Легко видеть, что $T(G) \leq G$, в самом деле, если $x, y \in T(G)$, то найдутся такие $m, n \in \mathbb{N}$, что $mx = ny = 0$, а тогда $mn(x - y) = 0$, так что разность двух элементов конечного порядка тоже является элементом конечного порядка. Группа $T(G)$ называется **подгруппой кручения** группы G. Обозначение $T(G)$ объясняется тем, что T — первая буква слова `torsion` (=кручение).

Предостережение. Условие, что G абелева здесь абсолютно необходимо! В неабелевой группе G элементы конечного порядка подгруппы не образуют. Например, в симметрической группе $\mathrm{Bij}(\mathbb{R}, \mathbb{R})$ отображения $x \mapsto -x$ и $x \mapsto 1 - x$ оба имеют порядок 2, но порядок их композиции $x \mapsto x + 1$ бесконечен.

Задача. Докажите, что $T(H \times G) = T(H) \times T(G)$.

Группа G называется **группой кручения** (`torsion group`), если $T(G) = G$, и **группой без кручения** (`torsion-free group`), если $T(G) = 0$. Если $0 < T(G) < G$, то группа G называется **смешанной**. С точки зрения общей теории групп группы кручения это *в точности* периодические абелевы группы, все элементы которых имеют конечный порядок. Все ненулевые элементы группы без кручения имеют бесконечный порядок, а в смешанной группе встречаются ненулевые элементы как конечного, так и бесконечного порядка. Любая конечная абелева группа является группой кручения, а свободная абелева группа — группой без кручения.

Лемма. *Фактор-группа $G/T(G)$ не имеет кручения.*

Доказательство. В самом деле, пусть $x \in G/T(G)$ элемент конечного порядка, пусть, скажем, $x^m = e$. Представим x в виде $x = yT(G)$, где $y \in G$. Равенство $x^m = e$ означает, что $y^m T(G) = T(G)$ или, иными словами, $y^m \in T(G)$. Но тогда $y \in T(G)$. Тем самым, $x = e$, как и утверждалось.

Задача. Пусть $H \leq G$ — подгруппа абелевой группы G. Убедитесь, что $H/T(H)$ изоморфна подгруппе в $G/T(G)$.

Указание. Обратите внимание, что $T(H) = H \cap T(G)$.

Теорема. *Конечно-порожденная абелева группа без кручения G является свободной абелевой группой.*

С точностью до несущественных деталей идея доказательства этой теоремы состоит в том, чтобы выбрать конечную систему образующих группы G и показать, что если эта система линейно зависима, то в G можно построить более короткую систему образующих. Разумеется, нет никакой надежды применить эту идею для группам, не являющимся конечно порожденными. И действительно, аддитивная группа $\mathbb{Q} = \mathbb{Q}^+$ не имеет кручения, но в то же время, конечно, не может быть свободной (любые два ее элемента линейно зависимы!)

Доказательство. Пусть $Y \subseteq G$ — какая-то конечная система образующих группы G. Выберем в Y максимальное линейно независимое подмножество $X = \{x_1, \ldots, x_n\}$. Подгруппа $H = \langle x_1, \ldots, x_n \rangle$ в G, порожденная множеством X, свободна, $H \cong \mathbb{Z}^n$. В силу максимальности X для любого $y \in Y \setminus X$ система $\{y, x_1, \ldots, x_n\}$ уже является линейно зависимой. Таким образом, найдутся целые числа $m, m_1, \ldots, m_n$ не все равные нулю такие, что $my + m_1 x_1 + \ldots + m_n x_n = 0$. Так как $x_1, \ldots, x_n$ линейно независимы, то $m \neq 0$ и, значит $my \in H$ для

некоторого $m = m_y \in \mathbb{N}$. Обозначим теперь через m наименьшее общее кратное всех m_y, $y \in Y \setminus X$ (вспомним, что Y конечно!) Тогда $mY \subseteq H$ и, так как Y порождает G, то и $mG \leq H$. Но ведь G группа без кручения и, значит, ядро отображения $\mathrm{pow}_m : G \longrightarrow G$, $g \mapsto mg$, нулевое. Тем самым $G \cong mG \leq H \cong \mathbb{Z}^n$ есть подгруппа свободной абелевой группы ранга n и, значит, сама является свободной абелевой группой ранга $\leq n$.

Осталось резюмировать содержание этого и предыдущего параграфов.

Теорема. *Конечно порожденная абелева группа G представляется в виде прямой суммы $G \cong T(G) \oplus G/T(G)$ конечной группы $T(G)$ и свободной абелевой группы $G/T(G)$.*

Доказательство. В самом деле, предположим, что G порождается элементами $g_1, \ldots, g_n$ и пусть $F \cong \mathbb{Z}^n$ свободная абелева группа ранга n, с базисом $x_1, \ldots, x_n$. Рассмотрим проекцию $\varphi : F \longrightarrow G$, $x_i \mapsto g_i$. Как мы знаем из второй теоремы предыдущего параграфа, подгруппа $\varphi^{-1}(T(G)) \leq F$ является свободной абелевой группой ранга $\leq n$ и, в частности, $T(G)$ порождается не более, чем n элементами. Пусть, скажем, $T(G) = \langle y_1, \ldots, y_s \rangle$, $s \leq n$. Так как, кроме того, каждое y_i имеет конечный порядок m_i, то $|T(G)| \leq m_1 \ldots m_s$, в частности, группа $T(G)$ конечна. Рассмотрим теперь каноническую проекцию $\pi : G \longrightarrow G/T(G)$, $g \mapsto g + T(G)$. Ясно, что фактор-группа $G/T(G)$ конечно порождена — она порождается, например, классами $g_1 + T(G), \ldots, g_n + T(G)$ элементов $g_1, \ldots, g_n$ — и не имеет кручения. По предыдущей теореме она свободна. Осталось лишь сослаться на первую теорему предыдущего параграфа, утверждающую, что свободная фактор-группа выделяется прямым слагаемым.

Абелева группа G называется **расщепляемой**, если $T(G)$ выделяется в ней прямым слагаемым. Мы только что показали, что каждая конечно порожденная абелева группа расщепляема. Однако легко построить нерасщепляемые абелевы группы. Разумеется, такая группа не может быть конечно порожденной. В доказательстве следующей теоремы используются понятия делимой и приведенной группы, которые определены в § 9.

Теорема. *Пусть $G = \prod_{p \in \mathbb{P}} C_p$. Группа кручения $T(G)$ не выделяется в G прямым слагаемым.*

Доказательство. Любой элемент $x \in G$ представляется в виде $x = (x_p)$, $p \in \mathbb{P}$. Ясно, что если среди компонент x_p бесконечное число отличных от 0, то порядок x бесконечен. С другой стороны, если почти все компоненты x равны 0, то порядок

x равен произведению номеров ненулевых компонент. Это значит, что $T(G) = \bigoplus_{p\in\mathbb{P}} C_p$.

Заметим теперь, что $D(G) = 0$. В самом деле, если $x = (x_p)$ делится на простое число q, то найдется такое $y = (y_p)$, что $x_p = qy_p$ и, в частности, $x_q = 0$. Поэтому единственным элементом G, делящимся на все простые, является 0. С другой стороны, очевидно, что фактор-группа $G/T(G)$ делима. В самом деле, для того, чтобы убедиться, что она делима на n, достаточно заметить, что

$$\prod_{p\in\mathbb{P}} C_p/\bigoplus_{p\in\mathbb{P}} C_p \cong \prod_{\substack{p\in\mathbb{P}\\ p>n}} C_p/\bigoplus_{\substack{p\in\mathbb{P}\\ p>n}} C_p$$

Если бы $T(G)$ выделялась в G прямым слагаемым, то существовала бы такая подгруппа $H \leq G$, что $G = T(G) \oplus H$, $H \cong G/T(G)$. Согласно только что доказанному, эта подгруппа H должна быть одновременно делимой и приведенной. Но тогда $H = 0$, что невозможно.

§ 6. Примарное разложение

В этом параграфе мы представим конечную абелеву группу как прямую сумму примарных слагаемых. Напомним, что группа G называется **p-группой**, если порядок любого ее элемента есть степень p, для конечной группы G это условие эквивалентно тому, что ее порядок $|G|$ есть степень p. *Абелева* p-группа G часто называется **p-примарной** группой. Абелева группа G называется **примарной**, если она p-примарна для *какого-то* p. Таким образом, по определению абелева группа в том и только том случае примарна, когда порядки всех ее элементы являются степенями одного и того же простого числа. *Конечная* абелева группа в том и только том случае примарна, когда ее порядок примарен, иными словами, является степенью какого-то простого числа.

Пусть теперь G — произвольная группа, $p \in \mathbb{P}$. Обозначим через $G(p)$ множество всех элементов группы G, порядок которых равен p^m для некоторого $m \in \mathbb{N}$.

Лемма. *Если G абелева группа, то $G(p) \leq G$.*

Доказательство. Пусть $x, y \in G(p)$. Это значит, что $x^{p^l} = y^{p^m} = 1$ для подходящих $l, m \in \mathbb{N}$. Ясно, что $\mathrm{ord}(x^{-1}) = \mathrm{ord}(x) = p^l$. Пусть теперь $n = \max(l, m)$, так как G абелева, то $(xy)^{p^n} = 1$.

Построенная так подгруппа $G(p)$ абелевой группы G называется ее **p-примарной компонентой**. Разумеется, для *конечных* абелевых групп понятие p-примарной компоненты совпадает с понятием

силовской p-подгруппы. Однако силовские подгруппы рассматриваются в любых конечных группах (не обязательно абелевых!), в то время как примарные компоненты рассматриваются в любых абелевых группах (не обязательно конечных!) Разложение, существование которого утверждается в следующей теореме, называется **примарным разложением** (`Primärzerlegung`).

Теорема. *Пусть G — конечная абелева группа. Если $p_1, \dots, p_s$ – все простые, делящие порядок группы G, то*

$$G = G(p_1) \oplus \dots \oplus G(p_s).$$

Иными словами, утверждается, что конечная абелева группа является прямым произведением своих силовских p-подгрупп по всем простым делящим ее порядок. В Главе 9 мы доказываем более общий результат, состоящий в том, что любая конечная *нильпотентная* группа является прямым произведением своих силовских p-подгрупп. Специфика абелева случая состоит в том, что примарное разложение легко обобщается и на бесконечные периодические группы.

Доказательство. Докажем вначале единственность разложения. Допустим, что $x_1 \dots x_s = 1$ для некоторых $x_i \in G(p_i)$ и пусть

$$m = \operatorname{ord}(x_1) \dots \widehat{\operatorname{ord}(x_j)} \dots \operatorname{ord}(x_s)$$

— произведение порядков всех элементов x_i, кроме j-го. Так как $m \perp p_j$, а $\operatorname{ord}(x_j) = p_j^l$, то $m \perp \operatorname{ord}(x_j)$ и, значит, $\operatorname{ord}(x_j^m) = \operatorname{ord}(x_j)$. Поэтому

$$x_j^m = x_1^m \dots x_j^m \dots x_s^m = (x_1 \dots x_s)^m = e.$$

Значит, $x_j^m = e$ и, тем самым, $x_j = e$.

Для доказательства существования разложения воспользуемся следующей леммой. Пусть m — делитель порядка группы G. Рассмотрим отображение $\operatorname{pow}_m : G \longrightarrow G$, $g \mapsto mg$, возведения в m-ю степень. Ядро этого гомоморфизма будет коротко обозначаться через $G_m = \{g \in G \mid mg = 0\}$, а его образ — через $mG = \{mg \mid g \in G\}$. Напомним, что натуральное число n такое, что $nG = 0$ называется **показателем** группы G. В качестве показателя группы G можно, например, взять ее порядок $|G|$.

Лемма. *Если показатель n абелевой группы G представляется в виде $n = lm$ для некоторых $l \perp m$, то $G = G_l \oplus G_m$.*

Для завершения доказательства теоремы нам остается лишь применить индукцию по количеству простых множителей порядка группы G.

Доказательство леммы. Заметим, прежде всего, что $G = lG + mG$. В самом деле, так как $l \perp m$, то найдутся такие r, s, что $rl + ms = 1$. Поэтому

$$G = (rl + sm)G = rlG + smG \leq lG + mG \leq G,$$

как и утверждалось. С другой стороны, $G_l \cap G_m = 0$. В самом деле, для любого $g \in G_l \cap G_m$ имеем $lg = mg = 0$. Но тогда $g = (rl + sm)g = 0$.

Для доказательства леммы остается лишь заметить, что так как $nG = 0$, то $lG \leq G_m$ и $mG \leq G_l$. Но это значит, что $G_l + G_m \geq mG + lG = G$ и $lG \cap mG \leq G_l \cap G_m = 0$, так что, окончательно, $G_l = mG$, $G_m = lG$ и $G = G_l \oplus G_m = mG \oplus lG$.

Из этой леммы, в частности, вытекает следующий результат, являющийся слабой формой **китайской теоремы об остатках**.

Следствие. *Если $n = lm$ для некоторых $l \perp m$, то $C_n \cong C_l \oplus C_m$.*

В действительности, китайская теорема об остатках утверждает, что при условии взаимной простоты l и m имеет место изоморфизм *колец*

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}.$$

Этот результат доказывается в книге III. Пока же мы утверждаем лишь, что изоморфны *аддитивные группы* этих колец.

Задача. Докажите, что $C_m \oplus C_n \cong C_{\mathrm{lcm}(m,n)} \oplus C_{\gcd(m,n)}$.

Читатель может без труда убедиться в том, что не только конечные абелевы группы, но и вообще все периодические абелевы группы допускают примарное разложение.

Теорема. *Каждая группа кручения G представляется как прямая сумма своих примарных компонент $G = \bigoplus_{p \in \mathbb{P}} G(p)$.*

Разумеется, отличие общего случая от случая конечных абелевых групп состоит в том, что теперь, вообще говоря, среди примарных компонент может быть бесконечное число нетривиальных.

§ 7. Разложение на циклические слагаемые

> However, there is question whether there exist data to span the development in the years 1801 to 1869.
>
> Luboš Nový, [Origins], p.206

Бурбаки в историческом очерке к главам VI и VII своей *Алгебры* высказывают мнение, что **имплицитно** следующий результат был известен уже Гауссу около 1801 года. Первая *почти* явная формулировка была дана в 1869 году издателем трудов Гаусса Шерингом [250] и в 1870 году Кронекером [251] в контексте групп классов квадратичных форм. Однако первое полное доказательство для абстрактных абелевых групп было найдено только в 1879 году Фробениусом и Штикельбергером. Этот замечательный результат является одной из первых классификационных теорем в теории групп.

Basissatz. *Любая конечная абелева группа является прямой суммой примарных циклических групп.*

Эту теорему можно доказывать в следующей эквивалентной форме.

Теорема. *Примарные циклические группы C_{p^m} являются единственными неразложимыми конечными абелевыми группами.*

Доказательство. Достаточно доказать, что каждая абелева группа G, *не являющаяся* примарной циклической, допускает нетривиальное разложение в прямую сумму. По теореме предыдущего параграфа можно считать, что G является p-группой, скажем, $|G| = p^n$. Рассмотрим максимальную циклическую подгруппу A группы G. Пусть, скажем, $|A| = p^l$, где p^l — наибольший порядок элемента в G. Это значит, что $p^l G = 0$, но $p^{l-1}G \neq 0$. Индукцией по порядку G мы покажем, что A выделяется прямым слагаемым.

Предположим, что существует нетривиальная подгруппа $H \leq G$ такая, что $A \cap H = 0$. Рассмотрим каноническую проекцию $\varphi : G \longrightarrow G/H$. По индукционному предположению $\varphi(A)$ выделяется в G/H прямым слагаемым, т. е. найдется такая подгруппа $C \leq G/H$, что $\varphi(A) \oplus C = G/H$. Положим $B = \varphi^{-1}(C)$. Так как $B \geq H$, то $G = A+B$. Мы утверждаем, что в действительности $G = A \oplus B$. В самом деле, если $x \in A \cap B$, то $\varphi(x) \in \varphi(A) \cap C = 0$, так что $x \in \mathrm{Ker}(\varphi) = H$, но ведь $A \cap H = 0$ по условию.

Итак, нам осталось предъявить нетривиальную подгруппу $H \leq G$, имеющую тривиальное пересечение с A. Если в G найдется элемент x порядка p, не лежащий в A, то мы можем взять $H = \langle x \rangle$. Поэтому

нам осталось лишь исключить возможность того, что **все** элементы порядка p лежат в A. Так как группа A циклическая, это значило бы, что ядро $F = \{x \in G \mid px = 0\} = \{x \in A \mid px = 0\}$ умножения на p содержит **ровно** p элементов и, поскольку $p^{l-1}G \neq 0$ содержится в F, то $|p^{l-1}G| = p$. Тем самым, $|G| = p|pG| = p^2|p^2G| = \ldots = p^{l-1}|p^{l-1}G| = p^l = |A|$, так что уже сама группа G является циклической, вопреки предположению.

Задача. Докажите, что если C — циклическая подгруппа наибольшего порядка конечной абелевой группы A, то C выделяется в A прямым слагаемым (т. е. найдется такая подгруппа $B \leq A$, что $A = B \oplus C$).

Задача. Докажите, что если p — простой делитель порядка конечной абелевой группы G, то в G найдется подгруппа индекса p.

Следствие 1. *Если m — делитель порядка конечной абелевой группы G, то в G найдется подгруппа порядка m.*

Следствие 2. *В любой конечной абелевой группе G найдется такой ряд подгрупп $1 = G_0 < G_1 < \ldots < G_s = G$, что все фактор-группы G_i/G_{i-1} являются циклическими группами простого порядка.*

Имеется много частичных обобщений этой теоремы на группы удовлетворяющие тем или иным условиям конечности. Упомянем одно из них. Говорят, что G **группа конечного показателя**, если $nG = 0$ для какого-то натурального n. Следующая теорема часто называется **первой теоремой Прюфера**, но в действительности в 1923 году Прюфер доказал ее только для счетных групп [252] в то время как без упоминания о мощности она была доказана Бэром в 1934 году [253].

Теорема Прюфера—Бэра. *Любая абелева группа конечного показателя является прямой суммой примарных циклических групп.*

Задача. Докажите теорему Прюфера—Бэра для групп показателя p.

Исчерпывающее описание групп, представимых в виде прямой суммы примарных циклических групп было дано в 1940-х годах Леонидом Яковлевичем Куликовым [254]. Эти результаты можно найти в любой книге по теории абелевых групп, однако их полная версия требует для своей формулировки введения большого количества достаточно специфических понятий и уводит в сторону от наших основных тем. Поэтому мы ограничимся таким красивым следствием его основного результата. Мы уже знаем, что подгруппы свободных абелевых групп сами являются свободными абелевыми группами. Оказывается, этот результат можно обобщить следующим образом.

Теорема Куликова. *Каждая подгруппа в прямой сумме (примарных) циклических групп сама является прямой суммой (примарных) циклических групп.*

§ 8. Единственность разложения на циклические слагаемые

Хайнц Прюфер = `Heinz Prüfer` (10.11.1896 — 07 апреля 1934) — замечательный немецкий математик, основные работы которого относятся к теории алгебраических групп, алгебраической теории чисел, теории дифференциальных уравнений и топологии.

В двух предыдущих параграфах мы доказали, что каждая конечная абелева группа G может быть представлена в виде $G = G_1 \oplus \ldots \oplus C_s$, где каждое слагаемое примарное циклическое, $G_i \cong C_{p_i^{m_i}}$. Иными словами,

$$G \cong C_{p_1^{m_1}} \oplus \ldots \oplus C_{p_s^{m_s}}.$$

Естественно возникает вопрос, в какой степени слагаемые определены однозначно?

Примарные компоненты группы G определены совершенно однозначно в точном теоретико-множественном смысле, как подмножества в G. С другой стороны, примарная группа, вообще говоря, может раскладываться на циклические слагаемые многими различными способами. Так, например, если $V = \{1, a, b, c\}$ — четверная группа, то

$$V = \{1, a\} \oplus \{1, b\} = \{1, a\} \oplus \{1, c\} = \{1, b\} \oplus \{1, c\}$$

суть три *различных* разложения V в прямую сумму двух циклических слагаемых. Кроме того, конечно, $C_4 \oplus C_2 \cong C_2 \oplus C_4$, так что в разных разложениях одной и той же группы примарные слагаемые могут появляться в различном порядке (no pun indended!)

Что однако не зависит от способа разложения, это *порядки* и *кратности* примарных циклических слагаемых. Следующий результат является очень частным случаем теоремы Ремака—Крулля—Шмидта, которая доказана в следующей части книги. Эта теорема утверждает, что *набор* неразложимых слагаемых конечной группы (в действительности, группы, которая одновременно артинова и нетерова) определен однозначно с точностью до изоморфизма. Однако для конечных *абелевых* групп этот результат моментально доказывается непосредственно.

Fundamentalsatz. *Набор порядков циклических слагаемых, входящих в разложение G, не зависит от способа разложения на примарные циклические слагаемые.*

Доказательство. Так как примарные слагаемые конечной абелевой группы определены однозначно, мы можем с самого начала ограничиться случаем примарной группы. Будем вести доказательство индукцией по порядку $|G|$ группы G, в качестве базы индукции можно

взять $|G| = 1$. В самом деле, рассмотрим два разложения абелевой p-группы группы G на циклические слагаемые. Пусть, скажем,

$$G = H_1 \oplus \ldots \oplus H_r = G_1 \oplus \ldots \oplus G_s$$

где $H_i \cong C_{p_i^{l_i}}$ и $G_i \cong C_{p_i^{m_i}}$. Рассмотрим гомоморфизм возведения в p-ю степень $\mathrm{pow}_p : G \longrightarrow G$, $x \mapsto px$. Так как ядро $\mathrm{pow}_p : C_{p^m} \longrightarrow C_{p^m}$ имеет порядок p, то с точки зрения первого разложения ядро $\mathrm{pow}_p : G \longrightarrow G$ имеет порядок p^r, а с точки зрения второго — порядок p^s. Таким образом, $r = s$. Посмотрим теперь для разнообразия на образ pG гомоморфизма pow_p. Пусть среди слагаемых H_i ровно q не изоморфных C_p, а среди G_i таких слагаемых ровно t. Переставив, если нужно, слагаемые, можно считать, что это, соответственно, первые q и первые t слагаемых. Тем самым, pG раскладывается в прямую сумму двумя различными способами

$$pG = pH_1 \oplus \ldots \oplus pH_q = pG_1 \oplus \ldots \oplus pG_t.$$

Как мы только что доказали, $q = t$ и так как $|pG| < |G|$, то по индукционному предположению еще раз переставляя, если нужно, слагаемые, можно считать, что $H_i \cong G_i$ для всех $i = 1, \ldots, t$. Так как $pC_{p^m} \cong C_{p^{m-1}}$, мы получаем равенства $l_i - 1 = m_i - 1$ для всех $i = 1, \ldots, t$. Тем самым, $l_i = m_i$ для всех таких i, с другой стороны для всех $i = t+1, \ldots, s$ как l_i, так и m_i равны 1. Теорема полностью доказана.

Упражнение (теорема о сокращении). Пусть F, G, H — конечные абелевы группы. Докажите, что если $F \oplus G \cong H \oplus G$, то $F \cong H$.

§ 9. Тип абелевой группы, примеры

Резюмируя содержание двух предыдущих параграфов, мы можем утверждать, что каждая конечная абелева группа однозначно, с точностью до порядка слагаемых, представляется в виде прямой суммы примарных циклических групп

$$G = C_{p_1^{m_1}} \oplus \ldots \oplus C_{p_s^{m_s}},$$

где $p_i \in \mathbb{P}$. Для краткости мы будем говорить, что такая группа является (конечной) **абелевой группой типа** $(p_1^{m_1}, \ldots, p_s^{m_s})$. Это обозначение особенно часто используется в случае p-групп, когда все

p_i совпадают между собой. Вот два типа p-групп играющие, наряду с циклическими p-группами, совершенно исключительную роль в теории конечных групп:

• **элементарная абелева группа** E_{p^m} — группа типа $(p, \dots, p)$. Например, четверная группа $V = E_4$ — это элементарная абелева группа типа $(2, 2)$.

• **гомоциклическая группа** — группа типа $(p^m, \dots, p^m)$.

Перечислим все абелевы p-группы, делящиеся на небольшую степень простого числа.

• Имеется единственная группа порядка p — циклическая группа C_p и *две* группы порядка p^2, как заметил Нетто, обе абелевы, а именно,

◦ циклическая группа C_{p^2},

◦ элементарная абелева группа $E_{p^2} = C_p \oplus C_p$.

• Имеется *три* абелевы группы порядка p^3:

◦ циклическая C_{p^3},

◦ группа $C_{p^2} \oplus C_p$ типа (p^2, p),

◦ элементарная абелева группа $E_{p^3} = C_p \oplus C_p \oplus C_p$.

• Имеется *пять* абелевых групп порядка p^4:

◦ циклическая C_{p^4},

◦ группа $C_{p^3} \oplus C_p$ типа (p^3, p),

◦ гомоциклическая группа $C_{p^2} \oplus C_{p^2}$ типа (p^2, p^2),

◦ группа $C_{p^2} \oplus C_p \oplus C_p$ типа (p^2, p, p)

◦ элементарная абелева группа $E_{p^4} = C_p \oplus C_p \oplus C_p \oplus C_p$.

• Имеется *семь* абелевых групп порядка p^5:

◦ циклическая (p^5),

◦ элементарная абелева (p, p, p, p, p),

◦ и группы типов (p^4, p), (p^3, p^2), (p^3, p, p), (p^2, p^2, p), (p^2, p, p, p).

• Имеется *одинадцать* абелевых групп порядка p^6:

◦ циклическая (p^6),

◦ элементарная абелева (p, p, p, p, p, p),

◦ неэлементарные гомоциклические (p^3, p^3), (p^2, p^2, p^2),

◦ и группы типов (p^5, p), (p^4, p^2), (p^4, p, p), (p^3, p^2, p), (p^3, p, p, p), (p^2, p^2, p, p), (p^2, p, p, p, p).

Вообще, ясно, что количество $A(p^m)$ неизоморфных абелевых групп порядка p^m равно количеству представлений p^m в виде

$$p^m = p^{m_1} \dots p^{m_s} = p^{m_1+\dots+m_s}$$

где $m_1 \geq \dots \geq m_s$. В свою очередь количество таких представлений равно количеству **разбиений** числа n на неубывающие натуральные слагаемые, $m = m_1 + \dots + m_s$, $m_1 \geq \dots \geq m_s$. Количество таких разбиений m задает арифметическую функцию $p(m)$, где `p` — это первая буква выражения `partition function`. Это одна из важнейших функций, играющая ключевую роль в теории алгебраических групп, теории представлений и т. д. Простой явной формулы для этой функции неизвестно, но, конечно, для нее есть хорошие асимптотики и рекуррентные алгоритмы. Ниже приводится таблица значений $A(p^m) = p(m)$, $1 \leq m \leq 200$, вычисленная при помощи функции `PartitionsP` системы `Mathematica`. Вычисление этой таблицы занимает 0 секунд, т. е. время меньшее, чем гранулярность контроля распределения времени `CPU` равная 0.001 секунды. Но уже для небольших значений m таких, скажем, как $51 \leq m \leq 100$, явное *перечисление* всех групп порядка p^m занимает время от нескольких десятков секунд до заметного количества минут.

Упражнение. Перечислите все 15 типов абелевых групп порядка p^7, все 22 типа абелевых групп порядка p^8 и все 30 типов абелевых групп порядка p^9.

Заметим, что знание количества абелевых p-групп позволяет легко найти количество абелевых групп $A(n)$ любого конечного порядка n. В самом деле, из теоремы о примарном разложении следует, что функция A **мультипликативна**, в том смысле, который обычно вкладывают в этот термин специалисты по теории чисел, иными словами, $A(kl) = A(k)A(l)$ для любых *взаимно простых* $k \perp l$. В частности, если $n = p_1^{m_1} \dots p_s^{m_s}$ — каноническое разложение n на простые, то

$$A(n) = A(p_1^{m_1}) \dots A(p_s^{m_s}).$$

Например, если p, q, r — три попарно различных простых числа, то $A(pq) = A(pqr) = 1$, $A(p^2q) = A(p^2qr) = 2$, $A(p^2q^2) = 4$, $A(p^3q) = A(p^3qr) = 3$, $A(p^3q^2) = 6$ и т. д. Теперь начинающий должен взять любой задачник по высшей алгебре и прорешать несколько упражнений в следующем духе.

Количество $A(p^m)$ абелевых групп порядка p^m, $1 \leq m \leq 200$

m	A	m	A	m	A	m	A
1	1	51	239943	101	214481126	151	45060624582
2	2	52	281589	102	241265379	152	49686288421
3	3	53	329931	103	271248950	153	54770336324
4	5	54	386155	104	304801365	154	60356673280
5	7	55	451276	105	342325709	155	66493182097
6	11	56	526823	106	384276336	156	73232243759
7	15	57	614154	107	431149389	157	80630964769
8	22	58	715220	108	483502844	158	88751778802
9	30	59	831820	109	541946240	159	97662728555
10	42	60	966467	110	607163746	160	107438159466
11	56	61	1121505	111	679903203	161	118159068427
12	77	62	1300156	112	761002156	162	129913904637
13	101	63	1505499	113	851376628	163	142798995930
14	135	64	1741630	114	952050665	164	156919475295
15	176	65	2012558	115	1064144451	165	172389800255
16	231	66	2323520	116	1188908248	166	189334822579
17	297	67	2679689	117	1327710076	167	207890420102
18	385	68	3087735	118	1482074143	168	228204732751
19	490	69	3554345	119	1653668665	169	250438925115
20	627	70	4087968	120	1844349560	170	274768617130
21	792	71	4697205	121	2056148051	171	301384802048
22	1002	72	5392783	122	2291320912	172	330495499613
23	1255	73	6185689	123	2552338241	173	362326859895
24	1575	74	7089500	124	2841940500	174	397125074750
25	1958	75	8118264	125	3163127352	175	435157697830
26	2436	76	9289091	126	3519222692	176	476715857290
27	3010	77	10619863	127	3913864295	177	522115831195
28	3718	78	12132164	128	4351078600	178	571701605655
29	4565	79	13848650	129	4835271870	179	625846753120
30	5604	80	15796476	130	5371315400	180	684957390936
31	6842	81	18004327	131	5964539504	181	749474411781
32	8349	82	20506255	132	6620830889	182	819876908323
33	10143	83	23338469	133	7346629512	183	896684817527
34	12310	84	26543660	134	8149040695	184	980462880430
35	14883	85	30167357	135	9035836076	185	1071823774337
36	17977	86	34262962	136	10015581680	186	1171432692373
37	21637	87	38887673	137	11097645016	187	1280011042268
38	26015	88	44108109	138	12292341831	188	1398341745571
39	31185	89	49995925	139	13610949895	189	1527273599625
40	37338	90	56634173	140	15065878135	190	1667727404093
41	44583	91	64112359	141	16670689208	191	1820701100652
42	53174	92	72533807	142	18440293320	192	1987276856363
43	63261	93	82010177	143	20390982757	193	2168627105469
44	75175	94	92669720	144	22540654445	194	2366022741845
45	89134	95	104651419	145	24908858009	195	2580840212973
46	105558	96	118114304	146	27517052599	196	2814570987591
47	124754	97	133230930	147	30388671978	197	3068829878530
48	147273	98	150198136	148	33549419497	198	3345365983698
49	173525	99	169229875	149	37027355200	199	3646072432125
50	204226	100	190569292	150	40853235313	200	3972999029388

Упражнение. Сколько имеется неизоморфных абелевых групп порядков 72, 108, 216, 360? Что это за группы?

Упражнение. Изоморфны ли группы $C_{36} \oplus C_{24}$ и $C_{48} \oplus C_{18}$?

§ 10. Подгруппы свободной абелевой группы, 2^{nd} installment: классификация

В действительности классификацию конечно порожденных групп можно доказать иначе, и несколько проще, так, как мы это делаем в книге IV в контексте конечно порожденных модулей над кольцом главных идеалов. Это элементарное доказательство является принадлежащей Артину [255] обработкой темы Фробениуса—Штикельбергера, которые как раз и обнаружили связь между классификацией конечно порожденных абелевых групп и опубликованной в 1861 году [256] теоремой Смита.

Генри Смит (Henry John Stephen Smith, 02 ноября 1826, Дублин — 09 февраля 1883, Оксфорд) — замечательный ирландский математик, основные работы которого относятся к теории чисел, теории квадратичных форм, теории эллиптических функций и геометрии. После окончания Оксфордского университета в 1850 году он начал преподавать там и в 1860 году стал профессором. В 1883 году Смит разделил с Минковским премию Парижской Академии наук за работу на тему о суммах пяти квадратов, Смит не дожил нескольких дней до получения премии, а для восемнадцатилетнего Минковского эта премия была началом его блистательной научной карьеры.

Это доказательство не требует отдельного рассмотрения конечных групп и групп без кручения, а сразу доказывает, что любая конечно порожденная абелева группа является прямой суммой (конечных или бесконечных) циклических групп, после чего ко всем конечным циклическим слагаемым можно применить китайскую теорему об остатках. Позже в своих исследованиях канонических форм операторов над произвольным полем K Фробениус именно таким способом доказывал аналогичный результат для модулей над $K[t]$.

А именно, пусть G — конечно порожденная абелева группа с системой образующих $g_1, \dots, g_n$. Рассмотрим свободную абелеву группу $F \cong \mathbb{Z}^n$ с базисом $x_1, \dots, x_n$ той же мощности. Как мы знаем из § ?, существует единственный гомоморфизм $\varphi : F \longrightarrow G$, отображающий x_i в g_i. Поэтому для того, чтобы описать с точностью до изоморфизма все n-порожденные абелевы группы, достаточно описать подгруппы в $\mathbb{Z}^n$. В § 2 мы уже доказали, что каждая такая подгруппа свободна и ее ранг не превосходит n. Полное описание подгрупп в $\mathbb{Z}^n$ сразу

вытекает из теоремы Смита о канонической форме матриц над $\mathbb{Z}$ с точностью до эквивалентности.

Теорема Смита. *Для любой матрицы $a \in M(n, m, \mathbb{Z})$ существуют такие обратимые матрицы $b \in \mathrm{GL}(n, \mathbb{Z})$ и $c \in \mathrm{GL}(m, \mathbb{Z})$, что bac представляет собой окаймленную нулями диагональную матрицу $d = \mathrm{diag}(d_1, \dots, d_r)$, где $d_i \in \mathbb{N}_0$, причем $d_i | d_{i+1}$ для всех $i = 1, \dots, r$. Матрица d определяется матрицей a однозначно.*

Полученная в этой теореме диагональная матрица d называется **формой Смита** матрицы a. При этом d_1 есть наибольший общий делитель элементов матрицы a, произведение $d_1 d_2$ есть наибольший общий делитель миноров второго порядка матрицы a и, вообще для любого l произведение $d_1 d_2 \dots d_l$ есть наибольший общий делитель миноров l-го порядка матрицы a.

В действительности аналог формы Смита имеет место *по крайней мере* для матриц над любым кольцом главных идеалов R — для кольца $R = K[t]$ многочленов от одной переменной над полем это как раз и было доказано Фробениусом. Несколько доказательств теоремы Смита для различных классов колец и различные ее следствия подробнейшим образом обсуждаются в книге IV, посвященной линейной алгебре. То доказательство которое мы приводим ниже, работает только для эвклидовых колец, но для наших целей этого вполне достаточно.

Для наших целей теорему Смита удобнее сформулировать чуть иначе. А именно, пусть $H \leq F$ — подгруппа свободной абелевой группы конечного ранга F. Пусть, далее, $m \leq n$ — ранги групп H и F, соответственно, $x_1, \dots, x_n$ — базис F, а $y_1, \dots, y_m$ — базис H. Рассмотрим матрицу a состоящую из координат векторов y_j в базисе $(x_1, \dots, x_n)$, иными словами, $(x_1, \dots, x_n)a = (y_1, \dots, y_m)$. При замене базиса (x_i) матрица a умножается слева на матрицу перехода от нового базиса к старому. С другой стороны при замене базиса (y_j) матрица a умножается справа на матрицу перехода от старого базиса к новому. Так как унимодулярные матрицы это *в точности* матрицы, выступающие в качестве матриц замены базиса, то теореме Смита можно придать следующую эквивалентную форму.

Теорема. *Пусть $H \leq F$ — подгруппа конечно порожденной свободной абелевой группы F. Тогда существует такой базис $x_1, \dots, x_n$ в F, и такие $d_1, \dots, d_r \in \mathbb{N}_0$, что $d_1 | d_2 | \dots | d_r$, что $d_1 x_1, \dots, d_r x_r$ образуют базис группы H.*

Доказательство. Будем вести доказательство индукцией по рангу F. Для случаев $n = 0$ и $n = 1$ доказывать нечего, поэтому мы можем

считать, что $n \geq 2$ и для всех групп меньшего ранга теорема уже доказана. Если $H = 0$, то доказывать тоже нечего, пусть поэтому $H \neq 0$.

Выберем такой базис $x_1, \ldots, x_n$ в F и такой элемент $y \in H$, что коэффициент a_1 в выражении $y = a_1x_1 + \ldots + a_nx_n$ принимает наименьшее возможное *положительное* значение, для всех выборов базиса в F и всех элементов $y \in H$. Отсюда не[]медленно вытекает, что a_1 делит все a_i, $i \geq 2$. В самом деле, иначе переставляя, если нужно, x_i и x_2, мы можем считать, что a_1 не делит a_2. Поделим a_2 на a_1 с остатком (здесь использована эвклидовость $\mathbb{Z}$). Если $a_2 = qa_1 + r$, $0 < r < a_1$, то $y = rx_2 + a_1(x_1 + qx_2) + a_3x_3 + \ldots + a_nx_n$ и, значит, в выражении y в базисе $x_2, x_1 + qx_2, x_3, \ldots, x_n$ получается положительная координата r строго меньшая, чем a_1, что невозможно.

Итак, $a_i = q_ia_1$ для всех $i \geq 2$ и, значит, перейдя, если нужно от базиса $x_1, x_2, \ldots, x_n$ к базису $x_1 + q_2x_2 + \ldots + q_nx_n, x_2, \ldots, x_n$, мы можем с самого начала считать, что $a_1x_1 \in H$. Мы утверждаем, что a_1 и есть искомое d_1. Для того, чтобы убедиться в этом, нам достаточно проверить, что для любого элемента $z = b_1x_1 + \ldots + b_nx_n \in H$ его первая координата b_1 делится на a_1. В самом деле, если это не так, то поделим b_1 на a_1 с остатком (здесь снова использована эвклидовость $\mathbb{Z}$). Если $b_1 = qa_1 + r$, $0 < r < a_1$, то первая координата $z - qy = rx_1 + (b_2 - qa_2)x_2 + \ldots + (b_n - qa_n)x_n \in H$ положительная и строго меньше, чем a_1, что невозможно. Итак, мы доказали, что a_1 делит все координаты всех векторов из H во всех базисах F. Положим $d_1 = a_1$ и завершим доказательство по индукции.

При этом мы можем действовать точно так же, как в § 2. А именно, рассмотрим проекцию $\pi : F \longrightarrow \langle x_1 \rangle$ с ядром $G = \langle x_2, \ldots, x_n \rangle$. Образ $\pi(H) = \langle d_1x_1 \rangle$ является свободной абелевой группой и, значит, выделяется в H прямым слагаемым, $H = \langle d_1x_1 \rangle \oplus \operatorname{Ker}(\pi|_H)$. В свою очередь $\operatorname{Ker}(\pi|_H) = H \cap G$ является подгруппой в свободной абелевой группе G ранга $n-1$ и к ней применимо индукционное предположение.

Вот еще одна переформулировка теоремы Смита. Разумеется, сам Смит никогда не формулировал ее таким образом!

Теорема. *Любую конечно порожденную абелеву группу G можно представить в виде*

$$G = C_{d_1} \oplus \ldots \oplus C_{d_r} \oplus \mathbb{Z} \oplus \ldots \oplus \mathbb{Z},$$

где $d_1|d_2|\ldots|d_r$. При этом d_i и количество бесконечных циклических слагаемых однозначно определяются группой G.

Доказательство. Пусть $G = \langle g_1, \dots, g_n \rangle$. Построим свободную абелеву группу F с базисом $z_1, \dots, z_n$ и пусть H — ядро проекции $\varphi : F \longrightarrow F$, $z_i \mapsto g_i$. Согласно только что доказанному в F можно выбрать базис $x_1, \dots, x_n$ такой, что $d_1x_1, \dots, d_rx_r$ образуют базис в H. Но это и значит, что $G \cong F/H$ имеет требуемый вид.

Следствие. *Любую конечную абелеву группу G можно представить в виде $G = C_{d_1} \oplus \dots \oplus C_{d_r}$, где $d_1|d_2| \dots |d_r$. При этом d_i однозначно определяются группой G.*

§ 11. Делимые группы

Говорят, что элемент x абелевой группы G **делится на** n (`is divisible by` n), если найдется $y \in G$ такое, что $ny = x$. Иными словами x делится на n если x лежит в образе $\mathrm{pow}_n(G) = nG$ возведения в n-ю степень. Элемент x называется **делимым**, если он делится на любое натуральное число n. Следующая задача показывает, что если x — элемент конечного порядка $o(x)$, то делимость достаточно проверять для делителей $o(x)$.

Задача. Докажите, что если $n \perp o(x)$, то x делится на n.

Решение. В самом деле, если $kn + lo(x) = 1$ для некоторых целых k и l, то мы можем положить $y = kx$.

Множество всех делимых элементов в группе G обозначается через $U(G)$ и называется **ульмовской подгруппой** группы G. Ясно, что $U(G) = \bigcap\limits_{n \in \mathbb{N}} nG$ действительно является подгруппой G. В этом легко убедиться непосредственно. В самом деле, если $x, y \in U(G)$, то для любого $n \in \mathbb{N}$ найдутся такие $u, v \in G$, что $nu = x$, $nv = y$, и тогда $n(u - v) = x - y$, так что разность двух делимых элементов тоже является делимым элементом.

Группа G называется **делимой** (`divisible`), если $U(G) = G$. Таким образом, группа G в том и только том случае делима, когда для любого натурального n гомоморфизм $\mathrm{pow}_n : G \longrightarrow G$ сюръективен, $nG = G$. Делимые абелевы группы часто называются еще **инъективными**, в русской литературе используется и термин **полные** абелевы группы.

Пусть теперь G — произвольная абелева группа. Обозначим через $D(G)$ подгруппу, порожденную всеми содержащимися в G делимыми подгруппами. Легко видеть, что подгруппа $D(G)$ делима и содержит все делимые подгруппы в G. Она называется **делимой частью** группы G. Обозначение $D(G)$ объясняется тем, что D — первая буква

слова `divisible` (=делимый). Абелева группа G называется **приведенной** (`reduced`), если $D(G) = 0$.

Предостережение. В некоторых книгах через $D(G)$ обозначается коммутант группы G, в этом случае D истолковывается как первая буква слова `derived` (=производный). Однако мы всегда обозначаем коммутант группы G через $[G, G]$. В Главе 7 мы действительно пользуемся обозначением $D_i(G)$ для i-го члена ряда коммутантов, при этом $D_1(G) = [G, G]$. Однако ряд коммутантов редко рассматривается при изучении абелевых групп, поэтому я не думаю, что здесь может возникнуть конфликт обозначений.

Упражнение. Убедитесь, что $D(H \times G) = D(H) \times D(G)$.

Упражнение. Убедитесь, что $D(G)$ вполне характеристическая подгруппа в G.

Упражнение. Докажите, что группа $H/D(G)$ приведенная.

Делимая абелева группа без кручения называется **однозначно делимой**. Иными словами, по определению в однозначно делимой группе $D(G) = G$, а $T(G) = 0$. В однозначно делимой группе для любого $x \in G$ и любого $n \in \mathbb{N}$ существует *единственный* элемент y такой, что $ny = z$. В самом деле, если y, z два таких элемента, что $ny = nz = x$, то $n(y - z) = 0$. Но тогда в силу отсутствия кручения $y - z = 0$ и, значит, $y = z$.

Хотя это и не понадобится нам в дальнешем, опишем явную конструкцию подгруппы $D(G)$. Для этого заметим, что $D(G) = U(D(G)) \leq U(G)$. По определению $U(G)$ состоит из элементов делимых в G, однако, они совсем не обязаны оставаться делимыми в $U(G)$. Поэтому $U(U(G)) \leq U(G)$ но, вообще говоря, здесь может иметь место строгое неравенство. Итерируя предыдущее включение можно заключить, что $D(G) = U(D(G)) \leq U(U(G)) = U^2(G)$. По той же причине $D(G) = U(D(G)) \leq U(U^2(G)) = U^3(G)$ и так далее. Конечно, если на каком-то шаге $U^{n+1}(G) = U^n(G)$, то группа $U^n(G)$ делима и, значит, $D(G) = U^n(G)$. Однако в общем случае мы получим строго убывающую цепочку подгрупп $G > U(G) > U^2(G) > \ldots$ возьмем ее пересечение $U^\omega = \bigcap\limits_{n \in \mathbb{N}} U^n(G)$, после чего продолжим это занятие положив $U^{\omega+1} = U(U^\omega(G))$ и далее до полного удволетворения, пока не дойдем все-таки до подгруппы $U^\gamma(G)$ такой, что $U(U^\gamma(G)) = U^\gamma(G)$. Ясно, что это и будет $D(G)$. Однако для групп без кручения процедура построения ульмовских подгрупп обрывается на первом шаге.

Задача. Докажите, что если G — группа без кручения, то $D(G) = U(G)$.

§ 12. Примеры делимых групп

Ясно, что в циклических группах никаких делимых элементов $x \neq 0$ нет, поэтому нет их и в прямых суммах таких групп. В частности, конечные абелевы группы и свободные абелевы группы являются приведенными. Несложно привести и примеры делимых групп:

• Аддитивная группа $\mathbb{Q}$ делима — она специально строилась так, чтобы в ней было возможно деление на любое натуральное число! Более того, эта группа является даже однозначно делимой.

• Квазициклическая группа μ_{p^∞} делима для любого $p \in \mathbb{P}$. В самом деле, из первой задачи этого параграфа мы уже знаем, что если $m \in \mathbb{N}$ взаимно просто с p, то $\mathrm{pow}_m : \mu_{p^\infty} \longrightarrow \mu_{p^\infty}$, $x \mapsto x^m$, биективно — в действительности уже $\mathrm{pow}_m : \mu_{p^r} \longrightarrow \mu_{p^r}$ биективно для всех $r \in \mathbb{N}$. Поэтому любой элемент группы μ_{p^∞} делится на все натуральные числа взаимно простые с p. С другой стороны, образующая группы $\mu_{p^{r+1}}$ в p-й степени дает образующую группы μ_{p^r}. Поэтому в группе $\mu_{p^{r+l}}$ все элементы группы μ_{p^r} делятся на p^l. Осталось заметить, что любое натуральное число n представляется в виде $n = p^r m$, где $m \perp p$. Так как из каждого элемента этой группы существует p различных корней p-й степени, эта группа не является однозначно делимой.

Постараемся осознать и рационализировать рассуждение, фигурирующее в доказательстве делимости группы μ_{p^∞}. Для этого введем более общее понятие p-делимой группы. Абелева группа G называется **p-делимой**, если $p^r G = G$ для любого $r \in \mathbb{N}$.

Упражнение. Докажите, что абелева группа G в том и только том случае p-делима, когда $pG = G$, т. е. когда любой ее элемент делится на p.

Упражнение. Докажите, что группа в том и только том случае делима, когда она p-делима для любого $p \in \mathbb{P}$.

Упражнение. Докажите, что p-группа в том и только том случае делима, когда она p-делима.

Упражнение. Пусть $H \leq G$. Докажите, что если как H, так и G/H обе p-делимы, то G тоже p-делима.

Следующие два упражнения позволяют строить много других примеров делимых групп.

Упражнение. Докажите, что любая фактор-группа делимой группы делима.

Упражнение. Докажите, что прямые суммы и прямые произведения делимых групп делимы.

Следствие. *Любую абелеву группу можно вложить в делимую абелеву группу.*

Доказательство. Бесконечная циклическая группа $\mathbb{Z}$ вкладывается в делимую группу $\mathbb{Q}$. Следовательно, свободная абелева группа $\mathbb{Z}^X$

вкладывается в делимую группу $\mathbb{Q}^X$. Произвольная абелева группа G представима как фактор-группа $G = \mathbb{Z}^X/H$ по какой-то подгруппе $H \leq \mathbb{Z}^X$. Таким образом G вкладывается в делимую группу $\mathbb{Q}^X/H$.

Следующая задача дает характеризацию делимых групп в терминах подгруппы Фраттини $\Phi(G)$. А именно, утверждается, что абелева группа G в том и только том случае делима, когда она совпадает со своей подгруппой Фраттини, $\Phi(G) = G$. Удивительной эта характеризация кажется только на первый взгляд, после классификации делимых групп она станет очевидной!

Задача. Докажите, что абелева группа G в том и только том случае делима, когда в G не существует максимальных подгрупп.

Задача. Докажите, что группа в том и только том случае делима, когда все ее нетривиальные фактор-группы бесконечны.

В частности, делимыми являются группа $\mathbb{Q}/\mathbb{Z}$, аддитивные группы $\mathbb{R}$, $\mathbb{C}$, мультипликативные группы $\mathbb{R}_+$, $\mathbb{C}^*$, группа углов $\mathbb{T} = \mathbb{R}/\mathbb{Z}$, и т. д. Вот два основных источника делимых групп в алгебре:

• Если $\mathrm{char}(K) = 0$, то аддитивная группа K^+ (однозначно) делима. Тем самым, любое векторное пространство над полем характеристики 0 делимо как абелева группа. Более того, векторные пространства над $\mathbb{Q}$ это *в точности* однозначно делимые абелевы группы.

• Если $\overline{K} = K$ — алгебраически замкнутое поле произвольной характеристики, то мультипликативная группа K^* делима.

Однако оказывается, все эти примеры получаются из двух рассмотренных выше. Для этого прежде всего истолкуем μ_{p^∞} как аддитивную группу. Заметим, что фактор-группа $\mathbb{Q}/\mathbb{Z}$ является периодической: порядок класса $m/n + \mathbb{Z}$ делит n. Как замечено в § 4, каждая периодическая абелева группа раскладывается в прямую сумму своих примарных компонент, $\mathbb{Q}/\mathbb{Z} = \bigoplus\limits_{p\in\mathbb{P}} \mathbb{Q}/\mathbb{Z}(p)$.

Задача. Докажите, что $\mathbb{Q}/\mathbb{Z}(p) \cong \mu_{p^\infty}$.

Указание. Группа $\mathbb{Q}/\mathbb{Z}(p)$ порождена элементами

$$1/p, 1/p^2, \ldots, 1/p^r, \ldots$$

Так сопоставьте им что-нибудь разумное!

Теперь у нас все готово, чтобы сформулировать еще один важнейший классификационный результат теории абелевых групп.

Теорема. *Каждая делимая абелева группа представляется как прямая сумма подгрупп, изоморфных либо $\mathbb{Q}$, либо $\mathbb{Q}/\mathbb{Z}(p)$ для какого-то $p \in \mathbb{P}$.*

§ 13. Универсальное свойство делимых групп

В 1940 году Рейнгольд Бэр [257] обнаружил, что совершенно исключительная роль делимых групп связана с тем, что делимые группы — это *в точности* инъективные модули над $\mathbb{Z}$. Определение инъективного модуля получается обращением всех стрелок в определении проективного модуля. Абелева группа G называется **инъективной**, если для любой абелевой группы H, и любого гомоморфизма $\varphi : F \longrightarrow G$ из подгруппы $F \leq H$ в G существует гомоморфизм $\psi : H \longrightarrow G$, продолжающий φ, т. е. такой, что $\psi|_F = \varphi$:

$$\begin{array}{ccccc} 0 & \longrightarrow & F & \longrightarrow & H \\ & & {\scriptstyle\varphi}\big\downarrow & & \\ & & G & & \end{array}$$

Абелева группа в том и только том случае инъективна, когда она делима. Докажем пока первую половину этого утверждения.

Теорема Бэра. *Делимая группа инъективна.*

Доказательство. В самом деле, предположим, что $H \neq G$ и покажем, что если $g \in G \setminus H$, то φ можно продолжить на подгруппу $\langle H, g\rangle$. Для элемента g имеет место следующая альтернатива: либо $ng \notin H$ для всех $n \in \mathbb{N}$, либо $ng \in H$ для какого-то натурального n. В первом случае мы можем продолжить φ до гомоморфизма $\theta : \langle H, g\rangle \longrightarrow F$ полагая $\theta(g) = 0$. Во втором случае возьмем наименьшее $n \in \mathbb{N}$ такое, что $ng \in H$ и рассмотрим $\varphi(ng) \in F$. Так как группа F делима, то найдется такое $x \in F$, что $nx = \varphi(ng)$. Полагая теперь $\theta(h + rg) = \varphi(h) + rx$, $0 \leq r < n$, мы снова получим гомоморфизм (проверьте!) Итак, при $H \neq G$ гомоморфизм φ всегда можно продолжить на какую-то строго большую подгруппу.

Рассмотрим теперь множество M подгрупп в G, на которые можно продолжить гомоморфизм φ. Так как объединение возрастающей цепочки подгрупп из M лежит в M (почему?), то по лемме Куратовского—Цорна в M есть максимальный элемент. Однако мы только что показали, что ни одна собственная подгруппа в G не может быть максимальным элементом M. Это значит, что единственным максимальным элементом M является сама G.

Мы знаем, что свободная фактор-группа выделяется прямым слагаемым. Естественно, для делимых групп выполняется двойственное утверждение.

Следствие. *Если $H \leq G$ — делимая подгруппа абелевой группы G, то H выделяется в G прямым слагаемым.*

Доказательство. Согласно свойству инъективности тождественный гомоморфизм $\varphi = \mathrm{id}_H : H \longrightarrow H$ продолжается до гомоморфизма $\psi : G \longrightarrow H$. Но тогда $G = H \oplus \mathrm{Ker}(\psi)$.

Задача. Докажите, что если $H \leq G$ — делимая подгруппа абелевой группы, а $F \leq G$ — любая подгруппа такая, что $F \cap H = 0$, то дополнительную к H подгруппу можно выбрать так, чтобы она содержала F.

Следствие. *Каждую абелеву группу G, можно представить в виде $G = D(G) \oplus H$ для некоторой приведенной подгруппы H. При этом подгруппа H определена однозначно с точностью до изоморфизма.*

Доказательство. По предыдущему следствию $D(G)$ выделяется прямым слагаемым, при этом дополнительная подгруппа $H \cong G/D(G)$ обязана быть приведенной.

§ 14. Классификация делимых групп

Теорема. *Делимая абелева группа G представляется как прямая сумма подгрупп, каждая из которых изоморфна либо $\mathbb{Q}$, либо $\mathbb{Q}/\mathbb{Z}(p)$ для какого-то $p \in \mathbb{P}$.*

Доказательство. Очевидно, что $H = T(G)$ тоже делима и, следовательно, как мы знаем из предыдущего параграфа, выделяется в G прямым слагаемым, таким образом, $G = H \oplus F$, где F — делимая группа без кручения. Мы также знаем, что периодическая группа H раскладывается в прямую сумму своих примарных компонент $H(p)$, $p \in \mathbb{P}$, каждая из которых снова делима. Таким образом, мы можем с самого начала считать, что либо G делимая p-примарная группа, либо что G делимая групп без кручения.

Следуюший пример еще раз драматически иллюстрирует разницу между прямым произведением и прямой суммой. Мы уже знаем, что группа $\bigoplus\limits_{p\in\mathbb{P}} \mu_{p^\infty}$ изоморфна $\mathbb{Q}/\mathbb{Z}$. Да, но чему изоморфна $\prod\limits_{p\in\mathbb{P}} \mu_{p^\infty}$?

Следствие. *Группа* $G = \prod\limits_{p\in\mathbb{P}} \mu_{p^\infty}$ *изоморфна* $\mathbb{R}/\mathbb{Z} \cong \mathbb{T}$

Доказательство. В самом деле, p-компонента группы G равна μ_{p^∞}, а так как G имеет мощность континуума, она обязана содержать еще континуум слагаемых изоморфных $\mathbb{Q}$. Но группа $\mathbb{R}/\mathbb{Z}$ именно так и устроена.

Следствие. *Группа* $\overline{\mathbb{F}_p}^*$ *изоморфна* $\prod\limits_{\substack{q\in\mathbb{P}\\ q\neq p}} \mu_{q^\infty}$.

Аппендикс 3: ИСТОЧНИКОВЕДЕНИЕ

— И Вы все это прочитали?
— Нет. Я, конечно, работаю с книгами, но не обязан их читать.

Артуро Перес-Реверте. *Клуб Дюма, или тень Ришелье*

Я вас обрадую, всеобщая молва,
Что есть проект насчет лицеев, школ, гимназий;
Там будут лишь учить по нашему: раз, два;
А книги сохранят так: для больших оказий.

Сергей Сергеич, нет! Уж коли зло пресечь:
Забрать все книги бы да сжечь.

А. С. Грибоедов. *Горе от ума*

§ 1. ♣ AMS Subject Classification

Полезно представлять себе общую структуру предмета, для этого служат **предметные классификации**. К сожалению, используемая в российском библиотечном деле УДК (=**универсальная десятичная классификация**) в том, что касается математики устарела лет на 100. Поэтому я приведу классификацию Американского Математического Общества, которая достаточно систематически обновляется. Эта классификация тоже далеко не идеальна, но, поскольку знание не организовано в виде дерева, ни одна древесная классификация по определению не может быть идеальной. Тем не менее, эту классификацию по крайней мере можно принять за основу — и она фактически используется в Mathematical Reviews и Zentralblatt für Mathematik.

По этой классификации легко определить точки роста. Дело в том, что изначально — с учетом того, что могут появиться новые рубрики — рубрикам (кроме, конечно, 20-01, 20-02 и т. д.) присваивались номера, делящиеся на 5. Поэтому в тех местах, где наряду с рубрикой x5 есть рубрика x6 или x7, или с рубрикой x0 есть рубрика x1 или x2. Большей частью это новые рубрики, которые появились или окончательно отпочковались от старых за последние 20-30 лет. Обратите внимание, что в некоторых случаях старые рубрики полностью исчезли! Большей частью появление таких новых рубрик свидетельствует о том, что в этом месте наблюдался значительный рост количества публикаций. Обратите внимание, например, как разделились 20C05 — групповые кольца, 20C10 — целочисленные представления, 20C30 — представления конкретных групп, 20D05 — неразрешимые группы, 20E05 — свободные и близкие к ним группы.

20-XX **Теория групп и обобщения**

20-00 Справочная литература (справочники, словари, библиографии и т. д.)
20-01 Учебная литература (учебники, методические статьи и т. д.)

20-02 Исследовательская литература (монографии, обзорные статьи)
20-03 Историческая литература
20-04 Явные компьютерные вычисления и программы (но не теория вычислений или программирования)
20-06 Труды конференций, сборники статей и т. д.

20Axx **Основания теории групп**

20A05 Аксиомы и элементарные свойства
20A10 Метаматематические консидерации (по поводу проблемы слов см. 20F10)
20A15 Приложения логики к теории групп
20A99 None of the above, but in this section

20Bxx **Группы перестановок**

20B05 Общая теория конечных групп перестановок
20B07 Общая теория бесконечных групп перестановок
20B10 Характеризации
20B15 Примитивные группы
20B20 Кратно транзитивные конечные группы
20B22 Кратно транзитивные бесконечные группы
20B25 Конечные группы автоморфизмов алгебраических, геометрических и комбинаторных объектов (см. также 05Bxx, 12F10, 20G40, 20H30, 51-XX)
20B27 Бесконечные группы автоморфизмов
20B30 Симметрические группы
20B35 Подгруппы симметрических групп
20B40 Вычислительные методы
20B99 None of the above, but in this section

20Cxx **Теория представлений групп**

20C05 Групповые кольца конечных групп и модули над ними
20C07 Групповые кольца бесконечных групп и модули над ними
20C08 Алгебры Гекке и их представления
20C10 Целочисленные представления конечных групп
20C11 p-адические представления конечных групп
20C12 Целочисленные представления бесконечных групп
20C15 Обыкновенные представления и характеры
20C20 Модулярные представления и характеры
20C25 Проективные представления и мультипликаторы
20C30 Представления конечной симметрической группы
20C32 Представления бесконечной симметрической группы
20C33 Представления конечных групп типа Ли
20C34 Представления спорадических групп
20C35 Применения представлений групп в физике
20C40 Вычислительные методы
20C99 None of the above, but in this section

20Dxx **Абстрактные конечные группы**

20D05 Классификация простых и неразрешимых групп

20D06 Простые группы: знакопеременные группы и группы типа Ли
20D08 Простые группы: знакопеременные группы
20D10 Разрешимые группы, теория формаций, классы Шунка, классы Фиттинга, π=длина, ранги (см. также 20F17)
20D15 Нильпотентные группы, p-группы
20D20 Силовские подгруппы, силовские свойства, π-группы, π-структура
20D25 Специальные подгруппы (Фраттини, Фиттинга, и т. д.)
20D30 Ряды и решетки подгрупп
20D35 Субнормальные подгруппы
20D40 Произведения подгрупп
20D45 Автоморфизмы
20D50 Накрытия подгрупп
20D65 Арифметические и комбинаторные свойства
20D99 None of the above, but in this section

20Exx **Структура и классификация бесконечных или конечных групп**

20E05 Свободные неабелевы группы
20E06 Свободные произведения, амальгамированные произведения, HNN-расширения и обобщения
20E07 Теоремы о подгруппах, рост подгрупп
20E08 Группы, действующие на деревьях
20E10 Квазимногообразия и многообразия групп
20E15 Цепочки и решетки подгрупп, субнормальные подгруппы
20E18 Пределы, проконечные группы
20E22 Расширения, сплетения и другие конструкции
20E25 Локальные свойства
20E26 Резидуальные свойства и обобщения
20E28 Максимальные подгруппы
20E32 Простые группы (см. также 20D05)
20E34 Общие структурные теоремы
20E36 Общие теоремы, касающиеся автоморфизмов групп
20E42 Группы с BN-парой, билдинги
20E45 Классы сопряженных элементов
20E99 None of the above, but in this section

20Fxx **Специальные аспекты бесконечных или конечных групп**

20F05 Образующие, соотношения и задания групп
20F06 Теория сокращений, приложения диаграм ван Кампена
20F10 Проблема слов, другие проблемы разрешимости, связь с логикой и автоматами (см. также 03B25, 03D05, 03D40-, 06B25, 08A50, 68Q70)
20F12 Коммутаторное исчисление
20F14 Производные ряды, центральные ряды и их обобщения
20F16 Разрешимые группы, сверхразрешимые группы (см. также 20D10)
20F17 Формации групп, классы Фиттинга (см. также 20D10)
20F18 Нильпотентные группы (см. также 20D10)
20F19 Обобщения разрешимых и нильпотентных групп
20F22 Другие классы групп, определенные рядами подгрупп
20F24 FC-группы и их обобщения
20F28 Группы автоморфизмов групп (см. также 20E36)

20F29 Представления групп как групп автоморфизмов алгебраических систем
20F32 Геометрическая теория групп (см. также 05C25, 20Exx, 20Gxx)
20F34 Фундаментальные группы и их автоморфизмы (см. также 57M05, 57Sxx)
20F36 Группы кос, группы Артина
20F38 Другие группы, возникающие в топологии и анализе
20F40 Связанные с группами лиевские структуры
20F45 Условия Энгеля
20F50 Периодические группы, локально конечные группы
20F55 Отражения и группы Коксетера (см. также 20D10)
20F60 Упорядоченные группы (см. главным образом 06F15)
20F65 Геометрическая теория групп (см. также 05C25, 20E08, 20Mxx)
20F67 Гиперболические группы и группы неположительной кривизны
20F69 Асимптотические свойства групп
20F99 None of the above, but in this section

20Gxx **Линейные алгебраические группы (классические группы)** (по поводу арифметической теории см. 11E57, 11H56, по поводу геометрической теории см. 14Lxx, 22Exx, по поводу других методов теории представлений см. 15A30, 22E45, 22E46, 22E47, 22E50, 22E55)
20G05 Теория представлений
20G10 Теория когомологий
20G15 Линейные алгебраические группы над произвольными полями
20G20 Линейные алгебраические группы над $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{H}$
20G25 Линейные алгебраические группы над локальными полями и их кольцами целых
20G30 Линейные алгебраические группы над глобальными полями и их кольцами целых
20G35 Линейные алгебраические группы над аделями и другими кольцами и схемами
20G40 Линейные алгебраические группы над конечными полями
20G42 Квантовые группы (квантовые алгебры функций) и их представления (см. также 16W35, 17B37, 81R50)
20G45 Приложения к физике
20G99 None of the above, but in this section

20Hxx **Другие группы матриц** (см. также 15A30)
20H05 Унимодулярные группы, конгруэнц-подгруппы (см. также 11F06, 19B37, 22E40, 51F20)
20H10 Фуксовы группы и их обобщения (см. также 11F06, 22E40, 30F35, 32Nxx)
20H15 Другие геометрические группы, включая кристаллографические группы (см. также 51-XX в особенности 51F15, 82B25)
20H20 Другие матричные группы над полями
20H25 Другие матричные группы над кольцами
20H30 Другие матричные группы над конечными полями
20H99 None of the above, but in this section

20Jxx **Связи с гомологической алгеброй и теорией категорий**
20J05 Гомологические методы в теории групп
20J06 Когомологии групп

20J10 Группы, возникающие как грцппы когомологий
20J15 Категория групп
20J99 None of the above, but in this section

Вот остальные темы, включенные в раздел `Теория групп и обобщения`. Поскольку они не относятся к собственно к теории групп, мы ограничимся перечислением названий подразделов:

20Kxx **Абелевы группы**
20Lxx **Группоиды**
20Mxx **Полугруппы**
20Nxx **Другие обобщения групп**
20Pxx **Вероятностные методы в теории групп**

Все эти названия, кроме, может быть, 20N, не требуют долгих экспликаций (`self-explanatory`). В подразделе 20N трактуются квазигруппы, гипергруппы, кучки (груды), полукучки (полугруды), кучкоиды (грудоиды), n-группы и прочие туманности (fuzzy groups).

§ 2. ♡ Теория групп: путеводитель по литературе

Скажи-ка, что глаза ей портить не годится,
И в чтеньи прок-от не велик;
Ей сна нет от французских книг,
А мне от русских больно спится.

А. С. Грибоедов, “Горе от ума”

1. Учебники по теории групп. Среди огромного количества книг, целиком или частично посвященных теории групп или ее приложениям, только четыре, а именно [**97**], [**118**], [**207**], [**220**] претендуют на то, чтобы быть введениями собственно в общую теорию групп.

• С моей точки зрения, **единственной** книгой на русском языке пригодной для первоначального ознакомления с теорией групп и, вместе с тем, достаточно полной, является книга Маршалла Холла [**207**]. Конечно, книга Холла несколько устарела, в частности, это касается терминологии.

• Написанная в 1916 году книга Отто Юльевича Шмидта [**220**] является *выдающимся* памятником истории нашей науки, но не дает представления о состоянии предмета в 1930-е годы*.

• Книга Куроша [**118**] не содержит ничего♯, что могло бы быть полезным

*Кроме того, в [**220**] для обозначения групп и их подмножеств используется фрактура, так что для современного студента ее чтение ничуть не легче, чем чтение любой другой книги на немецком языке!

♯Следующая глубокомысленная фраза в духе Гегеля характеризует уровень понимания Александром Геннадиевичем проблематики теории групп: “Конечной целью теории групп следует считать *задачу полного описания всех существующих в природе групп*”, [**118**], с.423–424. По поводу подобного глубокомыслия Джон фон Нейман заметил: THERE IS NO SENSE IN BEING PRECISE IF YOU DON’T EVEN UNDERSTAND WHAT YOU ARE TALKING ABOUT.

студентам или математикам неспециалистам[b], и совсем немного того, что могло бы быть полезным профессиональному алгебраисту. *Оба* содержательных результата книги Куроша, теоремы Куроша и Грушко, значительно лучше изложены в книгах Масси [**134**] и Серра [**345**] (имеется частичный русский перевод [259]).

• Книга Каргаполова—Мерзлякова [**97**] написана значительно лучше, чем книга Куроша, но тоже в высшей степени неуравновешена и вместо общей теории групп излагает *новосибирскую* теорию групп. С моей точки зрения, лучшей версией этой книги было литографированное издание Новосибирского университета, у которого было **три** автора: Каргаполов, Мерзляков и **Ремесленников**, в дальнейшим с каждым последующим изданием эта книга становилась все хуже и хуже. Еще одной особенностью этой книги является обилие доморощенной терминологии: копредставления называются там **генетическими кодами**, ряды подгрупп — **матрешками** (*нормальные и субнормальные матрешки*), etc.

• Как очень изящное современное введение в теорию групп можно рекомендовать замечательную книгу Олега Богопольского [**32**]. Несмотря на небольшой объем она дает *изумительно* ясное и достаточно продвинутое изложение нескольких ключевых тем как в теории конечных групп, так и в комбинаторной и геометрической теории групп.

• Следующие учебники алгебры содержат одну или две главы, посвященные теории групп, строению конечных групп и, в некоторых случаях, заданию групп образующими и соотношениями и/или теории представлений групп [**23**], [**30**], [**37**], [**48**], [**58**], [**59**], [**91**], [**108**] [**109**], [**110**], [**120**], [**123**], [**169**], [**170**], [**184**], [**185**], [**216**]. Я особенно призываю прочитать §§ 12–18 книги Игоря Ростиславовича Шафаревича [**216**], которые представляют собой введение в *содержательную* теорию групп для начинающих и неспециалистов.

• Из текстов общего характера можно упомянуть еще популярные книги [**6**], [**7**], [**75**], [**93**], [**191**] и сборники задач [**25**], [**82**], [**127**].

2. Отдельные аспекты теории групп. Книга Фукса [**194**] содержит весьма полное изложение теории абелевых групп. Впрочем, как уже отмечалось, с нашей точки зрения теория абелевых групп не имеет почти никакого отношения к теории групп, а является разделом линейной алгебры.

Имеется несколько весьма содержательных и полезных книг, посвященных отдельным аспектам теории групп:

• теория конечных групп [**64**], [**71**], [**90**], [**174**];

• теория представлений конечных групп [**38**], [**57**], [**79**], [**80**], [**119**], [**137**], [**139**], [**168**], [**189**], [**192**], [**205**];

• комбинаторная теория групп [**3**], [**23**], [**43**], [**68**], [**74**], [**117**], [**104**], [**112**], [**124**], [**129**], [**142**], [**146**], [**213**];

• когомологии групп [**5**], [**35**], [**98**], [**133**], [**166**].

Как мы уже упоминали, центральным объектом математики XX века были группы с дополнительными структурами: группы Ли, топологические группы,

[b] С этой точки зрения чрезвычайно поучительно сравнить книгу Куроша с написанной примерно в то же время статьей [258]. Невозможно не отметить, насколько более широкую и детальную панораму теории групп рисует Анатолий Иванович, в частности, все содержание книги [**118**] изложено там на страницах 301–302.

алгебраические группы, etc. Вот некоторые книги, посвященные группам с дополнительными структурами и наиболее важным конкретным группам:

• группы Ли [**2**], [**14**], [**42**], [**44**], [**60**], [**154**], [**156**], [**167**], [**214**], [**217**];

• представления групп Ли [**18**], [**86**], [**87**], [**99**], [**138**];

• топологические группы [**40**], [**41**], [**49**], [**69**], [**73**], [**96**], [**99**], [**153**], [**180**];

• проконечные группы [**5**], [**114**], [**166**];

• алгебраические группы [**5**], [**34**], [**60**], [**62**], [**95**], [**151**], [**195**], [**217**];

• арифметические группы [**5**], [**12**], [**151**], [**196**];

• группы Шевалле, группы Стейнберга [**165**], [**173**], [**136**];

• теория инвариантов [**50**], [**77**], [**84**], [**116**], [**172**];

• линейные группы [**13**], [**19**], [**46**], [**135**], [**136**], [**175**], [**176**];

• классические группы [**1**], [**13**], [**83**], [**88**], [**147**]

• упорядоченные группы [**101**], [**106**], [**107**], [**193**].

3. Приложения теории групп. Особенно обширна литература посвященная не собственно теории групп, а ее приложениям в математике, физике, химии, кристаллографии. Некоторые приложения теории групп в математике описаны в следующих книгах:

• алгебраическая топология [**134**], [**164**], [**206**], [**209**];

• классические геометрии [**11**], [**27**], [**28**], [**36**], [**51**], [**61**], [**76**], [**81**], [**100**], [**141**], [**159**], [**182**], [**203**], [**211**], [**224**];

• автоморфные формы [**12**], ?? , [**66**], [**85**], [**115**], [**122**], [**219**], [**200**];

• гармонический анализ [**126**], [**49**], [**121**], [**204**], [**210**];

• специальные функции [**56**], [**158**];

• теория кодирования [**29**], [**31**], [**105**], [**131**];

• алгебраическая комбинаторика [**17**], [**105**], [**179**];

• перечислительная комбинаторика [**4**], [**24**], [**149**], [**155**], [**162**], [**163**], [**198**], [**199**].

Применения групп за пределами математики. Разумеется, здесь мы приводим лишь незначительную выборку текстов, с содержательной точки зрения **вся** кристаллография и значительная часть теории твердого тела, теории полупроводников и т.д. являются просто разделами прикладной теории групп, мы не можем, конечно, упомянуть все работы в этих областях.

• Тексты общего характера [**16**], [**18**], [**47**], [**52**], [**55**], [**125**], [**150**], [**197**], [**223**], [**225**];

• Кристаллография и теория твердого тела [**9**], [**10**], [**15**], [**63**], [**78**], [**102**], [**130**], [**201**], [**148**], [**221**], [**190**], [**186**], [**187**], [**201**], [**222**];

• Симметрия молекул [**113**], [**190**], [**208**], [**212**];

• Симметрия атомов и ядер [**54**], [**94**], [**132**], [**212**];

• Симметрия элементарных частиц [**128**], [**160**], [**181**]

• Группы Лоренца и Пуанкаре [**67**], [**138**], [**188**], [**53**].

Изложение теории групп с точки зрения потребностей инженеров приведено в учебнике В. И. Смирнова [**171**]. Оно полностью устарело и представляет в настоящий момент чисто исторический интерес, но заслуживает внимания то обстоятельство, что уже в 1940-е годы Владимир Иванович осознавал необходимость включения теории групп в курс высшей математики для физиков, химиков и инженеров.

Книги по теории групп по-русски

[1] *Автоморфизмы классических групп, сб. перев.*, Мир, М., 1976, 264с.

[2] Дж. Адамс, *Лекции по группам Ли*, Наука, М., 1979, 144с.

[3] С. И. Адян, *Проблема Бернсайда и тождества в группах*, Наука, М., 1975, 335с.

[4] М. Айгнер, *Комбинаторная теория*, Мир, М., 1982, 556с.

[5] *Алгебраическая теория чисел*, Мир, М., 1969, 483с.

[6] П. С. Александров, *Введение в теорию групп, 1-е изд.*, Учпедгиз, М., 1938, 128с; 1-е изд., 1951, 126; 3-е изд., Наука, М., 1980, 143с.

[7] В. Б. Алексеев, *Теорема Абеля в задачах и решениях*, Наука, М., 1976, 207с.

[8] Л. К. Аминов, *Теория симметрии*, Ин-т Компьютерных Иссл., М., 2002, 191с.

[9] А. Анималу, *Квантовая теория кристаллических твердых тел*, Мир, М., 1981, 574с.

[10] А. И. Ансельм, *Введение в теорию полупроводников, 2-е изд.*, Наука, М., 1978.

[11] Б. Н. Апанасов, *Дискретные группы преобразований и структуры многообразий*, Наука, М., 1983, 242с.

[12] *Арифметические группы и автоморфные функции, сб. перев.*, Мир, М., 1969, 224с.

[13] Э. Артин, *Геометрическая алгебра*, Наука, М., 1990, 318с.

[14] Л. Ауслендер, Л. Грин, Ф. Хан, *Потоки на однородных пространствах*, Мир, М., 1966, 208с.

[15] Н. Ашкрофт, Н. Мермин, *Физика твердого тела, т.* I, II, Мир, М., 1979, 399с; 422с.

[16] С. Багавантам, Т. Венкатараману, *Теория групп и ее применение к физическим проблемам*, ИЛ, М., 1959, 301с.

[17] Э. Баннаи, Т. Ито, *Алгебрическая комбинаторика. Схемы отношений*, Мир, М., 1987, 373с.

[18] А. Барут, Р. Рончка, *Теория представлений групп и ее приложения, т.* I, II, Мир, М., 1980, 455с; 395с.

[19] Х. Басс, *Алгебраическая K-теория*, Мир, М., 1973, 591с.

[20] Л. Баумгартнер, *Теория групп*, ГТТИ, М.–Л. 1934, 120с.

[21] Р. Бауэр, *Введение в теорию групп*, 1937.

[22] Ю. А. Бахтурин, *Тождества в алгебрах Ли*, Наука, М., 1985, 447с.

[23] Ю. А. Бахтурин, *Основные структуры современной алгебры*, Наука, М., 1990, 318с.

[24] В. В. Белов, Е. М. Воробьев, В. Е. Шаталов, *Теория графов*, Высшая школа, М., 1976, 392с.

[25] В. А. Белоногов, *Задачник по теории групп*, Наука, М., 2000, 237с.

[26] В. А. Белоногов, А. Н. Фомин, *Матричные представления в теории конечных групп*, Наука, М., 1976, 126с.
[27] А. Бердон, *Геометрия дискретных групп*, Наука, М., 1986, 300с.
[28] М. Берже, *Геометрия, т.* I, Мир, М., 1984, 559с.
[29] Э. Берлекэмп, *Алгебраическая теория кодирования*, Мир, М., 1971, 477с.
[30] Г. Биркгоф, Т. Барти, *Современная прикладная алгебра*, Мир, М., 1976.
[31] Р. Блейхут, *Теория и практика кодов, контролирующих ошибки*, Мир, М., 1986, 576с.
[32] О. В. Богопольский, *Введение в теорию групп*, Ин-т Компьютерных Иссл., М., 2002, 148с.
[33] А. Б. Болотин, Н. Ф. Степанов, *Теория групп и ее применения в квантовой механике молекул*, Изд-во Моск. ун-та, М., 1973, 227с.
[34] А. Борель, *Линейные алгебраические группы*, Мир, М., 1972, 269с.
[35] К. Браун, *Когомологии групп*, Наука, М., 1987, 383с.
[36] Г. Бредон, *Введение в теорию компактных групп преобразований*, Наука, М., 1980, 440с.
[37] Н. Бурбаки, *Алгебра, Гл.* I – III. *Алгебраические структуры, линейная и полилинейная алгебра*, Наука, М., 1962, 516с.
[38] Н. Бурбаки, *Алгебра, Гл.* IV – VI. *Многочлены и поля, упорядоченные группы*, Наука, М., 1965, 300с.
[39] Н. Бурбаки, *Алгебра, Гл.* VII – IX. *Модули, кольца, формы*, Наука, М., 1966, 555с.
[40] Н. Бурбаки, *Общая топология, Гл.* III – VIII. *Топологические группы, числа и связанные с ними группы и пространства*, Наука, М., 1969, 392с.
[41] Н. Бурбаки, *Интегрирование, Гл.* VI – VIII. *Векторное интегрирование, мера Хаара, свертка и представления*, ГИФМЛ, М., 1970, 320с.
[42] Н. Бурбаки, *Группы и алгебры Ли, Гл.* I – III. *Алгебры Ли, свободные алгебры Ли и группы Ли*, Мир, М., 1976, 496с.
[43] Н. Бурбаки, *Группы и алгебры Ли, Гл.* IV – VI. *Группы Кокстера и системы Титса, группы, порожденные отражениями, системы корней*, Мир, М., 1972, 331с.
[44] Н. Бурбаки, *Группы и алгебры Ли, Гл.* IX. *Компактные вещественные группы Ли*, Мир, М., 1972, 173с.
[45] В. М. Бусаркин, Ю. М. Горчаков, *Конечные расщепляемые группы*, Наука, М., 1968, 111с.
[46] Р. Бэр, *Линейная алгебра и проективная геометрия*, НИЛ, М., 1955, 399с.
[47] Б. Л. ван дер Варден, *Методы теории групп в квантовой механике*, ОНТИ, Харьков, 1938, 199с.
[48] Б. Л. ван дер Варден, *Алгебра*, Наука, М., 1976, 648с.
[49] А. Вейль, *Интегрирование в топологических группах и его применения*, ИЛ, М., 1950.
[50] Г. Вейль, *Классические группы, их инварианты и представления*, ИЛ, М., 1947, 408с.
[51] Г. Вейль, *Симметрия*, Наука, М., 1968, 191с.
[52] Г. Вейль, *Теория групп и квантовая механика*, Наука, М., 1986, 495с.
[53] Ю. Верле, *Релятивистская теория реакций*, Атомиздат, М., 1969, 441с.
[54] Е. Вигнер, *Теория групп и ее приложение к квантовомеханической теории атомных спектров*, ИЛ, М., 1961.

[55] Е. Вигнер, *Этюды о симметрии*, ИЛ, М., 1971.
[56] Н. Я. Виленкин, *Специальные функции и теория представлений групп*, Наука, М., 1965, 588с.
[57] Э. Б. Винберг, *Линейные представления групп*, Наука, М., 1985.
[58] Э. Б. Винберг, *Начала алгебры*, УРСС, М., 1998, 191с.
[59] Э. Б. Винберг, *Курс алгебры*, Наука, М., 1999, 527с.
[60] Э. Б. Винберг, А. Л. Онищик, *Семинар по группам Ли и алгебраическим группам*, Наука, М., 1988, 343с.
[61] Дж. Вольф, *Пространства постоянной кривизны*, Наука, М., 1982, 480с.
[62] В. Е. Воскресенский, *Алгебраические торы*, Наука, М., 1977, 223с.
[63] У. А. Вустер, *Применение тензоров и теории групп для описания физических свойств кристаллов*, Мир, М., 1977.
[64] *Вычисления в алгебре и теории чисел*, vol. 2, Мир, М., 1976, 304с.
[65] Э. Галуа, *Сочинения*, ОНТИ, М.–Л., 1936, 336с.
[66] И. М. Гельфанд, М. И. Граев, И. И. Пятецкий-Шапиро, *Теория представлений и автоморфные функции*, Мир, М., 1987, 312с.
[67] И. М. Гельфанд, Р. А. Минлос, З. Я. Шапиро, *Представления группы вращений и группы Лоренца*, Физматгиз, М., 1958, 368с.
[68] *Гиперболические группы по Михаилу Громову*, Мир, М., 1992.
[69] А. Гишарде, *Когомологии топологических групп и алгебр Ли*, Мир, М., 1984, 262с.
[70] Л. И. Головина, *Линейная алгебра и некоторые ее приложения. 4-е изд.*, Наука, М., 1985, 392с.
[71] Д. Горенстейн, *Конечные простые группы. Введение в их классификацию*, Мир, М., 1985, 350с.
[72] Ю. М. Горчаков, *Группы с конечными классами сопряженных элементов*, Наука, М., 1978, 119с.
[73] Ф. Гринлиф, *Инвариантные средние на топологических группах*, Мир, М., 1973, 136с.
[74] М. Громов, *Гиперболические группы*, Ин-т Компьютерных Иссл., М., 2002, 159с.
[75] И. Гроссман, В. Магнус, *Группы и графы*, Мир, М., 1971, 247с.
[76] И. Груневальд, Й. Меннике, Ю. Эльстродт, *Группы, действующие на гиперболическом пространстве*, МЦНМО, М., 2003, 615с.
[77] Г. Б. Гуревич, *Основы теории алгебраических инвариантов*, Гостехиздат, М., 1948.
[78] Б. Н. Делоне, Н. Падуров, А. Д. Александров, *Математические основы анализа кристаллов и определение основного параллелепипеда повторяемости при помощи рентгеновских лучей*, ОНТИ, Л.–М., 1934, 328с.
[79] Г. Джеймс, *Теория представлений симметрических групп*, Мир, М., 1982.
[80] Т. том Дик, *Группы преобразований и теория представлений*, Мир, М., 1982, 227с.
[81] Б. А. Дубровин, С. П. Новиков, А. Т. Фоменко, *Современная геометрия. т.* I. *Методы и приложения*, Наука, М., 1979, 759с.
[82] Е. В. Дыбкова, И. Б. Жуков, А. А. Семенов, Р. А. Шмидт, *Основы теории групп*, Изд-во СПбГУ, 1996, 32с.
[83] Ж. Дьедонне, *Геометрия классических групп*, Мир, М., 1974, 204с.

[84] Ж. Дьедонне, Дж. Кэррол, Д. Мамфорд, *Геометрическая теория инвариантов*, Мир, М., 1974, 280с.
[85] Э. Жаке, Р. Ленглендс, *Автоморфные формы на* GL_2, Мир, М., 1973, 372с.
[86] Д. П. Желобенко, *Компактные группы Ли и их представления*, Наука, М., 1970, 664с.
[87] Д. П. Желобенко, А. И. Штерн, *Представления групп Ли*, Наука, М., 1983, 360с.
[88] *Изоморфизмы классических групп над целостными кольцами, сб. перев., т.20*, Мир, М., 1980, 272с.
[89] В. В. Ишханов, В. И. Мысовских, А. И. Скопин, *Теория групп*, Изд-во СПбГУ, 1997, 52с.
[90] *К теории конечных групп, сб. перев.*, vol. 16, Мир, М., 1979, 200с.
[91] Л. А. Калужнин, *Введение в общую алгебру*, Наука, М., 1973.
[92] Л. А. Калужнин, *Избранные главы теории групп*, КГУ, Киев, 1979, 51с.
[93] Л. А. Калужнин, В. И. Сущанский, *Преобразования и перестановки*, Наука, М., 1979, 112с.; 2-е изд., 1985, 160с.
[94] И. Г. Каплан, *Симметрия многоэлектронных систем*, Наука, М., 1969, 407с.
[95] И. Капланский, *Введение в дифференциальную алгебру*, ИЛ, М., 1959.
[96] И. Капланский, *Алгебры Ли и локально компактные группы*, Мир, М., 1974, 148с.
[97] М. И. Каргаполов, Ю. И. Мерзляков, *Основы теории групп*, Наука, М., 1-е изд. 1972, 240с.; 2-е изд. 1977, 238с.; 3-е изд. 1982, 288с.; 4-е изд. 1996, 287с.
[98] А. Картан, С. Эйленберг, *Гомологическая алгебра*, ИЛ, М., 1960, 510с.
[99] А. А. Кириллов, *Элементы теории представлений, 2–е изд.*, Наука, М., 1978, 343с.
[100] Ш. Кобаяси, *Группы преобразований в дифференциальной геометрии*, Наука, М., 1986, 224с.
[101] А. И. Кокорин, В. М. Копытов, *Линейно упорядоченные группы*, Наука, М., 1972, 199с.
[102] Р. Кокс, А. Голд, *Симметрия в твердом теле*, Наука, М., 1970, 424с.
[103] Г. С. М. Коксетер, *Введение в геометрию*, Наука, М., 1966, 648с.
[104] Г. С. М. Коксетер, У. О. Мозер, *Порождающие элементы и определяющие соотношения дискретных групп*, Наука, М., 1980, 240с.
[105] Дж. Конвей, Н. Слоэн, *Упаковки шаров, решетки и группы, т.* I, II, Мир, М., 1990, 413с.; 1991, 427с.
[106] В. М. Копытов, *Решеточно упорядоченные группы*, Наука, М., 1984, 320с.
[107] В. М. Копытов, Н. Я. Медведев, *Правоупорядоченные группы*, Научн. книга, Новосибирск, 1996, 246с.
[108] А. И. Кострикин, *Введение в алгебру*, Наука, М., 1977, 495с.
[109] А. И. Кострикин, *Введение в алгебру,* I. *Основы алгебры*, Физматлит, М., 2000.
[110] А. И. Кострикин, *Введение в алгебру,* III. *Основные структуры алгебры*, Физматлит, М., 2000, 271с.
[111] А. И. Кострикин, Ю. И. Манин, *Линейная алгебра и геометрия, 2е изд.*, 1986, 303с.
[112] А. И. Кострикин, *Вокруг Бернсайда*, Наука, М., 1986, 232с.
[113] Ф. А. Коттон, *Химические приложения теории групп*, Мир, М., 1965.
[114] Х. Кох, *Теория Галуа p-расширений*, Мир, М., 1973, 199с.

[115] Х. Кра, *Автоморфные формы и клейновы группы*, Мир, М., 1975, 296с.
[116] Х. Крафт, *Геометрические методы в теории инвариантов*, Мир, М., 1987, 312с.
[117] Р. Кроуэлл, Р. Фокс, *Введение в теорию узлов*, Мир, М., 1967, 348с.
[118] А. Г. Курош, *Теория групп, 1-е изд.*, Гостехиздат, М., 1944, 372с.; 2-е изд., ГИТТЛ, М., 1953, 468с.; 3–е изд., Наука, М., 1967, 647с.
[119] Ч. Кэртис, И. Райнер, *Теория представлений конечных групп и ассоциативных алгебр*, Наука, М., 1969, 668с.
[120] С. Ленг, *Алгебра*, Мир, М., 1968, 564с.
[121] С. Ленг, $SL_2(\mathbb{R})$, Мир, М., 1977, 430с.
[122] С. Ленг, *Введение в теорию модулярных форм*, Мир, М., 1979, 254с.
[123] Р. Лидл, Г. Пильц, *Прикладная абстрактная алгебра*, Изд-во Уральского Унив., Екатиренбург, 1996.
[124] Р. Линдон, П. Шупп, *Комбинаторная теория групп*, Мир, М., 1980, 447с.
[125] Т. Я. Любарский, *Теория групп и ее применения в физике*, Физматгиз, М., 1957.
[126] Лумис, *Абстрактный гармонический анализ.*
[127] Е. С. Ляпин, А. Я. Айзенштат, М. М. Лесохин, *Упражнения по теории групп*, Наука, М., 1967, 264.
[128] В. Д. Ляховский, Б. А. Болохов, *Группы симметрии и элементарные частицы*, Изд-во ЛГУ, М., 1983, 336с.
[129] В. Магнус, А. Каррас, Д. Солитер, *Комбинаторная теория групп*, Наука, М., 1974, 455с.
[130] О. Маделунг, *Теория твердого тела*, Наука, М., 1980, 416с.
[131] Ф. Дж. Мак-Вильямс, Н. Дж. Слоэн, *Теория кодов, исправляющих ошибки*, Связь, М., 1979, 744с.
[132] Дж. Макки, *Лекции по математическим основам квантовой механики*, Мир, М., 1965, 221с.
[133] С. Маклейн, *Гомология*, Мир, М., 1966, 543с.
[134] У. С. Масси, Дж. Столлингс, *Алгебраическая топология: введение*, Мир, М., 1977, 338с.
[135] Ю. И. Мерзляков, *Рациональные группы*, Наука, М., 1980, 464с.; 2-е изд., 1987, 448с.
[136] Дж. Милнор, *Введение в алгебраическую K-теорию*, Мир, Berlin et al., 1974, 196с.
[137] Ф. Мурнаган, *Теория представлений групп*, ИЛ, М., 1950.
[138] М. А. Наймарк, *Линейные представления группы Лоренца*, Физматгиз, М., 1958.
[139] М. А. Наймарк, *Теория представлений групп*, Наука, М., 1976, 559с.
[140] Ю. А. Неретин, *Категории симметрий и бесконечномерные группы*, Эдиториал, М., 1998, 429с.
[141] В. В. Никулин, И. Р. Шафаревич, *Геометрии и группы*, Наука, М., 1983, 239с.
[142] Х. Нейман, *Многообразия групп*, Мир, М., 1969, 264с.
[143] П. Ноден, К. Китте, *Алгебраическая алгоритмика*, Мир, М., 1999.
[144] *Общая алгебра: группы, кольца и модули*, Наука, М., 1990, 590с.
[145] *Общая алгебра: полугруппы, решетки, универсальные алгебры, категории*, Наука, М., 1991, 479с.

[146] А. Ю. Ольшанский, *Геометрия определяющих соотношений в группах*, Наука, М., 1989.
[147] О. О'Мира, *Лекции о симплектических группах*, Мир, М., 1979, 166с.
[148] Т. Пенкаля, *Очерки кристаллохимии*, Химия, Л., 1974, 496с.
[149] *Перечислительные задачи комбинаторного анализа*, Мир, М., 1979, 363с.
[150] М. И. Петрашень, В. Д. Трифонов, *Применение теории групп в квантовой механике*, ИЛ, М., 1967, 308с.
[151] В. П. Платонов, А. С. Рапинчук, *Алгебраические группы и теория чисел*, Наука, М., 1991, 654с.
[152] Б. И. Плоткин, *Группы автоморфизмов алгебраических систем*, Наука, М., 1966, 603с.
[153] Л. С. Понтрягин, *Непрерывные группы. 1-е изд.*, ГОНТИ, М.–Л., 1938, 316с.; 2-е изд., Гостехиздат, 1954, 516с.; 3-е изд., Наука, М., 1984, 519с.
[154] М. М. Постников, *Группы и алгебры Ли*, Наука, М., 1982, 447с.
[155] *Прикладная комбинаторная математика*, Мир, М., 1968, 362с.
[156] М. С. Рагунатан, *Дискретные подгруппы групп Ли*, Мир, М., 1977, 316с.
[157] *Разрешимые и простые бесконечные группы*, vol. 21, Мир, М., 1981, 208с.
[158] Р. Рихтмайер, *Принципы современной математической физики. т.* II. *Группы и теория представлений*, Мир, М., 1984, 381с.
[159] Б. А. Розенфельд, *Неевклидовы пространства*, Наука, М., 1969, 547с.
[160] Ю. Б. Румер, А. И. Фет, *Теория унитарной симметрии*, Наука, М., 1970, 400с.
[161] Ю. Б. Румер, А. И. Фет, *Теория групп и квантованные поля*, Наука, М., 1977, 247с.
[162] В. Н. Сачков, *Комбинаторные методы дискретной математики*, Наука, М., 1977, 319с.
[163] В. Н. Сачков, *Введение в комбинаторные методы дискретной математики*, Наука, М., 1982, 384с.
[164] Р. М. Свитцер, *Алгебраическая топология — гомотопии и гомологии*, Наука, М., 1985, 606с.
[165] *Семинар по алгебраическим группам*, Мир, М., 1973, 315с.
[166] Ж.-П. Серр, *Когомологии Галуа*, Мир, М., 1968, 208с 375.
[167] Ж.-П. Серр, *Алгебры Ли и группы Ли*, Мир, М., 1969, 375с.
[168] Ж.-П. Серр, *Линейные представления конечных групп*, Мир, М., 1970.
[169] Л. А. Скорняков, *Элементы алгебры*, Наука, М., 1981, 243с.
[170] Л. А. Скорняков, *Элементы общей алгебры*, Наука, М., 1983, 272с.
[171] В. И. Смирнов, *Курс высшей математики*.
[172] Т. Спрингер, *Теория инвариантов*, Мир, М., 1981, 191с.
[173] Р. Стейнберг, *Лекции о группах Шевалле*, Мир, М., 1975.
[174] М. Судзуки, *Строение группы и строение структуры ее подгрупп*, ИЛ, М., 1960, 158с.
[175] Д. А. Супруненко, *Разрешимые и нильпотентные линейные группы*, Изд-во Белорусск. ун-та, Минск, 1958.
[176] Д. А. Супруненко, *Группы матриц*, Наука, М., 1972, 351с.
[177] Д. А. Супруненко, *Группы подстановок*, Навука і Тэхніка, Минск, 1996, 366с.
[178] А. И. Сушкевич, *Теория обобщенных групп*, ГНТИ Украины, Харьков—Киев, 1937, 176с.
[179] В. И. Сущанский, В. С. Сикора, *Операції на группах підстановок: теорія та застосування*, Рута, Чернавці, 2003, 255с.

[180] У. И. Сян, *Когомологическая теория топологических групп преобразований*, Мир, М., 1979, 243с.
[181] *Теория групп и элементарные частицы, сб. статей*, Мир, М., 1967, 375с.
[182] У. Терстон, *Трехмерная геометрия и топология, т.1.*, МЦНМО, М., 2001, 312с.
[183] Д. К. Фаддеев, *Таблицы основных унитарных представлений федоровских групп*, Наука, М.–Л., 1961.
[184] Д. К. Фаддеев, *Лекции по алгебре*, Наука, М., 1984, 416с.
[185] К. Фейс, *Алгебра: кольца, модули, категории.* Т. 1, 1977, 676с.
[186] Е. С. Федоров, *Симметрия и структура кристаллов*, Изд-во АН СССР, М., 1949, 639с.
[187] Е. С. Федоров, *Правильное деление плоскости и пространства*, Наука, Л., 1979, 272с.
[188] Ф. И. Федоров, *Группа Лоренца*, Наука, М., 1979, 384с.
[189] У. Фейт, *Теория представлений конечных групп*, Наука, М., 1990, 461с.
[190] Р. Фларри, *Группы симметрии. Теория и химические приложения*, Мир, М., 1983, 395с.
[191] Э. Фрид, *Элементарное введение в абстрактную алгебру*, Мир, М., 1979, 260с.
[192] Г. Фробениус, *Теория характеров и представлений групп*, ОНТИ, Харьков, 1937.
[193] Л. Фукс, *Частично упорядоченные алгебраические системы*, Мир, М., 1965, 342с.
[194] Л. Фукс, *Бесконечные абелевы группы, т.* I, II, Мир, М., 1974, 335; 1977, 416с.
[195] Дж. Хамфри, *Линейные алгебраические группы*, Наука, М., 1980, 399с.
[196] Дж. Хамфри, *Арифметические группы*, Мир, М., 1983, 207с.
[197] М. Хамермеш, *Теория групп и ее применение к физическим проблемам*, Мир, М., 1966, 587с.
[198] Ф. Харари, *Теория графов*, Мир, М., 1973, 300с.
[199] Ф. Харари, Э. Палмер, *Перечисление графов*, Мир, М., 1977, 324с.
[200] Хариш-Чандра, *Автоморфные формы на полупростых группах Ли*, Мир, М., 1971, 246с.
[201] М. Харрисон, *Теория твердого тела*, Мир, М., 1972, 616с.
[202] В. Хейне, *Теория групп в квантовой механике*, ИЛ, М., 1963, 522с.
[203] С. Хелгасон, *Дифференциальная геометрия и симметрические пространства*, Мир, М., 1965.
[204] С. Хелгасон, *Группы и геометрический анализ*, Мир, М., 1987, 735с.
[205] Э. Хеннан, *Представления групп и прикладная теория вероятностей*, Мир, М., 1970, 118с.
[206] П. Хилтон, С. Уайли, *Теория гомологий: введение в алгебраическую топологию*, Мир, М., 1966, 452с.
[207] М. Холл, *Теория групп*, ИЛ, М., 1962, 468с.
[208] Р. Хохштрассер, *Молекулярные аспекты симметрии*, Мир, М., 1968, 384с.
[209] Э. Хьюзмоллер, *Расслоенные пространства*, Мир, М., 1970, 442с.
[210] Э. Хьюитт, К. Росс, *Абстрактный гармонический анализ, т.* I, Наука, М., 1975, 654с.

[211] Х. Цишанг, Э. Фогт, Ч.-Д. Холдевай, *Поверхности и дискретные группы*, Наука, М., 1988.
[212] Л. Цюлике, *Квантовая химия, т.1*, Мир, М., 1976, 512с.
[213] Б. Чандлер, В. Магнус, *Развитие комбинаторной теории групп*, Мир, М., 1985, 253с.
[214] Н. Г. Чеботарев, *Теория групп Ли*, Гостехиздат, М., 1940.
[215] С. Н. Черников, *Группы с заданными свойствами системы подгрупп*, Наука, М., 1980, 383с.
[216] И. Р. Шафаревич, *Основные понятия алгебры*, R. & C. Dynamics, Ижевск, 1999, 347с.
[217] К. Шевалле, *Теория групп Ли, т.* I – III, ИЛ, М., 1948, 315с.; 1958.
[218] Л. А. Шеметков, *Формации конечных групп*, Наука, М., 1978, 271с.
[219] Г. Шимура, *Введение в арифметическую теорию автоморфных функций*, Мир, М., 1973, 326с.
[220] О. Ю. Шмидт, *Абстрактная теория групп 1-е изд.*, Типография Н.Я.Оглоблина, Киев, 1916, 315; 2-е изд., ГТТИ, М., 1933, 180с., см. также Избранные Труды, Математика, М. Изд-во АН СССР, 1959, 315с..
[221] Г. Штрайтвольф, *Теория групп в физике твердого тела*, Мир, М., 1971, 262с.
[222] А. В. Шубников, *Атлас кристаллографических групп симметрии*, ОНТИ, Л., 1946.
[223] А. В. Шубников, В. А. Копциг, *Симметрия в науке и искусстве*, Наука, М., 1972, 339с.
[224] Л.П.Эйзенхарт, *Непрерывные группы преобразований*, ИЛ, М., 1947, 359с.
[225] Дж. Эллиот, П. Добер, *Симметрия в физике, т.* I, II, Мир, М., 1983, 364; 410с.

§ 3. ♠ Теория групп: a student's guide

Shapiro made a great production of learned references, correctly pronouncing all foreign words, whether in French, German, Serbian, Italian, Hungarian, Turkish, or Danish.

Saul Bellow. *Herzog*

Никаких работ других авторов цитировать не следует, особенно же категорически запрещается цитирование иностранцев*.

Мишель Монтень—Владимир Игоревич Арнольд. *Опыты*, книга II, гл. XII

Вот перечень книг, которые считаются стандартными, хотя каждая из них имеет свою цель, свой уровень, свой стиль изложения и все они сильно различаются между собой.

Эйичи Баннаи, Татцуро Ито. *Алгебраическая комбинаторика*

*Перевод В. И. Арнольда, цитируется по книге В. И. Арнольд, Нужна ли в школе математика? — М., МНЦМО, 2004, с.29; на стр. 16 добросовестный переводчик приводит и формулировку самого Монтеня.

1. Favorites list. Литература по теории групп на английском и немецком языках *необозрима*, так что я ограничусь ссылками на те немногие книги, которые читал, с которыми работал, и некоторые из книг, которые просто держал в руках, если по какой-то причине они поразили мое воображение или произвели на меня впечатление полезных, поучительных и/или забавных. Не указаны книги, которые показались мне либо слишком специальными и представляющими интерес лишь для 3-4 специалистов, либо стандартными, скучными, чисто компилятивными или графоманскими (тексты Григория Карпиловского и большинство вводных французских и американских учебников для undergraduates).

Мое общее ощущение таково, что **все** книги по теории групп (то же относится ко всей алгебре, а может быть и к математике в целом), изданные Springer и Cambridge University Press (C.U.P) могут быть рекомендованы. Вот некоторые из моих `фаворитов`.

• Наиболее сбалансированным введением в теорию групп для *всех* математиков, независимо от специальности, является книга Джозефа Ротмана [**338**].

• Книга Майкла Ашбахера [**231**] представляет собой изумительное по красоте и ясности введение в теорию конечных групп, вплоть до классификации конечных простых групп. Однако, начинающий должен иметь в виду, что некоторые доказательства там оформлены несколько сжато и их понимание может представлять трудности.

• Еще одно замечательное введение в теорию конечных групп и их представлений — книга Альперина и Белла [**229**].

• Лучшее введение в теорию представлений для математиков-неспециалистов — Фултон и Харрис [**270**]. Разумеется, для профессионалов ничто не может заменить знакомство со вторым изданием монументального труда Кэртиса и Райнера [**119**].

• Имеется несколько *монументальных* учебников и монографий по теории конечных групп, в том числе многотомные труды Мичио Судзуки [**350**] и Бертрама Хупперта [**297**].

• Совершенно особое место во всей математической литературе занимают книга Горенстейна [**275**] и цикл книг Горенстейна, Лайонса и Соломона, посвященных классификации [**277**] – [**281**].

• Укажем еще несколько **совершенно выдающихся** текстов, посвященных отдельным наиболее интересным классам групп, вполне доступных для начинающего: Картер [**249**], [**250**], Бенсон—Гроув ?? , Хамфри ?? , Спрингер [**348**], Ашбахер [**232**], [**233**], Серр ?? , Браун ?? и Ронан [**336**]. Полное построение всех 230 пространственных групп изложено в [**311**].

2. Систематический обзор.

• Труды классиков [**271**],,,,,,,,,

• Учебники алгебры [**228**], [**230**], [**254**], [**256**], [**258**], ?? , [**272**], [**273**], [**274**], [**288**], [**293**], [**296**], [**300**], [**301**], [**303**], [**308**], [**316**], [**317**], [**321**], [**330**], [**360**],,,,,,,,,,,,,,,

• Учебники по теории групп [**319**], [**334**], [**337**], [**338**], [**341**], [**342**], [**344**], [**346**], [**350**], [**369**],,,,,,

• Популярная литература [**244**], [**305**], [**325**],,,

• Конечные группы [**229**], [**231**], [**247**], [**275**], [**297**], [**298**], [**315**], [**347**], [**363**],,,,,,

• Классификация конечных простых групп **[233]**, **[257]**, **[268]**, **[276]**, **[277]**–**[281]**,,,,,,

• Спорадические группы **[232]**, **[283]**,,,,,,

• Представления конечных групп **[229]**, **[239]**, **[255]**, **[257]**, **[262]**, **[270]**, **[289]**, **[302]**, **[331]**,,,,,

• Группы типа Ли **[249]**, **[250]**, **[294]**, **[318]**, **[351]**,,,

• Алгебраические группы **[251]**, **[291]**, **[348]**,,,,,

• Арифметические группы **[226]**,,,,,,,

• Группы перестановок **[240]**, **[248]**, **[304]**, **[309]**, **[310]**, **[313]**, **[329]**, **[335]**, **[339]**, **[366]**, ,,,,

• Линейные группы **[236]**, **[241]**, **[259]**, **[261]**, **[355]**, **[362]**, **[364]**,,

• Классические группы **[260]**, **[286]**, **[304]**, **[312]**,,,,

• Группы Ли **[263]**, **[269]**, **[290]**, **[292]**, **[314]**, **[322]**, **[327]**, **[340]**, **[353]**,,,,,,,

• Представления групп Ли **[234]**, **[270]**, **[354]**, **[357]**, **[359]**, **[361]**,,,

• Группы Коксетера **[284]**, **[295]**, **[306]**,,,

• Топологические группы **[324]**, **[332]**, **[367]**,,,

• Группы и геометрии **[245]**, **[328]**, **[352]**,,,

• История теории групп **[243]**, **[282]**, **[368]**,,,

• Геометрическая теория групп **[287]**,,,,,,

• Комбинаторная теория групп **[238]**, **[253]**, **[266]**, **[345]**,,,,,,,,

• Когомологии групп **[227]**, **[235]**, **[252]**, **[285]**, **[349]**,,,,,,,

• Применения групп в физике, химии и минералогии **[237]**, **[265]**, **[311]**, **[323]**, **[326]**, **[356]**,,,,,,,,,

• Бесконечные группы **[307]**, **[333]**, **[343]**,,,,,,,

• Группы в геометрии и топологии **[242]**, **[253]**, **[264]**, **[320]**, **[365]**,

Книги по теории групп не совсем по-русски

[226] P. Abramenko, *Twin buildings and applications to S-arithmetic groups* Springer Lecture Notes Math., vol. 1641, Berlin et al., 1996.

[227] A. Adem, R. J. Milgram, *The cohomology of finite groups*, Springer, Berlin et al., 1994.

[228] W. A. Adkins, S. H. Weintraub, *Algebra: an approach via module theory*, Springer, Berlin et al., 1992, 526p.

[229] J. Alperin, . Bell.

[230] M. Artin, *Algebra*, Prentice Hall, Englewood Cliffs, N. J., 1991.

[231] M. Aschbacher, *Finite group theory, 2nd ed.*, C. U. P., Cambridge, 2000, 304p.

[232] M. Aschbacher, *Sporadic groups*, C. U. P., Cambridge, 1994.

[233] M. Aschbacher, *3-transposition groups*, C. U. P., Cambridge, 1997.

[234] M. Atiyah et al., *Representation theory of Lie groups*, C. U. P., Cambridge, 341p.

[235] A. Babakhanian, *Cohomology of finite groups*, Queen's Univ., Kingston, Ontario, 1999, 216p.

[236] A. Baker, *Matrix groups*, Springer Verlag, Berlin et al., 2002, 330p.

[237] V. Bargmann, *Group representations in mathematics and physics*, Berlin et al., 1970.
[238] G. Baumslag, *Topics in combinatorial group theory*, Birkhäuser, Boston et al., 1993.
[239] D. Benson, *Representations and cohomology: cohomology of groups and modules*, C. U. P., Cambridge, 1991.
[240] N. L. Biggs, A. T. White, *Permutation groups and combinatorial structures*, C. U. P., Cambridge, 1979.
[241] H. R. Blichfeldt, *Finite collineation groups*, Univ. Chicago Press, 1917, 193p.
[242] A. Borel, *Seminar on transformation groups. Ann. Math. Studies*, vol. 46, Princeton Univ. Press, 1960.
[243] A. Borel, *Essays in the history of Lie groups and algebraic groups*, Amer. Math. Soc., Providence, R. I., 2001, 184p.
[244] F. J. Budden, *The fascination of groups*, C. U. P., Cambridge, 1972.
[245] F. Buekenhout (ed.), *Handbook of incidence geometry: buildings and foundations*, Elsevier, Amsterdam et al., 1995.
[246] B. P. Burns, *Geometry: a path to groups*, C. U. P., Cambridge, 1987.
[247] W. Burnside, *Theory of groups of finite order, reprint of the 2nd ed.*, Dover, N.Y., 1955.
[248] P. J. Cameron, *Permutation groups*, C. U. P., Cambridge, 1999, 220p.
[249] R. W. Carter, *Simple groups of Lie type*, Wiley, London et al., 1972, 331p.
[250] R. W. Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley, London et al., 1985, 544p.
[251] C. Chevalley, *Classification des groupes de Lie algebriques, vol.* I, II, ENS, Paris, 1956-58.
[252] D. E. Cohen, *Groups of cohomological dimension one*, Springer, Berlin et al., 1972.
[253] D. E. Cohen, *Combinatorial group theory: a topological approach*, Queen Mary College, London, 1978.
[254] P. M. Cohn, *Algebra, 2nd ed.*, J. Wiley, vol.I — 1982; vol.II — 1989; vol.III — 1991.
[255] M. J. Collins, *Representations and characters of finite groups*, C. U. P., Cambridge, 1990, 242.
[256] E. Connell, *Elements of abstract and linear algebra.*
[257] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, *An atlas of finite groups*, Claredon Press, Oxford, 1972, 284.
[258] R. A. Dean, *Elements of abstract algebra*, Wiley, N. Y., 1966.
[259] L. E. Dickson, *Linear groups, reprint*, Dover, N. Y., 1958.
[260] J. Dieudonné, *Sur les groupes classiques*, Hermann, Paris, 1948.
[261] J. Dixon, *The structure of linear groups*, Van Nostrand — Reinhold, London et al., 1971, 183.
[262] L. Dornhoff, *Group representation theory. Parts A,B*, Marcel Dekker, N. Y. et al., 1971; 1972.
[263] J. J. Duistermaat, J. A. C. Kolk, *Lie groups*, Springer Verlag, Berlin et al., 2000, 344.
[264] P. Du Val, *Homographies, quaternions and rotations*, Oxford, 1964, 116p., см. § 20.
[265] F. J. Dyson, *Symmetry groups in nuclear and particle physics*, Benjamin, N. Y., 1966.

[266] B. Fine, G. Rosenberger, *Algebraic generalizations of discrete groups*, Marcel Dekker, N. Y. et al., 1999, 317.
[267] J. L. Fisher, *Application oriented algebra*, Crowell, N. Y., 1977.
[268] I. Frenkel, J. Lepowsky, A. Meurman, *Vertex operator algebras and the monster*, Academic Press, Boston et al., 1988, 502.
[269] H. Freudenthal, H. de Vries, *Linear Lie groups*, Academic Press, N. Y. et al., 1969, 547.
[270] . Fulton, Harris, *Representation theory, a first course.*
[271] É.Galois, *Écrits et mémoires mathématiques d'Évariste Galois*, Gauthier–Villars, Paris, 1962.
[272] A. Gill, *Applied algebra for computer scientists*, Prentice Hall, Englewood Cliffs, N. J., 1976.
[273] R. Godement, *Algebra*, Houghton-Miffin, Boston, 1968.
[274] L. J. Goldstein, *Abstract algebra*, Prentice Hall, Englewood Cliffs, N. J., 1973.
[275] D. Gorenstein, *Finite groups*, Harper & Row, N. Y., 1st ed. 1968; Chelsea, N. Y., 2nd ed. 1980.
[276] D. Gorenstein, *The classification of finite simple groups, vol.*I*, Groups of noncharacteristic 2 type*, Plenum Press, N. Y., 1983, 487.
[277] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups*, Amer. Math. Society, Providence, R. I., 1994, 165.
[278] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups, N.2, Part* I*, Ch. G. General group theory*, Amer. Math. Society, Providence, R. I., 1996, 218.
[279] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups, N.3, Part* I*, Ch. A. Almost simple K-groups*, Amer. Math. Society, Providence, R. I., 1998, 419.
[280] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups, N.2, Part* II*, Ch. 4. Uniqueness theorems*, Amer. Math. Society, Providence, R. I., 1999, 341.
[281] D. Gorenstein, R. Lyons, R. Solomon, *The classification of the finite simple groups, N.5, Part* III*, Ch. 6. The generic case*, Amer. Math. Society, Providence, R. I., 2002, 467.
[282] J. J. Gray, *Linear differential equations and group theory from Riemann to Poincaré*, Birkhäuser, Basel et al., 2000, 338.
[283] R. L. Griess, *Twelve sporadic groups*, Springer Verlag, Berlin et al., 1998, 169.
[284] L. C. Grove, C. T. Benson, *Finite reflection groups, 2nd ed.*, Springer, Berlin et al., 1985.
[285] C. Gruenberg, *Cohomological topics in group theory* Springer Lecture Notes Math., Berlin et al., 1970.
[286] A. Hahn, O. T. O'Meara, *The classical groups and K-theory*, Springer, Berlin et al., 1989, 576.
[287] P. de la Harpe, *Topics in geometric group theory*, Univ. Chicago Press, Chicago, Il., 2000, 310.
[288] I. N. Herstein, *Topics in algebra*, Blaisdell Publ., Waltham, Mass. et al., 1964.
[289] V. E. Hill, *Groups and characters*, Chappman & Hall, Boca Raton, Fl., 2000, 239.
[290] G. Hochschild, *The structure of Lie groups*, Holden Day, 1965, 230.
[291] G. Hochschild, *Basic theory of algebraic groups and Lie algebras*, Springer, Berlin et al., 1981.

[292] W.-Y. Hsiang, *Lectures on Lie groups*, World Scientific, London et al., 2000, 108.
[293] Hu Sze-Tsen, *Elements of modern algebra*, Holden Day, San Francisco et al., 1965, 208.
[294] J. Humphreys, *Introduction to Lie algebras and representation theory, 3rd revised printing*, Springer Verlag, Berlin et al., 1980.
[295] J. Humphreys, *Reflection groups and Coxeter groups*, C. U. P., Cambridge, 1992.
[296] T. W. Hungerford, *Algebra*, Springer, Berlin et al., 1974, 502.
[297] B. Huppert, *Endliche Gruppen,* Bd. I, Springer, Berlin et al., 1967, 793.
[298] B. Huppert, N. Blackburn, *Finite groups,* vol. II, III, Springer, Berlin et al., 1982, 531; 454.
[299] I. M. Isaacs, *Character theory of finite groups*, Academic Press, N. Y. et al., 1976.
[300] I. M. Isaacs, *Algebra.*
[301] N. Jacobson, *Basic algebra*, W. H. Freeman, N. Y., vol. I — 1985; vol.II — 1989.
[302] D. James, M. Liebeck, *Representations and characters of groups, 2nd ed.*, C. U. P., Cambridge, 2001, 458.
[303] R. E. Johnson, *University algebra*, Prentice Hall, Englewood Cliffs, N. J., 1966, 271.
[304] C. Jordan, *Traité des substitutions et des équations algebriques*, Gauthier-Villars, Paris, 1870.
[305] D. Joyner, *Adventures in group theory*, John Hopkins Univ., Baltimore, 2002, 262.
[306] R. Kane, *Reflection groups and invariant theory*, Springer Verlag, Berlin et al., 2001, 379.
[307] O. Kegel, B. A. F. Wehrfritz, *Locally finite groups*, Amsterdam, 1973, 210.
[308] J. L. Kelley, *Algebra, a modern introduction*, Van Nostrand, Princeton, N. J. et al., 1965, 335.
[309] A. Kerber, *Algebraic combinatorics via finite group actions*, Biblographisches Inst., Mannheim, 1991.
[310] A. Kerber, *Applied finite group actions*, Springer Verlag, Berlin et al., 1999, 454.
[311] Sh. K. Kim, *Group theoretical methods and applications to molecules and crystals*, C. U. P., Cambridge, 1999, 492.
[312] P. B. Kleidman, M. W. Liebeck, *The subgroup structure of the finite classical groups*, C. U. P., Cambridge, 1990, 303.
[313] M. Ch. Klin, R. Pöschel, K. Rosenbaum, *Angewandte Algebra. Einführung in gruppentheoretisch-kombinatorische Methoden*, DVW, Berlin, 1988, 208.
[314] A. W. Knapp, *Lie groups beyond an introduction, 2nd ed.*, Birkhäuser, Boston et al., 2002, 812.
[315] H. Kurzweil, B. Stellmacher, *Theorie der endlichen Gruppen: eine Einführung*, Springer Verlag, Berlin et al., 1998, 341.
[316] S. Lang, *Algebraic structures*, Addison-Wesley, Reading, Mass. et al., 1967.
[317] J. D. Lipton, *Elements of algebra and algebraic computing*, Addison-Wesley, Reading, Mass. et al., 1981,, 342.
[318] G. Lusztig, *Characters of reductive groups over a finite field. Ann. Math. Studies*, vol. 107, Princeton Univ. Press, 1984, 384.
[319] I. D. MacDonald, *The theory of groups*, Claredon Press, Oxford, 1968.
[320] W. Magnus, *Non-Euclidean tesselations and their groups*, Academic Press, N. Y., 1976.

[321] M. Marcus, H. Minc, *Modern University algebra*, MacMillan, N. Y. et al., 1966, 244.
[322] G. A. Margulis, *Discrete subgroups of semisimple Lie groups*, Springer, Berlin et al., 1991.
[323] K. Mathiak, P. Stingl, *Gruppentheorie für Chemiker, Physiko-Chemiker und Mineralogen*, Viehweg, Braunschweig, 1968.
[324] K. Maurin, *General eigenfuction expansions and unitary representations of topological groups*, PWN, Warszawa, 1968, 367.
[325] R. Mirman, *Group theory: an intuitive approach*, World Scientific, London et al., 1995.
[326] R. Mirman, *Point groups, space groups, crystals, molecules*, World Scientific, London et al., 1999, 707.
[327] K. Nomizu, *Lie groups and differential geometry. vol.* I, II, N. Y., 1963; 1969.
[328] A. Pasini, *Diagram geometries*, Claredon Press, Oxford, 1994.
[329] D. Passman, *Permutation groups*, Academic Press, N. Y. et al., 1968.
[330] S. Perlis, *Introduction to algebra*, Blaisdell Publ., Waltham, Mass. et al., 1966, 440.
[331] B. Puttaswamaiah, J. D. Dixon, *Modular representations of finite groups*, Academic Press, N. Y. et al., 1977, 242.
[332] L. Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Univ., Kingston, Ontario, 1999, 316.
[333] D. J. S. Robinson, *Finiteness conditions and generalised soluble groups, vol.* I, II, Springer, Berlin et al., 1972.
[334] D. J. S. Robinson, *A course in the theory of groups*, Springer, Berlin et al., 1982.
[335] . Robinson, *Representations of the symmetric group.*
[336] M. Ronan, *Lectures on buildings*, Academic Press, N. Y. et al., 1989.
[337] J. S. Rose, *A course on group theory*, C. U. P., Cambridge, 1978.
[338] J. J. Rotman, *The theory of groups, an introduction, 2nd ed.*, Allyn & Bacon, Boston, 1973.
[339] B. E. Sagan, *The symmetric groups: representations, combinatorial algorithms, and symmetric functions, 2nd ed.*, Springer Verlag, Berlin et al., 2001, 238.
[340] A. Sagle, R. Walde, *Introductions to Lie groups and Lie algebras*, Academic Press, N. Y. et al., 1973.
[341] E. Schenkman, *Group theory*, N. Y., 1965.
[342] W. R. Scott, *Group theory*, Engelwood Cliffs N. J., Prentice Hall, 1964.
[343] D. Segal, *Polycyclic groups*, C. U. P., Cambridge, 1983.
[344] J.-A. de Séguier, *Theorie des groupes finis. Eléments de la théorie des groupes abstraits*, Gauthier-Villars, Paris, 1904.
[345] J.-P. Serre, *Arbres, amalgames,* SL_2, Astèrisque or Springer, Berlin et al..
[346] G. Smith, O. Tabachnikova, *Topics in group theory*, Springer Verlag, Berlin et al., 2000, 255.
[347] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung,* 4te Aufl., Birkhäuser, Basel et al., 1956, 271.
[348] T. Springer, *Linear algebraic groups*, Birkhäuser, Boston et al., 1981, 304.
[349] U. Stammbach, *Homology in group theory* Springer Lecture Notes Math., vol. 359, Berlin et al., 1973.
[350] M. Suzuki, *Group theory,* vol. I, II, Springer Verlag, Berlin et al., 1982, 434.

[351] F. G. Timmesfeld, *Abstract root subgroups and simple groups of Lie type*, Birkhäuser Verlag, Basel, 2001, 389.
[352] J. Tits, *Buildings of spherical type and finite BN-pairs* Springer Lecture Notes Math., vol. 386, Berlin et al., 1974.
[353] V. S. Varadarajan, *Lie groups, Lie algebras and their representations*, Prentice Hall, 1974.
[354] V. S. Varadarajan, *An introduction to harmonic analysis on semisimple groups*, C. U. P., Cambridge, 1999, 316.
[355] B. van der Waerden, *Gruppen von linearen Transformationen*, Springer, Berlin et al., 1935.
[356] M. Wagner, *Gruppentheoretische Methoden in der Physik*, Vieweg & Sohn, Braunschweig, 1998, 461.
[357] N. Wallach, *Harmonic analysis on homogeneous spaces*, N. Y., 1973.
[358] R. B. Warfield, *Nilpotent groups* Springer Lecture Notes Math., vol. 513, Berlin et al., 1976.
[359] G. Warner, *Harmonic analysis on semi-simple Lie groups vol.* I, II, Berlin, 1972.
[360] S. Warner, *Modern algebra, vol.*I, II, Prentice Hall, Englewood Cliffs, N. J., 1965.
[361] A. Wawrzyńczyk, *Współczesna teoria funkcji specjalnych*, PAN, Warszawa, 1978, 525.
[362] B. A. F. Wehrfritz, *Infinite linear groups*, Springer, Berlin et al., 1973, 229.
[363] B. A. F. Wehrfritz, *Finite groups: a second course on group theory*, World Scientific, London et al., 1999, 123.
[364] B. A. F. Wehrfritz, M. Shirvani, *Skew linear groups*, C. U. P., Cambridge, 1986, 253.
[365] A. T. White, *Graphs, groups and surfaces, 2nd ed.*, North Holland, Amsterdam, 1984.
[366] H. Wielandt, *Finite permutation groups*, Academic Press, N. Y. et al., 1964.
[367] J. S. Wilson, *Profinite groups*, Claredon Press, Oxford et al., 1998, 284.
[368] H. Wussing, *Die Genesis des abstrakten Gruppenbegriffes. Ein Beitrag zur Entstehungsgeschichte der abstrakten Gruppentheorie*, Berlin, 1969, 258pp.
[369] H. Zassenhaus, *The theory of groups*, Dover Publications, N.Y., 1999, 265.

§ 4. ♠ Электронный ресурс

§ 5. ♣ Использованная литература

Приведем список книг, которые непосредственно цитируются в основном тексте один или два раза. Большей частью эти ссылки не предназначены для студента, по крайней мере студента младших курсов! Однако, как мне кажется, аспиранту, профессиональному алгебраисту или тому, кто преподает алгебру на университетском уровне, многие из этих ссылок могут оказаться интересными и полезными. Учитывая интересы этих категорий читателей, я указываю все использованные мной источники. Они делятся на следующие категории:

• Источники (главным образом, статьи из научно-популярных журналов типа American Mathematical Monthly, но в некоторых случаях исследовательские статьи и даже диссертации), из которых взяты отдельные факты, задачи и доказательства.

• Книги и обзорные статьи, где можно найти более детальную информацию по тому или иному специальному вопросу.

• Работы классиков теории групп, в которых — по моему непросвещенному мнению! — были *впервые* введены те или иные понятия или приведены *первые* (а в исключительных случаях вторые, третьи, ...) доказательства ключевых результатов. Однако, не будучи профессиональным историком, я во многих случаях не проводил специальных изысканий, а доверялся старинным книгам, составителям избранных трудов и тем современным источникам, которые представлялись мне заслуживающими наибольшего доверия.

• Некоторые статьи по истории алгебры и биографии математиков, которые показались мне особенно надежными, полными или интересными.

• Источники эпиграфов и цитат, в тех случаях, когда по каким-то причинам я хотел показать, что они подлинные, либо дать возможность читателю сверить мою версию с оригиналом. Все постраничные ссылки в этом списке **фактические**, ни одной выдуманной среди них нет.

• Переводы на русский язык произведений классиков науки и некоторых других книг, представляющих, по моему мнению, общематематический интерес. Иными словами, таких книг, прочесть которые — или хотя бы ознакомиться с которыми — должен каждый образованный математик.

Источники

[1] И. Ф. Стравинский, *О музыкальном феномене*, В кн. Статьи и материалы, Советский композитор, М., 1973, 527с., см. с. 24.

[2] Р. Фейнман, Р. Лейман, М. Сэндс, *Фейнмановские лекции по физике, т. 3. Излучение, волны, кванты*, Мир, М., 1967, 238с., см. с. 9.

[3] П. Тейяр де Шарден, *Феномен человека: преджизнь, жизнь, мысль, сверхжизнь*, Наука, М., 1987, 240с., см. с. 38.

[4] Г. Селье, *От мечты к открытию.*

[5] Р. Грэхем, Д. Кнут, О. Паташник, *Конкретная математика*, М., 1998, 703с.

[6] Г. Вуссинг, *О генезисе абстрактного понятия группы*, Историко-математические исследования **17** (1966), 11–30.

[7] Л. Инфельд, *Эварист Галуа. Избранник богов*, Молодая Гвардия, М., 1965, 352с.

[8] А. Дальма, *Эварист Галуа. Революционер и математик*, Наука, М., 1984, 111с.

[9] Е. М. Полищук, *Софус Ли* (1842–1899), Наука, Л., 1983, 213с.

[10] *Справочная книга по математической логике, ч.*I, *Теория моделей*, Наука, М., 1982, 391с.

[11] У. Фейт, *Некоторые следствия классификации конечных простых групп*, Успехи мат. наук **38** (1983), no. 2, 127–133.

[12] Д. Е. Кнут, *Все про TEX*, Протвино, Изд-во АО RDTEX, 1993 finalinfo 575с., см. с.xi–xii.

[13] Из письма Гаусса Шумахеру от 01.11.1844, см. Briefwechsel Gauss—Schumacher, Bd. 4, 1862, S.337.

[14] H. R. Pitt, *Measure and integration for use*, Claredon Press, Oxford, 1985, 143pp.

[15] G.-C. Rota, *The Phenomenology of Mathematical Beauty,*, Synthese **3** (1997), no. 2.
[16] H. Hankel, Die Entwickelung der Mathematik in den letzten Jahrhunderten. — Akad. Vortrag Tübingen 29.04.1869.
[17] H. Turnbull, цитируется по J. R. Newman, *The world of mathematics*, N.Y., 1956.
[18] J. Bertrand, *D'Alembert*, Paris, 1889, pp. 56–57.
[19] Дж. Займан, *Современная квантовая теория*, Мир, М., 1971, 288с., см. с.9.
[20] Андронов Витт Хайкин.
[21] Ватсон, *Бесселевы функции.*
[22] Л. Янг, *Лекции по вариационному исчислению и теории оптимального управления*, Мир, М., 1974, 488с.
[23] В. И. Арнольд, *Математические методы классической механики. 2-е изд*, М., Наука, 1979, 431с.
[24] В. Феллер, *Введение в теорию вероятностей и ее приложения, т.1*, Мир, М., 1967, 498с.
[25] Г. Гретцер, *Общая теория решеток.*, Мир, М., 1982, 452с., см. с.396.
[26] H. Weber, *Beweis des Satzes, daß jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fahig ist*, Math. Ann. **20** (1882), 301–329.
[27] О. Оре, *Замечательный математик Нильс Генрих Абель*, ГИФМЛ, М., 1961, 343с.
[28] А. И. Мальцев, *Алгебраические системы*, Наука, М., 1970, 392с.; см. с.98.
[29] В. И. Арнольд, *Теория катастроф. 2-е изд*, Изд-во Моск. ун-та, М., 1983, 80с.
[30] В. И. Арнольд, *Обыкновенные дифференциальные уравнения*, Наука, М., 1971, 239с.
[31] В. И. Арнольд, *Дополнительные главы теории обыкновенных дифференциальных уравнений*, М., Наука, 1978, 304с.
[32] В. И. Арнольд, А. Авец, *Эргодические проблемы классической механики*, РХД, Ижевск, 1999, 281с.
[33] В. И. Арнольд, А. Н. Варченко, С. М. Гусейн-Заде, *Особенности дифференцируемых отображений. Т.*I. *Классификация критических точек, каустик и волновых фронтов*, М., Наука, 1982, 304с.
[34] В. И. Арнольд, А. Н. Варченко, С. М. Гусейн-Заде, *Особенности дифференцируемых отображений. Т.*II. *Монодромия и особенности интегралов*, М., Наука, 1984, 335с.
[35] H. Furstenberg, *The inverse operation in groups*, Proc. Amer. Math. Soc. **6** (1955), 991–997.
[36] А. И. Мальцев, *Основы линейной алгебры. 3-е изд*, Наука, М., 1970, 390с.
[37] А. И. Мальцев, *Алгоритмы и рекурсивные функции*, Наука, М., 1965, 391с.
[38] А. И. Мальцев, *Избранные труды. Т.*I. *Классическая алгебра*, Наука, М., 1976, 482с.
[39] А. И. Мальцев, *Избранные труды. Т.*II. *Математическая логика и [очень] общая теория алгебраических систем*, Наука, М., 1976, 388с.
[40] И. Букур, А. Деляну, *Введение в теорию категорий и функторов*, Мир, М., 1972, 259с. См. главу IV, в особенности теорему 4.1.
[41] M. E. Larsen, *Gruppeteori*, København, 1981, p.37.

[42] M. E. Larsen, *Rubik's revenge: the group theoretic solution*, Amer. Math. Monthly (1985, June–July), 381–390.

[43] C. Davis, *A bibliographical survey of groups with two generators and their relations*, N. Y., Courant Inst. Math. Sci., 1972, 353pp.

[44] A. Cayley, *On the theory of groups as depending on the symbolic equation* $\theta^n = 1$. III, Philos. Mag. **7** (1859), 34–37.

[45] A. Cayley, *On the theory of groups*, Amer. J. Math. **11** (1889), 139–157.

[46] G. A. Miller, *The operation groups of order* $8p$*, p being any prime number*, Philos. Mag. **42** (1896), 195–200.

[47] R. Le Vavasseur, *Sur les groupes d'opérations.* II, C. R. Acad. Sci. Paris, 1896, t.122, 516–517.

[48] G. A. Miller, *The regular substitution groups whose orders are less than* 48, Philos. Mag. **42** (1896), 195–200.

[49] G. A. Miller, *On the operation groups whose orders are less than* 64 *and those whose order is* $2p^3$*, p being any prime number*, Quart. J. Math. **30** (1898), 243–263.

[50] G. A. Miller, *Determination of all the abstract groups of order* 72, Amer. J. Math. **51** (1929), 491–494.

[51] G. A. Miller, *Determination of all the groups of order* 96, Ann. Math. **31** (1930), 163–168.

[52] J. K. Senior, A. C. Lunn, *Determination of the groups of orders* 101–161*, omitting order* 128, Amer. J. Math. **56** (1934), 328–338.

[53] J. K. Senior, A. C. Lunn, *Determination of the groups of orders* 162–215*, omitting order* 192, Amer. J. Math. **57** (1935), 254–260.

[54] R. Le Vavasseur, *Les groupes d'ordre* $16p$*, p etant un nombre premier impair*, C. R. Acad. Sci. Paris, 1899, t.129, 26–27, полное изложение в Ann. Univ. Toulouse, 1903, t.5, pp. 63–123.

[55] K. R. Biermann, *Die Mathematik und ihre Dozenten and der Berliner Universität 1810–1920*, Berlin, 1973.

[56] R. Haubisch, *Frobenius, Schur, and the Berlin algebraic tradition*, Mathematics in Berlin, Berlin, 1998, pp. 83–96.

[57] G. Gordon, *The answer is* $2^n n!$ *What's the Question?*, Amer. Math. Monthly **109** (1999), no. August–September, 636–645.

[58] И. И. Шафрановский, *История кристаллографии,* XIX *век*, Наука, Л., 1980, 324с., см. с.232.

[59] Ф. Клейн, *Лекции об икосаэдре и решении уравнений пятой степени*, Наука, М., 1989.

[60] Л. Р. Форд, *Автоморфные функции*, ОНТИ, М.–Л., 1936.

[61] Ф. Клейн, *История математики в* XIX *столетии*, Наука, М., 1989, 454с.

[62] Ф. Клейн, *Элементарная математика с точки зрения высшей, т.*I*, Арифметика, алгебра, анализ*, Наука, М., 1987, 431с.

[63] Ф. Клейн, *Элементарная математика с точки зрения высшей т.*II*, Геометрия*, Наука, М., 1987, 416с.

[64] Д. Пойа, Г. Сеге, *Задачи и теоремы из анализа, Т.*I*, Т.*II*, 3-е изд*, Наука, М., 1978, 391с., 431с.

[65] Г. Г. Харди, Д. Е. Литтлвуд, Г. Полиа, *Неравенства*, ИЛ, М., 1948, 456с.

[66] Д. Пойа, *Математика и правдоподобные рассуждения*, ИЛ, М., 1957, pp. 1–535.

[67] Д. Пойа, *Как решить задачу.*
[68] Г. Смит, *Драгоценные камни*, Мир, М., 1980, 586с.
[69] M. Senechal, *Finding the finite groups of symmetries of the sphere*, Amer. Math. Monthly (1990), no. April, 329–335.
[70] С. Дали, *50 магических секретов мастерства*, ЭКСМО-Пресс, М., 2002, 271с., 45-й секрет на с.259–260.
[71] Г. Вейль, *Избранные труды*, Наука, М., 1984, 511с..
[72] М. Г. А. Ньюмен, *Герман Вейль*, Успехи Мат. Наук. **31** (1976), no. 4, 239–250.
[73] H. S. M. Coxeter, *Regular polytopes*, Methuen, London et al., 1963.
[74] Д. Пидо, *Геометрия и искусство*, Мир, М., 1979, 332с., см. с.139.
[75] Г. Гусман, *О книге*, Книга, М., 1982, 112с.
[76] Д. Э. Кнут, *Искусство программирования. т.1, Основные алгоритмы, 3-е изд*, Вильямс, М.–СПб–Киев, 2000, 712с., см. с.49, 111.
[77] H. M. S. Coxeter, *The golden ratio, phyllotaxis and Wythoff's game*, Scripta Math. **19** (1953), 135–143.
[78] Ле Корбюзье, *Модулер*, В кн. Архитектура XX века, Прогресс, М., 1970, pp. 233–257.
[79] W. M. Kantor, *Some consequences of the classification of finite simple groups*, Contemp. Math., 1985 **45**, 159–173.
[80] Ф. Клейн, *Эрлангенская программа*, В кн. Об основаниях геометрии, Гостехиздат, М., 1956, pp. 399–434.
[81] А. Мессиа, *Квантовая механика, т.*2, Наука, М., 1979, 583с., см. с.366–368.
[82] Г. Жюлиа, *Анри Пуанкаре, его жизнь и деятельность*, В кн.: А. Пуанкаре, Избранные труды. Т. III., Наука, М., 1974, pp. 664–673.
[83] А. Пуанкаре, *О кривых, определяемых дифференциальными уравнениями*, М.–Л., 1947, 392с.
[84] А. Пуанкаре, *Лекции по небесной механике*, Наука, М., 1965, 571с.
[85] А. Пуанкаре, *Ценность науки*, СПб, 1906, 195с.
[86] А. Пуанкаре, *Наука и гипотеза*, СПб, 1906, 238с.
[87] А. Пуанкаре, *Наука и метод*, СПб, 1910, 238с.
[88] А. Пуанкаре, *Последние мысли*, Пг, 1923, 133с.
[89] А. Пуанкаре, *О науке*, Наука, М., 1983, 559с.
[90] А. Пуанкаре, *Избранные труды. Т.* I. *Новые методы небесной механики*, Наука, М., 1971, 771с.
[91] А. Пуанкаре, *Избранные труды. Т.* II. *Топология, Теория чисел*, Наука, М., 1972, 999с.
[92] А. Пуанкаре, *Избранные труды. Т.* III. *Математика, теоретическая физика*, Наука, М., 1974, 771с.
[93] Р. Пирс, *Ассоциативные алгебры*, Мир, М., 1986, 541с. см. с.462–463.
[94] Ж.-П. Серр, *Локальная теория полей классов*, в книге **[5]**, с.201–249, в особенности см. стр.201–215.
[95] Дж. Тэйт, *Глобальная теория полей классов*, в книге **[5]**, с.250–309, в особенности см. стр.287–294.
[96] R. Brauer, *Emil Artin*, Bull. Amer. Math. Soc. **73** (1967), 27–43.
[97] H. Cartan, *Emil Artin*, Abh. Math. Sem. Hamburg **28** (1965), 1–5.
[98] C. Chevalley, *Emil Artin* (1898–1962), Bull. Soc. Math. France **92** (1964), 1–10.
[99] H. Zassenhaus, *Emil Artin, his life and work*, Notre Dame J. Formal Logic **5** (1964), 1–9.

[100] *Война мышей и лягушек*, М.–Л., 1936.
[101] O. Schreier, *Abstrakte kontinuierliche Gruppen*, Abh. Math. Sem. Univ. Hamburg **4** (1925), 15–32.
[102] F. Leja, *Sur la notion du groupe abstrait topologique*, Fundamenta Math. **9** (1927), 37–44.
[103] Дж. фон Нейман, *Теория самовоспроизводящихся автоматов*.
[104] Дж. фон Нейман, О. Моргенштерн, *Теория игр и экономическое поведение*.
[105] Дж. фон Нейман, *Избранные труды по функциональному анализу. Т.* I, М., Наука, 1987, 376с.
[106] Дж. фон Нейман, *Избранные труды по функциональному анализу. Т.* II, Наука, М., 1987, 370с.
[107] А. Вейль, *Введение в теорию кэлеровых многообразий*.
[108] А. Вейль, *Основы теории чисел*.
[109] А. Вейль, *Эллиптические функции по Эйзенштейну и Кронекеру*.
[110] А. Вейль, *Адели и алгебраические группы*.
[111] Л .С .Понтрягин, *Основы комбинаторной топологии*.
[112] Л .С .Понтрягин, *Обыкновенные дифференциальные уравнения*.
[113] Л .С .Понтрягин, *Математическая теория оптимальных процессов*.
[114] Л .С .Понтрягин, *Жизнеописание Льва Семеновича Понтрягина, составленное им самим*.
[115] Ф. Петер, Г. Вейль, *О полноте примитивных представлений компактной непрерывной группы*, Успехи мат. наук **2** (1936), 144–160.
[116] A. Haar, *Der Massbegriff in der Theorie der kontinuierlichen Gruppen*, Ann. Math. **34** (1933), 147–169.
[117] Э. Картан, *Избранные труды*, МНЦМО, М., 1998, 392с.
[118] Д. Гильберт, *Основания геометрии*, ОГИЗ,, М., 1948, 491с.
[119] *Проблемы Гильберта*, Наука, М., 1969, 239с.
[120] Д. Гильберт, Р. Курант, *Методы математической физики.* I.
[121] Д. Гильберт, Р. Курант, *Методы математической физики.* II.
[122] Д. Гильберт, П. Бернайс, *Основания математики,* I. *Логические исчисления и формализация математики*, Наука, М., 1979, 557с.
[123] Д. Гильберт, П. Бернайс, *Основания математики.* II. *Теория доказательств*, Наука, М., 1982, 652с.
[124] Д. Гильберт, *Избранные труды, Т.* I, Факториал, М., 1998, 574с.
[125] Д. Гильберт, *Избранные труды, Т.* II, Факториал, М., 1998, 640с.
[126] Д. Гильберт, С. Кон-Фоссен, *Наглядная геометрия*, Наука, М., 1981, 344с.
[127] J. von Neumann, *Die Einführung analytischer Parameter in topologischen Gruppen*, Ann. Math. **34** (1933), 170–190.
[128] L. Pontrjagin, *The theory of topological commutative groups*, Ann. Math. **35** (1934), 361–388, имеется русский перевод, Успехи мат. наук, 1936, т.2, с.177–195.
[129] A. Gleason, *Groups without small subgroups*, Ann. Math. **56** (1952), no. 2, 193–212.
[130] D. Montgomery, L. Zippin, *Small subgroups in finite dimensional groups*, Ann. Math. **56** (1952), no. 2, 213–241.
[131] К. Шевалле, *Введение в теорию алгебраических функций одной переменной (1951)*.
[132] К. Шевалле, *Алгебраическая теория спиноров (1954)*.

[133] К. Шевалле, *Теория полей классов (1954).*

[134] К. Шевалле, *Основные понятия алгебры (1956).*

[135] Д. Дюге, *Теоретическая и прикладная статистика*, 1972, см. ч.II, гл. IV.

[136] Ф. Кертеси, *Введение в конечные геометрии*, 1976, см. § 1.14.

[137] В. В. Вагнер, *Обобщенные группы*, Докл. АН СССР **84** (1952), 119–1122.

[138] G. B. Preston, *Inverse semi-groups*, J. London Math. Soc. **29** (1954), 396–403.

[139] H. Brandt, *Über eine Verallgemeinerung des Gruppenbegriffes*, Math. Ann. **96** (1927), 360–366.

[140] A. Loewy, *Über abstrakt definierte Transmutationssysteme oder Mischgruppen*, J. reine angew. Math. **157** (1927), 239–254.

[141] L. Sylow, *Théorèmes sur les groupes de substitutions*, Math. Ann. **5** (1872), 584–594.

[142] N. A'Campo, M. Burger, *Réseaux arithmétiques et commensurateur d'après G. A. Margulis*, Invent. Math. **116** (1994), no. 1–3, 1–25.

[143] O. Ore, *Contributions to the theory of groups*, Duke Math. J. **5** (1939), 431–460, см. с.436.

[144] R. Schmidt, *Subgroup lattices of groups*, de Gruyter, Berlin, 1994, см. с.202.

[145] J. Thompson, W. Feit, *Solvability of groups of odd order*, Pacif. J. Math. **13** (1963), no. 3, 775–1029, lemma 8.6.

[146] J. Neubüser, *Die Untergruppenverbände der Gruppen der Ordnung* ≤ 100 *mit Ausnahme von Gruppen der Ordnungen* 64 *und* 96, Habilitationsschrift, Kiel, 1967.

[147] G. Frattini, *Intorno alla generazione dei gruppi di operazioni*, Rend. Acad. Lincei **1** (1885), 281–285.

[148] P. Diaconis, R. L. Graham, W. M. Kantor, *The mathematics of perfect shuffles*, Adv. Appl. Math. **4** (1983), 175–196.

[149] А. Ю. Ольшанский, А. Л. Шмелькин, *Бесконечные группы*, ВИНИТИ, Фундаментальные направления, Алгебра–4 (1989), М., 5–113, см. с.50–51.

[150] Ph. Hall, *On representatives of subsets*, J. London Math. Soc. **10** (1935), 26–30.

[151] М. Холл, *Комбинаторика*, М., 1970, см. гл.5, теорема 5.1.7.

[152] G. A. Miller, *On a method due to Galois*, Quart. J. Math. **41** (1910), 382–384.

[153] H. W. Chapman, *A note on the elementary theory of groups of finite order*, Messenger Math. **42** (1913), 132–134.

[154] G. Scorza, *A proposito di un teorema di Chapman*, Boll. Unione Mat. Italiana **6** (1927), 1–6.

[155] J. Alonso, *Representatives for cosets*, Amer. Math. Monthly (1972), 886–890.

[156] Б. Л. ван дер Варден, *Пробуждающаяся наука: математика древнего Египта, Вавилона и Греции*, ГИФМЛ, М., 1959, 459с.

[157] Б. Л. ван дер Варден, *Пробуждающаяся наука* II*: рождение астрономии.*

[158] O. Ore, *On coset representatives in groups*, Proc. Amer. Math. Soc. **9** (1958), 665–670, см. theorem 4.3.

[159] E. Weiss, *Coset representatives*, Portug. Math. **26** (1967), 259–260.

[160] B. L. van der Waerden, *Ein Satz über Klasseneinteilungen von endlichen Mengen*, Abh. Math. Sem. Hamburg **5** (1927), 185–188.

[161] J. L. Lagrange, *Réflexions sur la résolution algébriques des équations*, Oeuvres, vol. 3, 1771, pp. 205–421.

[162] G. Frobenius, *Über die Kongruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, J. reine angew. Math. **101** (1887), 273–299, (= Abh., II, pp. 304–330).

[163] R. Dedekind, *Zur Theorie der Ideale*, Göttingen Nachrichten, Math.-Phys. Klasse (1894), 272–277, (= Werke, II, pp. 43–48).

[164] A. Krieg, *Hecke algebras*, Mem. Amer. Math. Soc. **435** (1990).

[165] R. W. Hall, *Hecke C^*-algebras*, Penn. State Univ. (1999), 1–79, theorem 2.7.

[166] J.-B. Bost, A. Connes, *Hecke algebras, type III factors and phase transitions with spontaneous symmetry breaking in number theory*, Selecta Math. **1** (1995), 411–457.

[167] D. Tall, *To prove or not to prove*, Mathematics Reviews **1** (1991), no. 3, 29–32.

[168] R. Dedekind, *Über Gruppen, deren sämtliche Theiler Normaltheiler sind*, Math. Ann. **48** (1896), 548–561.

[169] R. Baer, *Situation der Untergruppen und Struktur der Gruppe*, Sitzubgsberichte Heidelberg. Akad. Wiss. **2** (1933), 12–17.

[170] M. O. Searcòid, *A reordering of Sylow theorems*, Amer. Math. Monthly (1987), no. February, 165–168.

[171] K. Hirsch, *On a theorem of Burnside*, Quart. J. Math. **1** (1950), 97–99.

[172] А. П. Дицман, *О р-группах*, Докл. АН СССР **15** (1937), 71–76.

[173] H. Wielandt, *Eine Verallgemeinerung der invarianten Untergruppen*, Math. Zeitschrift **45** (1939), 209–244.

[174] D. S. Robinson, *Joins of subnormal subgroups*, Ill. J. Math. **9** (1965), 144–168.

[175] I. Schur, *Über die Darstellungen der symmetrischen und alternierenden Gruppen durch gebrochenen linearen Substitutionen*, J. reine angew. Math. **132** (1911), 85–137.

[176] J. A. Gallian, *Another proof that A_5 is simple*, Amer. Math. Monthly **91** (1984), 134–135.

[177] K. H. Parshall, *A study in group theory: Leonard Eugene Dickson's Linear groups*, Math. Intelligencer **13** (1991), 7–11.

[178] K. H. Parshall, *In pursuit of the finite division algebra theorem and beyond: Joseph H. M. Wedderburn, Leonard E. Dickson, and Oswald Veblen*, Arch. Intern. Hist. Sci. **33** (1983), 274–299.

[179] R. Lipschitz, *Untersuchungen über die Summen von Quadraten*, Bonn, 1886, 147.

[180] M.-F. Vigneras, *Arithmetique des algebres des quaternions*, vol. 800, Lect. Notes Math., 1980.

[181] A. Hurwitz, *Über die Zahlentheorie der Quaternionen*, Nachrichten Ges. Wiss. Göttingen, Math.–Phys. Kl. (1896), no. 4, 313–340, (= Math. Werke, Bd. 2, Basel, 1933, S.303–330).

[182] J. Baez, *This week's finds in mathematical physics, week 198*, September 06, 2003, `http//math.ucr.edu/home/baez/week198.html`.

[183] С. В. Стахов, *Евклидовы подкольца в теле кватернионов, связанные с правильными многогранниками*, Канд. Дисс., Ленингр. Ун-т, 1985, 141.

[184] R. A. Wilson, *The geometry of Hall—Janko group as a quaternionic reflection group*, Geom. Dedic. **20** (1986), 157–173.

[185] J. A. Gallian, J. Van Buskirk, *The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$*, Amer. Math. Monthly **91** (1984), 196–197.

[186] W. von Dyck, *Gruppentheoretische Studien.*, Math. Ann. **20** (1882), 1–44.

[187] B. H. Neumann, *A two-generator group isomorphic to a proper factor group*, J. London Math. Soc. **25** (1950), 247–248.
[188] G. Higman, *A finitely related group with an isomorphic proper factor group*, J. London Math. Soc. **26** (1951), 59–61.
[189] H. K. Iyer, Rocky Mountain J. Math. **9** (1979), no. 4, 653–670.
[190] G. L. Walls, *Automorphism groups*, Amer. Math. Monthly (1986), no. June–July, 459–462, см. теорему A.
[191] Х. Минк, *Перманенты*, Мир, М., 1982, 213с., см. теорему 1.3 на с.30.
[192] G. Frobenius, *Darstellung der Gruppen durch lineare Substitutionen*, Sitzungsberichte Akad. Wiss. zu Berlin (1896), 994–1015, (= Ges. Abh.).
[193] I. Schur, *Über die Darstellung der endlichen Gruppen durch gebrochene lineare Substitutionen*, J. reine angew. Math. **127** (1904), 20–50.
[194] E. Noether, *Hyperkomplexe Grössen und Darstellungstheorie*, Math. Z. **30** (1929), 641–692.
[195] H. Maschke, *Über den arithmetischen Character der Coefficienten der Substitutionen endlicher linearer Substitutionsgruppen*, Math. Ann. **50** (1898), 482–498.
[196] G. Hamel, *Eine Basis aller Zahlen und die unstetige Lösungen der Funktionalgleichung* $f(x+y) = f(x) + f(y)$, Math. Ann. **60** (1905), 459–462.
[197] A. J. Coleman, *The greatest mathematical paper of all time*, Math. Intelligencer **11** (1989), no. 3, 29–38.
[198] H. Zassenhaus, *Zum Satz von Jordan—Hölder—Schreier*, Abh. Math. Sem. Hamburg **11** (1934), 106–108.
[199] O. Schreier, *Über den Jordan—Hölderschen Satz*, Abh. Math. Sem. Hamburg **6** (1928), 300–302.
[200] C. Jordan, *Commentaire sur Galois*, Math. Ann. **1** (1869), 141–160.
[201] O. Hölder, *Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen*, Math. Ann. **34** (1889), 26–56.
[202] L. Novy, *Origins of modern algebra*, Academia, Praha, 1973, 252pp., см. с. 206–208.
[203] К. Шеннон, *Работы по теории информации и кибернетике*, ИИЛ, М., 1963, 333–402.
[204] A. T. White, *Ringing the cosets*, Amer. Math. Monthly (1987), no. October, 721–746.
[205] А. С. Компанеец, *Симметрия в микро- и макромире*, Наука, М., 1978, 207с., см. с.25–26.
[206] Д. Кнут, *Искусство программирования. Т.* II. *Получисленные алгоритмы*, Вильямс, М.–СПб.–Киев, 2000, 828с.
[207] Д. Кнут, *Искусство программирования. Т.* III. *Сортировка и поиск*, Вильямс, М.–СПб.–Киев, 2000, 822с.
[208] D. E. Knuth, *Two notes on notation*, Amer. Math. Monthly **99** (1992), 403–422.
[209] A. E. Fekete, *Apropos two notes on notation*, Amer. Math. Monthly (1994), no. October, 771–778.
[210] C. Jordan, *Sur la limite de transitivite des groupes non alternes*, Bull. Soc. Math. France **1** (1873).
[211] M. B. Nathanson, *On the greatest order of an element of the symmetric group*, Amer. Math. Monthly **79** (1972), 500–501.
[212] W. Miller, *The maximum order of an element of a finite symmetric group*, Amer. Math. Monthly (1987), no. June–July, 497–506.

[213] N. L. Nicolas, *Ordre maximal d'un élément du groupe des permutations*, Bull. Soc. Math. France **97** (1969), 129–191.
[214] E. Landau, *Über die Maximalordnung der Permutation gegebenen Grades*, Archiv der Math. u. Phys., Ser.3 **5** (1903), 92–103.
[215] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen,*, vol. I, 2nd ed, Chelsea, N. Y., 1953, см. с. 222–229.
[216] J. Massias, *Majoration explicite de l'ordre maximum d'un élément du groupe symétrique*, Ann. Fac. Sci. Toulouse Math. **6** (1984), no. 3–4, 269–281.
[217] P. Erdös, P. Turán, *On some problems of statistical group theory*, Z. Wahrscheinlichkeitstheorie verw. Gebiete **18** (1965), 151–163.
[218] J. D. Dixon, *The probability of generating the symmetric group*, Math. Z. **110** (1969), 199–205.
[219] W. Johnson, M. Silver, *A model for permutations*, Amer. Math. Monthly (1974), no. May, 503–506.
[220] Д. Вакарелов, *Игра и математика*, Народна Просвета, София, 1986, 204с.
[221] П. Дж. Камерон, *Конечные группы подстановок и конечные простые группы*, Успехи мат. наук **38** (1983), no. 3, 135–157.
[222] J. Bertrand, *Mémoire sur le nombre de valeurs que peut prendre un fonction quand on y permute les lettres qu'elle renferme*, J. Ecole Polytechnique **30** (1845), 123–140.
[223] P. L. Tschebycheff, *Mémoire sur les nombres premiers*, J. Math. pures appl. **17** (1852), 366–390.
[224] P. Erdös, *Beweis eines Satzes von Tschebyscheff*, Acta Reg. Univ. Hungar. **5** (1932), 194–198.
[225] J. A. Serret, *Mémoire sur le nombre de valeurs que peut prendre un fonction quand on y permute les lettres qu'elle renferme*, J. Math. pures appl. 1850 **15**, 1–44.
[226] D. Livingston, A. Wagner, *Transitivity of finite permutation groups on unordered sets*, Math. Z. **90** (1965), 393–403.
[227] T. Witt, *Über Steinersche Systeme*, Abh. Math. Sem. Hamburg **12** (1938), 265–275.
[228] J. Tits, *Sur les systemes de Steiner associes aux trois "grandes" groupes de Mathieu*, Rend. Math. e Appl. **23** (1964).
[229] W. Jónsson, *On the Mathieu groups M_{22}, M_{23}, M_{24} and the uniqueness of the associated Steiner systems*, Math. Z. **125** (1972), 193–214.
[230] I. Kersten, *Ernst Witt* (1911–1991), Jahresber. Deutsch. Math. Verein. **95** (1993), no. 4, 166–180.
[231] На русском языке эта статья опубликована как глава 11 в книге Дж. Конвей, Н. Слоан, *Упаковки шаров, решетки и группы*, Т.I, М. Мир, 1990 413с., см. с.374–410.
[232] O. Hölder, *Bildung zusammengesetzter Gruppen*, Math. Ann. **46** (1895), 321–422.
[233] H. A. Bender, *A new method for the determination of the group of isomorphisms of the symmetric group of degree n*, Amer. Math. Monthly **31** (1924), 287–289.
[234] E. Witt, *Die 5-transitiven Gruppen von Mathieu*, Abh. Math. Sem. Univ. Hamburg **12** (1938), 256–264.
[235] D. W. Miller, *On a theorem of Hölder*, Amer. Math. Monthly **65** (1958), 252–254.
[236] G. Janusz, J. J. Rotman, *Outer automorphisms of S_6*, Amer. Math. Monthly **89** (1982), 407–410.

[237] T. A. Fournelle, *Symmetries of the cube and outer automorphisms of S_6*, Amer. Math. Monthly (1993), no. April, 377–380.
[238] T. Y. Lam, D. B. Leep, *Combinatorial structure of the automorphisms of S_6*, Expositio Math. (1993).
[239] R. E. Solazzi, *Four-dimensional symplectic groups*, J. Algebra **49** (1977), no. 1, 225–237.
[240] В. Н. Сачков, *Комбинаторные методы дискретной математики*, Наука, М., 1977, 319с.
[241] Н. Дж. Де Брейн, *Теория перечисления Пойа*, В кн.: Прикладная комбинаторная математика, Мир, М., 1968, pp. 61–106.
[242] P. Neumann, *A lemma that is not Burnside's*, Math. Scientist **4** (1979), 133–141.
[243] G. C. Smith, *Introductory mathematics: algebra and analysis*, Springer SUMS, London et al., 1998 Supplement: `http://www.math.bath.ac.uk/~masgcs/book1/`.
[244] Н. К. Верещагин, А. Шень, *Начала теории множеств*, МЦНМО, М., 1999, 127с.
[245] G. F. Frobenius, L. Stickelberger, *Über Gruppen von vertauschbaren Elementen*, J. reine angew. Math. **86** (1879), 217–262.
[246] T. Szele, *Ein Analogon der Körpertheorie für abelsche Gruppen*, J. reine angew. Math. **188** (1950), 167–192.
[247] R. Baer, *Abelian groups without elements of finite order*, Duke Math. J. **3** (1937), 68–122.
[248] E. Specker, *Additive Gruppen von Folgen ganzer Zahlen*, Portug. Math. **9** (1950), 131–140.
[249] S. MacLane, *Duality for groups*, Bull. Amer. Math. Soc. **56** (1950), 485–516.
[250] E. Schering, *Die Fundamental-Classen der zusammengesetzbaren arithmetischen Formen*, Abh. Ges. Wiss. Göttingen **14** (1869), 3–13.
[251] L. Kronecker, *Auseinandersetzungen einiger Eigenschaften der Klassenzahl idealer complexer Zahlen*, Monatsberichte Akad. Wiss. Berlin (1870), 881–889, (= Werke, Bd. I, S.271–282).
[252] H. Prüfer, *Untersuchungen über die Zerlegbarkeit der abzählbaren primären abelschen Gruppen*, Math. Z. **17** (1923), 35–61.
[253] R. Baer, *Der Kern, eine charakteristische Untergruppe*, Compositio Math. **1** (1934), 254–283.
[254] Л. Я. Куликов, *К теории абелевых групп произвольной мощности.* I, II, Матем. сб. **9** (1941), 165–182; **16** (1945), 129–162.
[255] Э. Артин, *Теория Галуа*, МНЦМО, М., 2004, 66с., см. с.41–43.
[256] H. J. S. Smith, *On systems of linear indeterminate equations and congruences*, Phil. Trans. Cambridge Math. Soc. (1861), (= Collected Works, vol. I, Oxford, 1964, pp. 367–387).
[257] R. Baer, *Abelian groups that are direct summands of every containing abelian group*, Bull. Amer. Math. Soc. **46** (1940), 800–806.
[258] А. И. Мальцева, *Группы и другие алгебраические системы*, В кн. Математика, ее содержание, методы и значение, vol. 3, Изд-во АН СССР, М., 1956, pp. 248–331.
[259] Ж.-П. Серр, *Деревья, амальгамы и* SL_2, Математика, Сб. Перев. **18** (1974), no. 1, 3–51; no. 2, 3–27.

Apparatus

Ein Buch ohne Index ist kein Buch.

Mommsen

Однажды Будда пребывал в Раджагрихе на горе Гридхракуте с большим собранием великих бхикшу числом в двенадцать тысяч. Там же присутствовало восемьдесят тысяч бодхисаттв-махасаттв, были боги, драконы, якши, гандхарвы, асуры, гаруды, киннары и махараги, а также бхикшу, бхикшуни, упасаки и упасики. Там были великие вращающие колесо цари, малые вращающие колесо цари, цари золотого колеса, цари серебряного колеса и цари других колес; затем, были цари, принцы, министры и простые люди, мужчины и женщины, а также обладатели больших богатств — каждый в окружении сотен тысяч мириадов последователей.

Сутра неисчислимых смыслов

Index rerum

От гавайских гитар до гаванских сигар.

Венедикт Ерофеев. *Из записных книжек*

Халатное, поверхностное знакомство с митьковской лексикой приводит к быстрому искажению и, в конечном итоге, вырождению смысла цитат и выражений.

Владимир Шинкарев. *Митьки*, часть 8

Index personae

От сиамских близнецов до сионских мудрецов.

Венедикт Ерофеев. *Из записных книжек*

Основные обозначения

You might think the notation `curly B` is set up to be `balls`.

Miles Reid

Логические символы

??
$\vee$ — дизъюнкция (vel) ??
$\wedge$ — (а также &) конъюнкция ??
$\neg$ — негация ??
$\Longrightarrow$ — импликация ??
$\Longleftrightarrow$ — эквиваленция или логическая эквивалентность ??
$\forall$ — квантор всеобщности (Allgemeinheit, for All) ??
$\exists$ — квантор существования (Existenz, Exists) ??
$\exists!$ — ‘существует единственный’. ??
`True` — истина ??
`False` — ложь

Теоретико-множественные символы

??
$\in$ — знак принадлежности ??
$\notin$ — отрицание принадлежности ??
$\ni$ — то же, $A \ni a$??
$\subseteq$ — знак включения $A \subseteq B$??
$\supseteq$ — то же, $B \supseteq A$??
$\subset$ — знак строгого включения $A \subset B$??
$\supset$ — то же, $B \supset A$??
$\varnothing$ — пустое множество ??
$\{a, b, c, \dots\}$ — класс с элементами $a, b, c, \dots$??
$\{x \in A \mid P(x)\}$ — множество элементов из A, обладающих свойством P ??
$[a, a, b]$ — набор (мультимножество ??
(a, b, a) — тупель (упорядоченная n-ка) ??
$\Lambda = ()$ — нулька (пустой тупель) ??
$|X| = \mathrm{Card}(X)$ — мощность множества X ??
$\aleph_0$ — счетная мощность ??
2^X — множество подмножеств множества X ??
$\bigwedge(X)$ — множество конечных подмножеств множества X ??
$\bigwedge^m(X)$ — m-я внешняя степень множества X (множество m-элементных подмножеств в X) ??
$\cup$ — объединение ??
$\cap$ — пересечение ??
$\setminus$ — теоретико-множественная разность ??
$\triangle$ — симметрическая разность (булева сумма) ??
$\sqcup$ — дизъюнктное объединение (копроизведение множеств) ??
$\coprod$ — дизъюнктное объединение семейства множеств ??
$\times$ — декартово произведение (произведение множеств) ??

$\prod$ — декартово (= прямое) произведение семейства множеств ??
$\sim$ или $\approx$ — отношение эквивалентности ??
$X/\sim$ — фактор-множество множества X по отношению эквивалентности $\sim$

Комбинаторика

?? $\binom{n}{m} = C_n^m = |\bigwedge^m(\underline{n})|$ — биномиальный коэффициент ??
D_n — количество беспорядков на n символах ??
$\begin{bmatrix} n \\ m \end{bmatrix}$ — число Стирлинга первого рода ??
$\left\{ {n \atop m} \right\} = S_{nm} = S(n,m)$ — число Стирлинга второго рода ??
$n!$ — факториал ??
$[x]_n = x(x+1)\dots(x+n-1)$ — возрастающий факториал ??
$[x]_n = x(x-1)\dots(x-n+1)$ — убывающий факториал ??
δ_{ij} — дельта Кронекера

Теоретико-числовые символы

?? $|$ — делимость ??
$\|$ — точная делимость ($m \parallel n$ означает, что $m|n \ \ \& \ \ m \perp n/m$) ??
$\equiv$ — сравнение по модулю ??
mod — модуль сравнения ??
$\perp$ — взаимная простота ??
gcd — наибольший общий делитель ??
lcm — наименьшее общее кратное ??
v_p — p-адический показатель ??
$|\ |_p$ — p-адическое нормирование, $|x|_p = p^{-v_p(x)}$??
d_p — p-адическая метрика ??
φ — функция Эйлера ??
$\lfloor x \rfloor$ — целая часть x

Числовые системы

?? $\mathbb{A}$ — целые алгебраические числа ??
$\mathbb{B}^n$ — открытый n-мерный единичный шар ??
$\overline{\mathbb{B}}^n$ — замкнутый n-мерный единичный шар ??
$\mathbb{C}$ — комплексные числа ??
$\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ — сфера Римана ??
$\mathbb{F}_q$ — конечное поле из q элементов ??
$\mathbb{I} = [0,1]$ — единичный отрезок ??
$\mathbb{H}$ — классические (alias гамильтоновы) кватернионы ??
$\mathbb{H}^n$ — n-мерное гиперболическое пространство ??
$\mathbb{N} = \{1,2,3,\dots\}$ — натуральные числа ??
$\mathbb{N}_0 = \{0,1,2,3,\dots\}$ — натуральные числа и 0 ??
$\mathbb{O}$ — октавы Кэли ??

$\mathbb{P} = \{2, 3, 5, 7, 11, \dots\}$ — рациональные простые ??
$\mathbb{Q} = \{m/n \mid m, n \in \mathbb{Z}, n \neq 0\}$ — рациональные числа ??
$\overline{\mathbb{Q}}$ — алгебраические числа ??
$\mathbb{Q}_+ = \mathbb{Q}_{>0} = \{x \in \mathbb{Q} \mid x > 0\}$ — положительные рациональные числа ??
$\mathbb{R}$ — вещественные (alias действительные) числа ??
$\mathbb{R}_+ = \mathbb{R}_{>0} = (0, +\infty)$ — положительные вещественные числа ??
$\mathbb{S}^n$ — n-мерная единичная сфера, $\mathbb{S}^1 = \mathbb{T}$??
$\mathbb{T} = \mathbb{R}/\mathbb{Z}$ — комплексные числа модуля 1 (alias ‘единичная окружность’) ??
$\mathbb{T}^n$ — вещественный (компактный) тор ??
$\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ — целые числа ??
$\mathbb{Z}/m\mathbb{Z}$ — кольцо классов вычетов по модулю m ??
$\mathbb{Z}_p$ — целые p-адические числа ??
$\mathbb{Z}[i]$ — кольцо целых Гауссовых чисел ??
$\mathbb{Z}[\omega]$ — кольцо целых Эйзенштейновых чисел ??
Hurw — кольцо целых гурвицевых кватернионов ??
Icos — кольцо икосианов ??
Lip — кольцо целых липшицевых кватернионов ??
$\underline{n} = \{1, \dots, n\}$ — начальный отрезок натурального ряда длины n ??
μ_n — группа корней n-й степени из 1 ??
μ_{p^∞} — группа корней степени p^n из 1 (квазициклическая группа)

Индивидуальные числа

??
i — мнимая единица (как элемент $\mathbb{C}$ или $\mathbb{H}$) ??
j, k — кватернионные единицы (как элементы $\mathbb{H}$) ??
ζ_n — первообразный корень степени n из 1 ??
$\sigma = \dfrac{1 - \sqrt{5}}{2} = \tau^{-1}$??
$\tau = \dfrac{1 + \sqrt{5}}{2}$ — золотое сечение ??
$\varphi = \tau$ — число Фидия (другое название τ) ??
$\widehat{\varphi} = \sigma$ — другое название σ ??
$\omega = \dfrac{1 + i\sqrt{3}}{2}$ — первообразный кубический корень из 1 ??
$\omega = \dfrac{1}{2}(-1 + i + j + k)$ — то же, иным манером

Функциональные символы

??
id или id_X — тождественное отображение ??
incl — вложение ??
pr — проекция (обычно проекция на сомножители) ??
π — проекция (обычно проекция на фактор-множество) ??
res или res^X_Y — ограничение отображения с X на множество Y ??
$|_Y$ — ограничение на подмножество Y, то же, что res^X_Y ??
$\longrightarrow$ — отображение множеств или гомоморфизм групп ??
$\mapsto$ — образ индивидуального элемента при отображении или гомоморфизме ??

Групповая символика: элементы

Групповая символика: подгруппы

*Или, как говорит РШ, изоморфность.

H_G — сердцевина группы H (наибольшая нормальная подгруппа в G, содержащаяся в H) ??
$H \trianglelefteq\trianglelefteq G$ — H субнормальная подгруппа в G ??
gH — правый смежный класс G по H ??
Hg — левый смежный класс G по H ??
FgH — смежный класс G по двойному модулю (F, H) ??
G/H — множество правых смежных классов G по H, фактор-группа ??
$H\backslash G$ — множество левых смежных классов G по H ??
$F\backslash G/H$ — множество двойных смежных классов G по (F, H), ??
$W(X)$ — множество полугрупповых слов в алфавите X ??
$l(w)$ — длина слова w ??
$\rho(w)$ — редуцированное слово эквивалентное w ??
$\langle X\rangle$ — подгруппа, порожденная подмножеством X ??
$\langle X\rangle^G$ — нормальная подгруппа G, порожденная подмножеством X ??
$\langle X|R\rangle$ — группа, порожденная множеством образующих X с определяющим множеством соотношений R ??
$\eqcirc$ — буквальное равенство (равенство групповых слов рассматриваемых как полугрупповые слова) ??
$|G : H|$ — индекс подгруппы H в группе G

Части группы

??
$C(G)$ — центр группы G ??
$C_i(G)$ — i-й член центрального ряда группы G ??
$C^i(G)$ — i-й гиперцентр группы G ??
$C_G(x)$ — централизатор элемента x группы G ??
$\mathrm{Comm}_G(H)$ — соизмеритель подгруппы H в G ??
$D(G) = [G, G]$ — коммутант группы G ??
$D_i(G)$ — i-й член ряда коммутантов группы G ??
$F(G)$ — подгруппа Фиттинга группы G ??
G^{ab} — абелианизация группы G ??
$G^n = \mathrm{Im}(\mathrm{pow}_n)$ — множество n-х степеней в G ??
$G_n = \mathrm{Ker}(\mathrm{pow}_n)$ — множество решений уравнения $x^n = 1$ в G ??
$L(G)$ — решетка подгрупп группы G ??
$L(D, G)$ — решетка промежуточных подгрупп H, $D \leq H \leq G$??
$N_G(X)$ — нормализатор подмножества X в G ??
$S_p(G)$ — силовская p-подгруппа группы G ??
$\mathrm{Syl}_p(G)$ — множество всех силовских p-подгрупп группы G ??
$\Theta(G)$ — структурная решетка группы G (состоящая из всех нормальных делителей группы G) ??
$\Phi(G)$ — подгруппа Фраттини группы G

Гомоморфизмы групп

??
$\mathrm{Aut}(G)$ — группа автоморфизмов G ??
$\mathrm{Aut}_n(G)$ — итерированная группа автоморфизмов G ??

Действия групп

Алгебраические системы

Линейная алгебра

Основные примеры групп

Симметрическая группа

Системы корней и группы симметрий

Кристаллография

Конструкции над группами

$*_F$ — амальгамированное произведение: $H *_F G$ амальгама групп H и G с объединенной подгруппой F ??
$\varinjlim$ — индуктивный (прямой) предел групп ??
$\varprojlim$ — проективный (обратный) предел групп

Абелевы группы

??
$A(p)$ — p-примарная компонента ??
$B(A)$ — группа границ ??
$D(A)$ — делимая часть ??
$H(A) = Z(A)/B(A)$ — группа гомологий ??
$T(A)$ — подгруппа кручения ??
$U(A)$ — ульмова подгруппа ??
$Z(A)$ — группа циклов

Группы типа Ли

??
$A_l(q) = \mathrm{PSL}(l+1, q)$ — ??
$B_l(q) = \mathrm{P\Omega}(2l+1, q)$ — ??
$C_l(q) = \mathrm{PSp}(2l, q)$ — ??
$D_l(q) = \mathrm{P\Omega}^+(2l, q)$ — ??
${}^2A_l(q^2) = \mathrm{PSU}(l+1, q^2)$ — ??
${}^2D_l(q^2) = \mathrm{P\Omega}^-(2l, q^2)$ — ??
$E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$ — исключительные группы Шевалле типов E_6, E_7, E_8, F_4, G_2 ??
${}^3D_4(q)$, ${}^2E_6(q^2)$ — скрученные группы Шевалле ??
${}^2B_2 = \mathrm{Sz}$ — группы Судзуки ??
${}^2F_4$, ${}^2G_2$ — группы Ри

Классические группы

??
$\mathrm{Aff}(n, R)$ — аффинная группа ??
$\mathrm{Cliff}(n, R)$ — группа Клиффорда ??
$\mathrm{GL}(n, R)$ — полная линейная группа ??
$\mathrm{GO}(n, R)$ — полная ортогональная группа ??
$\mathrm{GSp}(n, R)$ — полная симплектическая группа ??
$O(n, R)$ — ортогональная группа ??
$\mathrm{PGL}(n, R)$ — проективная группа ??
$\mathrm{PSL}(n, R)$ — специальная проективная группа ??
$\mathrm{PSO}(n, R)$ — проективная специальная ортогональная группа ??
$\mathrm{PSU}(n, R)$ — проективная специальная унитарная группа ??
$\mathrm{P\Omega}(n, R)$ — ??
$\mathrm{PSp}(n, R)$ — проективная симплектическая группа ??
$\mathrm{SL}(n, R)$ — специальная линейная группа ??
$\mathrm{SL}^{\pm}(n, R) = \{g \in \mathrm{GL}(n, R) \mid \det(g) = \pm 1\}$??

$\mathrm{SO}(n,R)$ — специальная ортогональная группа ??
$\mathrm{Sp}(n,R)$ — симплектическая группа ??
$\mathrm{Spin}(n,R)$ — спинорная группа ??
$\mathrm{St}(n,R)$ — группа Стейнберга ??
$\mathrm{SU}(n,R)$ — специальная унитарная группа ??
$T(V)$ — группа трансляций ??
$U(n,R)$ — унитарная группа ??
$\Omega(n,R)$ — ядро спинорной нормы ??
$\mathcal{L}$ — группа Лоренца ??
$\mathcal{L}_{\uparrow}$ — ортохронная группа Лоренца ??
$\mathcal{L}_{+\uparrow}$ — собственная группа Лоренца ??
$\mathcal{L}_{+}$ — специальная группа Лоренца ??
$\mathcal{P}$ — группа Пуанкаре ??
$\Gamma\mathrm{L}(n,R)$ — группа коллинеаций ??
$\{g|u\}$ — символ Зейтца ??
$[g]$ — класс матрицы g в проективной группе

Подгруппы $\mathrm{GL}(n,R)$

??
$B(n,R)$ — верхняя треугольная группа (Borel) ??
$B^{-}(n,R)$ — нижняя треугольная группа ??
$B(\nu,R)$ — группа верхних клеточно-треугольных матриц ??
$B^{-}(\nu,R)$ — группа нижних клеточно-треугольных матриц ??
$C(n,R)$ — множество скалярных матриц ??
$C(n,R,I)$ — полная конгруэнц-подгруппа уровня I ??
$D(n,R)$ — диагональная группа ??
$D(\nu,R)$ — группа клеточно-диагональных матриц ??
$E(n,R)$ — элементарная группа ??
$E(\nu,R)$ — элементарная клеточно-диагональная группа ??
$E(n,R,I)$ — относительная элементарная группа ??
$F(n,R,I) = E(n,I)$ — элементарная группа идеала I, рассматриваемого как кольцо без единицы уровня I ??
$\mathrm{EO}(n,R)$ — элементарная ортогональная группа ??
$\mathrm{Ep}(n,R)$ — элементарная симплектическая группа ??
$\mathrm{EU}(n,R)$ — элементарная унитарная группа ??
$\mathrm{GL}(n,R,I)$ — `Hauptkongruenzuntergruppe`, главная конгруэнц-подгруппа уровня I ??
$N(n,R)$ — группа мономиальных матриц (torus normaliser) ??
$N(\nu,R)$ — группа клеточно-мономиальных матриц ??
$\mathrm{SC}(n,R)$ — группа скалярных матриц с определителем 1 ??
$\mathrm{SL}(n,R,I)$ — `Hauptkongruenzuntergruppe`, главная конгруэнц-подгруппа уровня I в $\mathrm{SL}(n,R)$??
$U(n,R)$ — верхняя унитреугольная группа ??
$U^{-}(n,R)$ — нижняя унитреугольная группа ??
W_n — группа матриц перестановки (изоморфная S_n)

Группы в алгебре и топологии

Спорадические группы

Автор этой книги Николай Вавилов профессор кафедры высшей алгебры и теории чисел СПбГУ. Он родился в Санкт-Петербурге в год дракона в семье ученых. Его мама, Наталия Николаевна занималась физикой, а отец Александр Александрович был известным специалистом в области теории управления. После окончания в 1969 году 30-й школы он поступил на математико-механический факультет СПбГУ, с которым связана вся его дальнейшая карьера.

Основные научные интересы Вавилова относятся к теории алгебраических групп и групп типа Ли, теории представлений, алгебраической K-теории, теории алгебр Ли, группам и геометриям, теории ассоциативных колец, полилинейной алгебре, компьютерной алгебре. На эти темы он опубликовал более 100 статей в ведущих российских и международных журналах, выступал с сотнями докладов в университетах и на конференциях.

Много лет Вавилов работал за границей, дольше всего в Германии (больше пяти лет), Италии (больше трех лет), Польше, США, Великобритании, Греции, Китае, Бельгии и Израиле, а также профессионально посещал другие страны. Он прочел десятки курсов в Notre Dame, Northwestern, Университетах Милана и Падуи, Университете Крита, SISSA, Харбинском технологическом институте и других университетах.

Кроме родного Невского диалекта в двух вариантах (полунормативный великорусский и креативная василеостровская квеля) он преподает, пишет и смотрит сны на итальянском, немецком, английском и польском, и, сверх того, читает и пытается говорить еще на двух десятках европейских и азиатских языков (иногда до некоторой степени понимая смысл прочитанного/сказанного).

Помимо алгебры и геометрии он профессионально занимается научными вычислениями, преподаванием и сочинительством, а также серьезно интересуется другими разделами математики, классической и этнической музыкой, всеми видами изобразительных искусств, всем, что связано с языком и письмом, лингвистикой, физикой, химией, биологией, техникой, историей науки, китайской философией (он практикующий даосист), медиевистикой, средиземноморской и восточной кухней, энологией, путешествиями, всеми видами игр и головоломок — и многим другим.

Его жена Ольга преподает физику в Политехническом университете, а сын Александр — студент СПбГУ.