КОНКРЕТНАЯ ТЕОРИЯ ГРУПП

FIRST DRAUGHT

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. От мечты к открытию

---

[1]И.Ф.Стравинский, О музыкальном феномене. – В кн. Статьи и материалы, Советский композитор, М., 1973, с.1–527 (стр. 24).

[2]Р.Фейнман, Р.Лейман, М.Сэндс, Фейнмановские лекции по физике, т. 3. Излучение, волны, кванты 1967, Мир, М., с.1–238 (стр. 9).

[3]П.Тейяр де Шарден, Феномен человека: преджизнь, жизнь, мысль, сверхжизнь. 1987, Наука, М., с.1–240 (стр. 38)

Оглавление

7. Линейные группы

§ 1. Полная линейная группа
§ 2. Линейные группы над конечным полем
§ 3. Некоторые важнейшие подгруппы
§ 4. Блочные подгруппы
§ 5. Элементарные трансвекции
§ 6. Псевдоотражения
§ 7. Матрицы перестановки
§ 8. Трансвекции
§ 9. Соотношения между элементарными трансвекциями
§ 10. Корневые полупростые элементы
§ 11. Гомоморфизм редукции
§ 6. Элементарная группа
§ 8. Нормальность элементарной группы
§ 9. Группа Стейнберга??
§ 10. Конгруэнц-подгруппы
§ 11. Относительная элементарная группа
§ 12. Нормальные подгруппы $\mathrm{GL}(n, R)$
§ 13. Теорема Жордана-Диксона
§ 14. Определитель Дьедонне
§ 15. Автоморфизмы $\mathrm{GL}(n, R)$
§ 16. Разложение Брюа
§ 17. Разложение Гаусса
§ 18. Параболические подгруппы
§ 19. Неприводимые линейные группы
§ 20. Примитивные линейные группы
§ 21. Классические группы???
§ 22. Теорема Клиффорда
§ 23. Теорема Маклафлина

8. Абелевы группы

§ 1. Свободные абелевы группы
§ 2. Подгруппа кручения
§ 3. Примарное разложение
§ 4. Разложение на циклические слагаемые
§ 5. Подгруппы свободной группы

9. Конечные группы

§ 1. Центр p-группы, существование элемента порядка p, нормализаторное условие
§ 2. Принцип инволюций
§ 3. Количество подгрупп p-группы
§ 4. Решения уравнения $x^n = e$, теоремы Коши и Фробениуса
§ 5. Теоремы Силова
§ 6. Доказательство Виландта
§ 7. Нормализатор силовской подгруппы
§ 8. Силовские подгруппы в S_n
§ 9. Группы порядка pq, метациклические группы
§ 10. Группы порядка p^3, экстраспециальные группы

Was sind und was sollen die Gruppen

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

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 gotischen Architektur trifft man sogar komplizierte Raumgruppen[4].

Andreas Speiser[5], [Sp], S.1–2.

В настоящей главе мы начинаем изучение первой из фундаментальных классических структур алгебры – групп. Важность понятия группы для математики в целом 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: **теория чисел**, **теория алгебраических уравнений** и **геометрия**. Сам термин группа впервые ввел в 1830 году Эварист Галуа[6]. Этот термин происходит от 'grouper les permutations' – 'группировать перестановки'. В качестве типично Шпенглеровского совпадения отметим, что в том же самом 1830 году, когда

[4]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.

[5]**Шпайзер Андреас** (10.06.1885, Базель — 1970) — швейцарский алгебраист, основные работы которого относятся к теории групп и ее геометрическим приложениям и истории математики.

[6]**Эварист Галуа** (25.10.1811–31.05.1832) – 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. 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 группы, поля, нормальной подгруппы, простой и разрешимой группы, etc. Много важнейших понятий алгебры названы в его честь: теория Галуа, группа Галуа, поля Галуа, соответствие Галуа, когомологии Галуа. 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. 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 1846 году Лиувиллем, а широкое признание получили только в 1870-х годах.

Галуа впервые употребил термин ‘группа’, Гессель осуществил вывод 32 кристаллографических классов.

Однако я склонен верить, что в действительности понятие группы является **древнейшим** математическим понятием, более древним, чем понятие числа, и неотделимым от самой человеческой цивилизации. Группы появляются **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. Именно на этом основана 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, ...

Астральный план

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[7]

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'

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'[8]

[7] В.Феллер, Введение в теорию вероятностей и ее приложения, т.1, 1967, Мир, М., с.1–498.

[8] 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'.

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 контраст, аналогия и метафора. 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.

Пригоршня философем

> 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[9] 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** $\mathrm{GL}(n, K)$.

[9]**Софус Ли** (17.12.1842, Nordfjordeid (поселок недалеко от Бергена) – 18.02.1899, Кристиания (ныне Осло)) – замечательный норвежский математик, основатель теории групп и алгебр Ли. 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. В 1869–1870 годах получил стипендию для стажировки в Берлине и Париже, где близко подружился с Клейном. Во время этой поездки он 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. В 1872–1886 и 1898–1899 годах был профессором университета в Кристиании, а в 1886–1898 годах – в Лейпциге. В нашем курсе упоминаются алгебры Ли, скобка Ли, группы Ли, теория Ли и несколько теорем Ли.

• 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** [tD], [Hus].

• Центральным объектом **всей** математики XX века является понятие группы **с дополнительной структурой**: топологические группы, вещественные и комплексные группы Ли, алгебраические группы[10], p-адические аналитические группы, проконечные группы, адельные группы, etc. A *topological group* is perhaps **the** most important concept in modern Mathematics ([Mau], стр.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!)

• 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**[11]. 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

[10] Я помню свое удивление, когда первый раз увидел выражение 'алгебраические группы' – по наивности я тогда считал, что алгебраические группы это *абстрактные* группы. В действительности, алгебраическая группа, это группа, которая одновременно является алгебраическим многообразием, причем отображения, определяющие структуру группы, являются морфизмами многообразий.

[11] С точки зрения **теории моделей** порядок и размерность – это одно и то же, и то и другое являются частными случаями **ранга Морли**, см. Справочная книга по математической логике, Часть I, теория моделей, Наука, М, 1982, с.1–391.

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 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[12] 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 упоминается формулировка теоремы классификации, 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

[12]У.Фейт, Некоторые следствия классификации конечных простых групп, – Успехи Мат. Наук, 1983, т.38, N.2, с.127–133.

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**[13] **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. Это позволяет проиллюстрировать такие понятия как нормальный делитель, фактор-группа, расширения, сопряженность, когомологии на настоящих, а не учебных примерах.

[13]Существенно, что именно *рекапитуляцией*, а не *повторением*, как иногда переводят.

Напоминания из главы I

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*[14] 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** (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**.

[14] Имеется, впрочем, и исключения: сложение ординалов и некоторые экзотические примеры. ∎

Учебники по алгебре

Ниже упоминаются только тексты общего характера на русском языке. Дополнительная литература к отдельным главам указана в соответствующих местах курса.

[Ba1] Ю.А.Бахтурин, *Основные структуры современной алгебры*, Наука, М., 1990, pp. 1–318.

[BB] Г.Биркгоф, Т.Барти, *Современная прикладная алгебра*, Мир, М., 1976.

[B1] Н.Бурбаки, *Алгебра, Гл.* I – III. *Алгебраические структуры, линейная и полилинейная алгебра*, Наука, М., 1962, pp. 1–516.

[B2] Н.Бурбаки, *Алгебра, Гл.* IV – VI. *Многочлены и поля, упорядоченные группы*, Наука, М., 1965, pp. 1–300.

[B3] Н.Бурбаки, *Алгебра, Гл.* VII – IX. *Модули, кольца, формы*, Наука, М., 1966, pp. 1–555.

[Wae] Б.Л. ван дер Варден, *Алгебра*, Наука, М., 1976, pp. 1–648.

[Vi1] Э.Б.Винберг, *Начала алгебры*, УРСС, М., 1998, pp. 1–191.

[Vi2] Э.Б.Винберг, *Курс алгебры*, Наука, М., 1999, pp. 1–527.

[Ka1] Л.А.Калужнин, *Введение в общую алгебру*, Наука, М., 1973.

[K1] А.И.Кострикин, *Введение в алгебру*, Наука, М., 1977, pp. 1–495.

[K2] А.И.Кострикин, *Введение в алгебру,* I. *Основы алгебры*, Физматлит, М., 2000.

[K3] А.И.Кострикин, *Введение в алгебру,* III. *Основные структуры алгебры*, Физматлит, М., 2000, pp. 1–271.

[KM] А.И.Кострикин, Ю.И.Манин, *Линейная алгебра и геометрия, 2е изд.*, 1986, pp. 1–303.

[L1] С.Ленг, *Алгебра*, Мир, М., 1968, pp. 1–564.

[LP] Р.Лидл, Г.Пильц, *Прикладная абстрактная алгебра*, Изд-во Уральского Унив., Екатиренбург, 1996.

[LSh] П.Ноден, К.Китте, *Алгебраическая алгоритмика*, Мир, М., 1999.

[OA1] *Общая алгебра: группы, кольца и модули*, Наука, М., 1990, pp. 1–590.

[OA2] *Общая алгебра: полугруппы, решетки, универсальные алгебры, категории*, Наука, М., 1991, pp. 1–479.

[Sk1] Л.А.Скорняков, *Элементы алгебры*, Наука, М., 1981, pp. 1–243.

[Sk2] Л.А.Скорняков, *Элементы общей алгебры*, Наука, М., 1983, pp. 1–272.

[F1] Д.К.Фаддеев, *Лекции по алгебре*, Наука, М., 1984, pp. 1–416.

[Fai] К.Фейс, *Алгебра: кольца, модули, категории.* Т. 1, 1977, pp. 1–676.

[Sh] И.Р.Шафаревич, *Основные понятия алгебры*, R. & C. Dynamics, Ижевск, 1999, pp. 1–347.

Теория групп: путеводитель по литературе

1. Учебники по теории групп. Среди огромного количества книг, целиком или частично посвященных теории групп или ее приложениям, только четыре, а именно [KaM], [Kur], [Ha], [Sch] 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 [Ha]. Конечно, книга Холла несколько устарела, в частности, это касается терминологии. Написанная в 1916 году книга [Sch] является выдающимся памятником истории нашей науки, но не дает представления о состоянии предмета в 1930-е годы[15]. Книга Куроша [Kur] не содержит ничего[16], что могло бы быть полезным студентам или математикам неспециалистам[17], и совсем немного того, что могло бы быть полезным профессиональному алгебраисту[18]. Книга Каргаполова – Мерзлякова [KaM] написана несколько 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 введение в теорию групп можно рекомендовать замечательную книгу Олега Богопольского [Bog]. Несмотря на небольшой объем она дает очень ясное и достаточно продвинутое изложение нескольких ключевых тем как в теории конечных групп, так и в комбинаторной и геометрической теории групп.

Из текстов общего характера можно упомянуть еще популярные книги [Al], [Ale], [GM], [KS] и сборник задач [LAL]. Все цитированные во введении учебники алгебры содержат главу или две, посвященные теории групп и/или теории представлений. Я особенно призываю прочитать §§ 12–18 книги [Sh], которые представляют собой введение в *содержательную* теорию групп для начинающих и неспециалистов. Два изложения теории групп с точки зрения потребностей инженеров приведены в [Sm] и [Go]. Изложение в учебнике В.И.Смирнова [Sm] 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. Изложение теории групп в [Go] достаточно стандартно, но и сегодня смотрится неплохо.

2. Отдельные аспекты теории групп. Книга Фукса [Fu2] 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.

---

[15]Кроме того, в [Sch] 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!

[16]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*", [Kur], 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'.

[17]С этой точки зрения чрезвычайно поучительно сравнить книгу Куроша с написанной примерно в то же время статьей А.И.Мальцева, Группы и другие алгебраические системы. – В кн. Математика, ее содержание, методы и значение, Изд-во АН СССР, М., 1956, т.3, с.248–331. Невозможно не отметить, насколько более широкую и детальную панораму теории групп рисует Анатолий Иванович, в частности, все содержание книги [Kur] изложено там на страницах 301–302.

[18]Оба содержательных результата книги Куроша, теоремы Куроша и Грушко, значительно лучше изложены в книгах Масси [MS] и Серра [S4]. Имеется частичный русский перевод: Ж.-П.Серр, Деревья, амальгамы и SL_2. – Математика, Сб. Перев., 1974, т.18, N.1, с.3–51; N.2, с.3–27.

Имеется несколько весьма содержательных и полезных книг, посвященных отдельным аспектам теории групп:

• теория конечных групп [Vy], [Go], [Kon], [L3], [Suz];

• теория представлений конечных групп [BF], [Vin], [Ja], [tD], [CR], [Mur], [Na1], [S3], [Fe], [F], [Hen];

• комбинаторная теория групп [Adi], [B7], [Gro], [CF], [CM], [K4], [LSh], [MKS], [Neu], [Ol], [ChM];

• когомологии групп [Alg], [Br], [CE], [Mac], [S1].

Как мы уже упоминали, центральным объектом математики XX века были группы с дополнительными структурами: группы Ли, топологические группы, алгебраические группы, etc. Вот некоторые книги, посвященные группам с дополнительными структурами и наиболее важным конкретным группам:

• группы Ли [Ada], [AGH], [B6], [B8], [VO], [Pos], [Rag], [S2], [Che], [Ch];

• представления групп Ли [BR], [Zh], [ZhSh], [Kir], [Na1];

• топологические группы [B4], [B5], [We], [Gui], [Grn], [Kp2], [Kir], [Po];

• проконечные группы [Alg], [Koch], [S1];

• алгебраические группы [Alg], [Bo], [VO], [Vo], [Kp1], [PR], [Hu1], [Ch];

• арифметические группы [Alg], [Ari], [PR], [Hu2];

• группы Шевалле, группы Стейнберга [Sem], [St], [M];

• теория инвариантов [W1], [Gur], [DCM], [Kr], [Sp];

• линейные группы [Art], [Ba], [Bae], [Mer], [M], [Su1], [Su2];

• классические группы [Aut], [Art], [D], [Iso], [OM];

• упорядоченные группы [KoKo], [Kop], [KoMe], [Fu1].

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 [HW];

• классические геометрии [Apa], [Be], [Ber], [Bre], [W2], [Wo], [GME], [DNF], [Kob], [NSh], [Roz], [Ter], [He1], [Eis];

• автоморфные формы [Ari], [Brs], [GGP], [JL], [L3], [Shi], [Har];

• гармонический анализ [Lum], [We], [L3], [He2], [HR];

• специальные функции [Vil], [Ri];

• теория кодирования [Brl], [Bla], [CS], [MWS];

• алгебраическая комбинаторика [BI], [CS], [SUS];

• перечислительная комбинаторика [Aig], [BVSh], [Per], [Pri], [Sac], [Sov], [Hrr], [HP].

Применения групп за пределами математики. Разумеется, здесь приведена лишь незначительная выборка 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 [BVe], [BR], [Wae], [W3], [PT], [Ham], [ShK], [ED];

• Кристаллография и теория твердого тела [Ani], [Ans], [AM], [Wu], [DPA], [CG], [Mad], [Har], [Pen], [Str], [F2], [Fe1], [Fe2], [Shu];

• Симметрия молекул [Cot], [Fl], [Ho], [Zue];

• Симметрия атомов и ядер [Wig], [Kap], [Mck], [Zue];

• Симметрия элементарных частиц [LB], [RF1], [Th]

• Группы Лоренца и Пуанкаре [GMSh], [Na2], [Fed], [Wrl].

Книги по теории групп на русском языке

[Aut] *Автоморфизмы классических групп, сб. перев.*, Мир, М., 1976, pp. 1–264.

[Ada] Дж.Адамс, *Лекции по группам Ли*, Наука, М., 1979, pp. 1–144.

[Adi] С.И.Адян, *Проблема Бернсайда и тождества в группах*, Наука, М., 1975, pp. 1–335.

[Aig] М.Айгнер, *Комбинаторная теория*, Мир, М., 1982, pp. 1–556.

[Alg] *Алгебраическая теория чисел*, Мир, М., 1969, pp. 1–483.

[Al] П.С.Александров, *Введение в теорию групп, 3-е изд.*, Наука, М., 1980, pp. 1–143.

[Ale] В.Б.Алексеев, *Теорема Абеля в задачах и решениях*, Наука, М., 1976, pp. 1–207.

[Ami] Л.К.Аминов, *Теория симметрии*, Ин-т Компьютерных Иссл., М., 2002, pp. 1–191.

[Ani] А.Анималу, *Квантовая теория кристаллических твердых тел*, Мир, М., 1981, pp. 1–574.

[Ans] А.И.Ансельм, *Введение в теорию полупроводников, 2-е изд.*, Наука, М., 1978.

[Apa] Б.Н.Апанасов, *Дискретные группы преобразований и структуры многообразий*, Наука, М., 1983, pp. 1–242.

[Ari] *Арифметические группы и автоморфные функции, сб. перев.*, Мир, М., 1969, pp. 1–224.

[Art] Э.Артин, *Геометрическая алгебра*, Наука, М., 1990, pp. 1–318.

[AGH] Л.Ауслендер, Л.Грин, Ф.Хан, *Потоки на однородных пространствах*, Мир, М., 1966, pp. 1–208.

[AM] Н.Ашкрофт, Н.Мермин, *Физика твердого тела, т.* I, II, Мир, М., 1979, pp. 1–399; pp. 1–422.

[BaVe] С.Багавантам, Т.Венкатараману, *Теория групп и ее применение к физическим проблемам*, ИЛ, М., 1959, pp. 1–301.

[BI] Э.Баннаи, Т.Ито, *Алгебрическая комбинаторика. Схемы отношений*, Мир, М., 1987, pp. 1–373.

[BR] А.Барут, Р.Рончка, *Теория представлений групп и ее приложения, т.* I, II, Мир, М., 1980, pp. 1–455; pp. 1–395.

[Ba] Х.Басс, *Алгебраическая K-теория*, Мир, М., 1973, pp. 1–591.

[Bam] Л.Баумгартнер, *Теория групп*, ГТТИ, М., 1934.

[Bau] Р.Бауэр, *Введение в теорию групп*, ??, 1937.

[Ba2] Ю.А.Бахтурин, *Тождества в алгебрах Ли*, Наука, М., 1985, pp. 1–447.

[BVSh] В.В.Белов, Е.М.Воробьев, В.Е.Шаталов, *Теория графов*, Высшая школа, М., 1976, pp. 1–392.

[BF] В.А.Белоногов, А.Н.Фомин, *Матричные представления в теории конечных групп*, Наука, М., 1976, pp. 1–126.

[Be] А.Бердон, *Геометрия дискретных групп*, Наука, М., 1986, pp. 1–300.

[Ber] М.Берже, *Геометрия, т.* I, Мир, М., 1984, pp. 1–559.

[Brl] Э.Берлекэмп, *Алгебраическая теория кодирования*, Мир, М., 1971, pp. 1–477.

[Bla] Р.Блейхут, *Теория и практика кодов, контролирующих ошибки*, Мир, М., 1986, pp. 1–576.

[Bog] О.В.Богопольский, *Введение в теорию групп*, Ин-т Компьютерных Иссл., М., 2002, pp. 1–148.

[Bo] А.Борель, *Линейные алгебраические группы*, Мир, М., 1972, pp. 1–269.

[Br] К.Браун, *Когомологии групп*, Наука, М., 1987, pp. 1–383.

[Bre] Г.Бредон, *Введение в теорию компактных групп преобразований*, Наука, М., 1980, pp. 1–440.

[B1] Н.Бурбаки, *Общая топология, Гл.* III – VIII. *Топологические группы, числа и связанные с ними группы и пространства*, Наука, М., 1969, pp. 1–392.

[B2] Н.Бурбаки, *Интегрирование, Гл.* VI – VIII. *Векторное интегрирование, мера Хаара, свертка и представления*, ГИФМЛ, М., 1970, pp. 1–320.

[B3] Н.Бурбаки, *Группы и алгебры Ли, Гл.* I – III. *Алгебры Ли, свободные алгебры Ли и группы Ли*, Мир, М., 1976, pp. 1–496.

[B4] Н.Бурбаки, *Группы и алгебры Ли, Гл.* IV – VI. *Группы Кокстера и системы Титса, группы, порожденные отражениями, системы корней*, Мир, М., 1972, pp. 1–331.

[B5] Н.Бурбаки, *Группы и алгебры Ли, Гл.* IX. *Компактные вещественные группы Ли*, Мир, М., 1972, pp. 1–173.

[BG] В.М.Бусаркин, Ю.М.Горчаков, *Конечные расщепляемые группы*, Наука, М., 1968, pp. 1–111.

[Bae] Р.Бэр, *Линейная алгебра и проективная геометрия*, НИЛ, М., 1955, pp. 1–399.
[Wae] Б.Л. ван дер Варден, *Методы теории групп в квантовой механике*, ОНТИ, Харьков, 1939.
[Wei] А.Вейль, *Интегрирование в топологических группах и его применения*, ИЛ, М., 1950.
[W1] Г.Вейль, *Классические группы, их инварианты и представления*, ИЛ, М., 1947, pp. 1–408.
[W2] Г.Вейль, *Симметрия*, Наука, М., 1968, pp. 1–191.
[W3] Г.Вейль, *Теория групп и квантовая механика*, Наука, М., 1986, pp. 1–495.
[Wrl] Ю.Верле, *Релятивистская теория реакций*, Атомиздат, М., 1969, pp. 1–441.
[Wi] Е.Вигнер, *Теория групп и ее приложение к квантовомеханической теории атомных спектров*, ИЛ, М., 1961.
[Vil] Н.Я.Виленкин, *Специальные функции и теория представлений групп*, Наука, М., 1965, pp. 1–588.
[Vin] Э.Б.Винберг, *Линейные представления групп*, Наука, М., 1985.
[VO] Э.Б.Винберг, А.Л.Онищик, *Семинар по группам Ли и алгебраическим группам*, Наука, М., 1988, pp. 1–343.
[Wo] Дж.Вольф, *Пространства постоянной кривизны*, Наука, М., 1982, pp. 1–480.
[Vo] В.Е.Воскресенский, *Алгебраические торы*, Наука, М., 1977, pp. 1–223.
[Wu] У.А.Вустер, *Применение тензоров и теории групп для описания физических свойств кристаллов*, Мир, М., 1977.
[Vy] *Вычисления в алгебре и теории чисел*, vol. 2, Мир, М., 1976, pp. 1–304.
[GGP] И.М.Гельфанд, М.И.Граев, И.И. Пятецкий-Шапиро, *Теория представлений и автоморфные функции*, Мир, М., 1987, pp. 1–312.
[GMSh] И.М.Гельфанд, Р.А.Минлос, З.Я.Шапиро, *Представления группы вращений и группы Лоренца*, Физматгиз, М., 1958, pp. 1–368.
[Hyp] *Гиперболические группы по Михаилу Громову*, Мир, М., 1992.
[Gui] А.Гишарде, *Когомологии топологических групп и алгебр Ли*, Мир, М., 1984, pp. 1–262.
[Gol] Л.И.Головина, *Линейная алгебра и некоторые ее приложения. 4-е изд.*, Наука, М., 1985, pp. 1–392.
[Gor] Д.Горенстейн, *Конечные простые группы. Введение в их классификацию*, Мир, М., 1985, pp. 1–350.
[Gov] Ю.М.Горчаков, *Группы с конечными классами сопряженных элементов*, Наука, М., 1978, pp. 1–119.
[Grn] Ф.Гринлиф, *Инвариантные средние на топологических группах*, Мир, М., 1973, pp. 1–136.
[Gro] М.Громов, *Гиперболические группы*, Ин-т Компьютерных Иссл., М., 2002, pp. 1–159.
[GM] И.Гроссман, В.Магнус, *Группы и графы*, Мир, М., 1971.
[GME] И.Груневальд, Й.Меннике, Ю.Эльстродт, *Группы, действующие на гиперболическом пространстве*, МЦНМО, М., 2003, pp. 1–615.
[Gur] Г.Б.Гуревич, *Основы теории алгебраических инвариантов*, Гостехиздат, М., 1948.
[DPA] Б.Н.Делоне, Н.Падуров, А.Д.Алекскандров, *Математические основы анализа кристаллов и определение основного параллелепипеда повторяемости при помощи рентгеновских лучей*, ОНТИ, Л.–М., 1934, pp. 1–328.
[Ja] Г.Джеймс, *Теория представлений симметрических групп*, Мир, М., 1982.
[tD] Т.том Дик, *Группы преобразований и теория представлений*, Мир, М., 1982, pp. 1–227.
[DNF] Б.А.Дубровин, С.П.Новиков, А.Т.Фоменко, *Современная геометрия. т.* I. *Методы и приложения*, Наука, М., 1979, pp. 1–759.
[D] Ж.Дьедонне, *Геометрия классических групп*, Мир, М., 1974, pp. 1–204.
[DCM] Ж.Дьедонне, Дж.Кэррол, Д.Мамфорд, *Геометрическая теория инвариантов*, Мир, М., 1974, pp. 1–280.
[JL] Э.Жаке, Р.Ленглендс, *Автоморфные формы на* GL_2, Мир, М., 1973, pp. 1–372.
[Zh] Д.П.Желобенко, *Компактные группы Ли и их представления*, Наука, М., 1970, pp. 1–664.
[ZhSh] Д.П.Желобенко, А.И.Штерн, *Представления групп Ли*, Наука, М., 1983, pp. 1–360.

[Iso] *Изоморфизмы классических групп над целостными кольцами, сб. перев.*, vol. 20, Мир, М., 1980, pp. 1–272.
[IMS] В.В.Ишханов, В.И.Мысовских, А.И.Скопин, *Теория групп*, СПбГУ, СПб, 1997, pp. 1–52.
[Kon] *К теории конечных групп, сб. перев.*, vol. 16, Мир, М., 1979, pp. 1–200.
[Ka] Л.А.Калужнин, *Избранные главы теории групп*, КГУ, Киев, 1979, pp. 1–51.
[KS] Л.А.Калужнин, В.И.Сущанский, *Преобразования и перестановки*, Наука, М., 1979, pp. 1–112.
[Kap] И.Г.Каплан, *Симметрия многоэлектронных систем*, Наука, М., 1969, pp. 1–407.
[Ka1] И.Капланский, *Введение в дифференциальную алгебру*, ИЛ, М., 1959.
[Ka2] И.Капланский, *Алгебры Ли и локально компактные группы*, Мир, М., 1974, pp. 1–148.
[KaM] М.И.Каргаполов, Ю.И.Мерзляков, *Основы теории групп*, Наука, М., 1-е изд. 1972; 2-е изд. 1977; 3-е изд. 1982, pp. 1–288.
[KE] А.Картан, С.Эйленберг, *Гомологическая алгебра*, ИЛ, М., 1960, pp. 1–510.
[Kir] А.А.Кириллов, *Элементы теории представлений, 2–е изд.*, Наука, М., 1978, pp. 1–343.
[Kob] Ш.Кобаяси, *Группы преобразований в дифференциальной геометрии*, Наука, М., 1986, pp. 1–224.
[KoKo] А.И.Кокорин, В.М.Копытов, *Линейно упорядоченные группы*, Наука, М., 1972, pp. 1–199.
[CG] Р.Кокс, А.Голд, *Симметрия в твердом теле*, Наука, М., 1970, pp. 1–424.
[C?] Г.С.М.Коксетер, *Введение в геометрию*, Наука, М., 1966, pp. 1–648.
[CM] Г.С.М.Коксетер, У.О.Мозер, *Порождающие элементы и определяющие соотношения дискретных групп*, Наука, М., 1980, pp. 1–240.
[CS] Дж.Конвей, Н.Слоэн, *Упаковки шаров, решетки и группы, т.* I, II, Мир, М., 1990, pp. 1–413; pp. 421–791.
[Kop] В.М.Копытов, *Решеточно упорядоченные группы*, Наука, М., 1984, pp. 1–320.
[KoMe] В.М.Копытов, Н.Я.Медведев, *Правоупорядоченные группы*, Научная книга, Новосибирск, 1996, pp. 1–246.
[K4] А.И.Кострикин, *Вокруг Бернсайда*, Наука, М., 1986, pp. 1–232.
[Kot] Ф.А.Коттон, *Химические приложения теории групп*, Мир, М., 1965.
[Koch] Х.Кох, *Теория Галуа p-расширений*, Мир, М., 1973, pp. 1–199 1–375.
[Kr] Х.Кра, *Автоморфные формы и клейновы группы*, Мир, М., 1975, pp. 1–296.
[Kr] Х.Крафт, *Геометрические методы в теории инвариантов*, Мир, М., 1987, pp. 1–312.
[CF] Р.Кроуэлл, Р.Фокс, *Введение в теорию узлов*, Мир, М., 1967, pp. 1–348.
[Kur] А.Г.Курош, *Теория групп, 3–е изд.*, Наука, М., 1967, pp. 1–647.
[CR] Ч.Кэртис, И.Райнер, *Теория представлений конечных групп и ассоциативных алгебр*, Наука, М., 1969, pp. 1–668.
[LSh] Р.Линдон, П.Шупп, *Комбинаторная теория групп*, Мир, М., 1980, pp. 1–447.
[L2] С.Ленг, $SL_2(\mathbb{R})$, Мир, М., 1977, pp. 1–430.
[L3] С.Ленг, *Введение в теорию модулярных форм*, Мир, М., 1979, pp. 1–254.
[Lub] Т.Я.Любарский, *Теория групп и ее применения в физике*, Физматгиз, М., 1957.
[LAL] Е.С.Ляпин, А.Я.Айзенштат, М. М.Лесохин, *Упражнения по теории групп*, Наука, М., 1967, pp. 1–264.
[LB] В.Д.Ляховский, Б.А.Болохов, *Группы симметрии и элементарные частицы*, Изд-во ЛГУ, М., 1983, pp. 1–336.
[MKS] В.Магнус, А.Каррас, Д.Солитер, *Комбинаторная теория групп*, Наука, М., 1974, pp. 1–455.
[Mad] О.Маделунг, *Теория твердого тела*, Наука, М., 1980, pp. 1–416.
[MWS] Ф.Дж.Мак-Вильямс, Н.Дж.А.Слоэн, *Теория кодов, исправляющих ошибки*, Связь, М., 1979, pp. 1–744.
[Mck] Дж.Макки, *Лекции по математическим основам квантовой механики*, Мир, М., 1965, pp. 1–221.
[Mac] С.Маклейн, *Гомология*, Мир, М., 1966, pp. 1–543.
[MS] У.С.Масси, Дж.Столлингс, *Алгебраическая топология: введение*, Мир, М., 1977, pp. 1–338.

[Mer] Ю.И.Мерзляков, *Рациональные группы*, Наука, М., 1980, pp. 1–464.
[M] Дж.Милнор, *Введение в алгебраическую K-теорию*, Мир, Berlin et al., 1974, pp. 1–196.
[Mur] Ф.Мурнаган, *Теория представлений групп*, ИЛ, М., 1950.
[Na1] М.А.Наймарк, *Линейные представления группы Лоренца*, Физматгиз, М., 1958.
[Na2] М.А.Наймарк, *Теория представлений групп*, Наука, М., 1976, pp. 1–559.
[NSh] В.В.Никулин, И.Р.Шафаревич, *Геометрии и группы*, Наука, М., 1983, pp. 1–239.
[Neu] Х.Нейман, *Многообразия групп*, Мир, М., 1969, pp. 1–264.
[Ol] А.Ю.Ольшанский, *Геометрия определяющих соотношений в группах*, Наука, М., 1989.
[OM] О.О'Мира, *Лекции о симплектических группах*, Мир, М., 1979, pp. 1–166.
[Pen] Т.Пенкаля, *Очерки кристаллохимии*, Химия, Л., 1974, pp. 1–496.
[Per] *Перечислительные задачи комбинаторного анализа*, Мир, М., 1979, pp. 1–363.
[PT] М.И.Петрашень, В.Д.Трифонов, *Применение теории групп в квантовой механике*, ИЛ, М., 1967, pp. 1–308.
[PR] В.П.Платонов, А.С.Рапинчук, *Алгебраические группы и теория чисел*, Наука, М., 1991, pp. 1–654.
[Pl] Б.И.Плоткин, *Группы автоморфизмов алгебраических систем*, Наука, М., 1966, pp. 1–603.
[Po] Л.С.Понтрягин, *Непрерывные группы*, Наука, М., 1984, pp. 1–519.
[Pos] М.М.Постников, *Группы и алгебры Ли*, Наука, М., 1982, pp. 1–447.
[Pri] *Прикладная комбинаторная математика*, Мир, М., 1968, pp. 1–362.
[Rag] М.С.Рагунатан, *Дискретные подгруппы групп Ли*, Мир, М., 1977, pp. 1–316.
[Raz] *Разрешимые и простые бесконечные группы*, vol. 21, Мир, М., 1981, pp. 1–208.
[Ri] Р.Рихтмайер, *Принципы современной математической физики. т.* II. *Группы и теория представлений*, Мир, М., 1984, pp. 1–381.
[Roz] Б.А.Розенфельд, *Неевклидовы пространства*, Наука, М., 1969, pp. 1–547.
[RF1] Ю.Б.Румер, А.И.Фет, *Теория унитарной симметрии*, Наука, М., 1970, pp. 1–400.
[RF2] Ю.Б.Румер, А.И.Фет, *Теория групп и квантованные поля*, Наука, М., 1977, pp. 1–247.
[Sc1] В.Н.Сачков, *Комбинаторные методы дискретной математики*, Наука, М., 1977, pp. 1–319.
[Sc2] В.Н.Сачков, *Введение в комбинаторные методы дискретной математики*, Наука, М., 1982, pp. 1–384.
[Swi] Р.М.Свитцер, *Алгебраическая топология – гомотопии и гомологии*, Наука, М., 1985, pp. 1–606.
[Sem] *Семинар по алгебраическим группам*, Мир, М., 1973, pp. 1–315.
[S1] Ж.-П.Серр, *Когомологии Галуа*, Мир, М., 1968, pp. 1–208 1–375.
[S2] Ж.-П.Серр, *Алгебры Ли и группы Ли*, Мир, М., 1969, pp. 1–375.
[S3] Ж.-П.Серр, *Линейные представления конечных групп*, Мир, М., 1970.
[Sp] Т.Спрингер, *Теория инвариантов*, Мир, М., 1981, pp. 1–191.
[St] Р.Стейнберг, *Лекции о группах Шевалле*, Мир, М., 1975.
[Suz] М.Судзуки, *Строение группы и строение структуры ее подгрупп*, ИЛ, М., 1960, pp. 1–158.
[Su1] Д.А.Супруненко, *Разрешимые и нильпотентные линейные группы*, Минск, 1958.
[Su2] Д.А.Супруненко, *Группы матриц*, Наука, М., 1972, pp. 1–351.
[Suc] А.И.Сушкевич, *Теория обобщенных групп*, ГНТИ Украины, Харьков–Киев, 1937, pp. 1–176.
[SuS] В.И.Сущанский, В.С.Сикора, *Операції на группах підстановок: теорія та застосування*, Рута, Чурнавці, 2003, pp. 1–255.
[Hsi] У.И.Сян, *Когомологическая теория топологических групп преобразований*, Мир, М., 1979, pp. 1–243.
[Th] *Теория групп и элементарные частицы, сб.статей*, Мир, М., 1967, pp. 1–375.
[Ter] У.Терстон, *Трехмерная геометрия и топология, т.1.*, МЦНМО, М., 2001, pp. 1–312.
[F2] Д.К.Фаддеев, *Таблицы основных унитарных представлений федоровских групп*, Наука, М.–Л., 1961.
[Fe1] Е.С.Федоров, *Симметрия и структура кристаллов*, Изд-во АН СССР, М., 1949, pp. 1–639.

[Fe2] Е.С.Федоров, *Правильное деление плоскости и пространства*, Наука, Л., 1979, pp. 1–272.
[Fed] Ф.И.Федоров, *Группа Лоренца*, Наука, М., 1979, pp. 1–384.
[Fe] У.Фейт, *Теория представлений конечных групп*, Наука, М., 1990, pp. 1–461.
[Fl] Р.Фларри, *Группы симметрии. Теория и химические приложения*, Мир, М., 1983, pp. 1–395.
[Fr] Э.Фрид, *Элементарное введение в абстрактную алгебру*, Мир, М., 1979, pp. 1–260.
[F] Г.Фробениус, *Теория характеров и представлений групп*, ОНТИ, Харьков, 1937.
[Fu1] Л.Фукс, *Частично упорядоченные алгебраические системы*, Мир, М., 1965, pp. 1–342.
[Fu2] Л.Фукс, *Бесконечные абелевы группы, т.* I,II, Мир, М., 1974, pp. 1–335; 1977, pp. 1–416.
[Hu1] Дж.Хамфри, *Линейные алгебраические группы*, Наука, М., 1980, pp. 1–399.
[Hu2] Дж.Хамфри, *Арифметические группы*, Мир, М., 1983, pp. 1–207.
[Ham] М.Хамермеш, *Теория групп и ее применение к физическим проблемам*, Мир, М., 1966, pp. 1–587.
[Hrr] Ф.Харари, *Теория графов*, Мир, М., 1973, pp. 1–300.
[Hrr] Ф.Харари, Э.Палмер, *Перечисление графов*, Мир, М., 1977, pp. 1–324.
[Har] Хариш-Чандра, *Автоморфные формы на полупростых группах Ли*, Мир, М., 1971, pp. 1–246.
[Han] М.Харрисон, *Теория твердого тела*, Мир, М., 1972, pp. 1–616.
[Hei] В.Хейне, *Теория групп в квантовой механике*, ИЛ, М., 1963.
[He1] С.Хелгасон, *Дифференциальная геометрия и симметрические пространства*, Мир, М., 1965.
[He2] С.Хелгасон, *Группы и геометрический анализ*, Мир, М., 1987, pp. 1–735.
[Hen] Э.Хеннан, *Представления групп и прикладная теория вероятностей*, Мир, М., 1970, pp. 1–118.
[HW] П.Хилтон, С.Уайли, *Теория гомологий: введение в алгебраическую топологию*, Мир, М., 1966, pp. 1–452.
[Ha] М.Холл, *Теория групп*, ИЛ, М., 1962, pp. 1–468.
[Ho] Р.Хохштрассер, *Молекулярные аспекты симметрии*, Мир, М., 1968, pp. 1–384.
[Hus] Э.Хьюзмоллер, *Расслоенные пространства*, Мир, М., 1970, pp. 1–442.
[HR] Э.Хьюитт, К.Росс, *Абстрактный гармонический анализ, т.* I, Наука, М., 1975, pp. 1–654.
[ZVC] Х.Цишанг, Э.Фогт, Ч.-Д.Холдевай, *Поверхности и дискретные группы*, Наука, М., 1988.
[Zue] Л.Цюлике, *Квантовая химия, т.1*, Мир, М., 1976, pp. 1–512.
[ChM] Б.Чандлер, В.Магнус, *Развитие комбинаторной теории групп*, Мир, М., 1985, pp. 1–253.
[Cheb] Н.Г.Чеботарев, *Теория групп Ли*, Гостехиздат, М., 1940.
[Cher] С.Н.Черников, *Группы с заданными свойствами системы подгрупп*, Наука, М., 1980, pp. 1–383.
[Ch] К.Шевалле, *Теория групп Ли, т.* I – III, ИЛ, М., 1948, pp. 1–315; 1958.
[Shem] Л.А.Шеметков, *Формации конечных групп*, Наука, М., 1978, pp. 1–271.
[Shi] Г.Шимура, *Введение в арифметическую теорию автоморфных функций*, Мир, М., 1973, pp. 1–326.
[Sch] О.Ю.Шмидт, *Абстрактная теория групп, 2-е изд.*, ГТТИ, М., 1933, см. также Избранные Труды, 1959.
[Scht] Г.Штрайтвольф, *Теория групп в физике твердого тела*, Мир, М., 1971, pp. 1–262.
[Shu] А.В.Шубников, *Атлас кристаллографических групп симметрии*, ОНТИ, Л., 1946.
[ShK] А.В.Шубников, В.А.Копциг, *Симметрия в науке и искусстве*, Наука, М., 1972, pp. 1–339.
[Eis] Л.П.Эйзенхарт, *Непрерывные группы преобразований*, ИЛ, М., 1947, pp. 1–359.
[ED] Дж.Эллиот, П.Добер, *Симметрия в физике, т.* I, II, Мир, М., 1983, pp. 1–364; pp. 1–410.

Теория групп: a student's guide

— И Вы все это прочитали?
— Нет. Я, конечно, работаю с книгами, но не обязан их читать.

Артуро Перес-Реверте "Клуб Дюма, или тень Ришелье".

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. Наиболее сбалансированным введением в теорию групп для всех математиков, независимо от специальности, является книга Джозефа Ротмана [Ro]. Книга Майкла Ашбахера [A1] 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 – книга Альперина и Белла [AB]. Лучшее введение в теорию представлений для математиков-неспециалистов – Фултон и Харрис [FH]. Разумеется, для профессионалов ничто не может заменить знакомство со вторым изданием монументального труда Кэртиса и Райнера [CR]. Имеется несколько монументальных учебников и монографий по теории конечных групп, в том числе многотомные труды Мичио Судзуки [Suz] и Бертрама Хупперта [Hu]. Совершенно особое место во всей математической литературе занимают книга Горенстейна [Go] и цикл книг Горенстейна, Лайонса и Соломона, посвященных классификации [GLS1] – [GLS5]. Укажем еще несколько **совершенно выдающихся** текстов, посвященных отдельным наиболее интересным классам групп, вполне доступных для начинающего: Картер [Ca], [Ca], Бенсон–Гроув [BG], Хамфри [Hu4], Спрингер [Sp], Ашбахер [A2], [A3], Серр [S4], Браун и Ронан [Br], [Ron]. Полное построение всех 230 пространственных групп изложено в [Kim].

Учебники по теории групп

[Mac] I.D.MacDonald, *The theory of groups*, Claredon Press, Oxford, 1968.
[Rob] D.J.S.Robinson, *A course in the theory of groups*, Springer, Berlin et al., 1982.
[Ros] J.S.Rose, *A course on group theory*, C.U.P., Cambridge, 1978.
[Rot] J.J.Rotman, *The theory of groups, an introduction, 2nd ed.*, Allyn & Bacon, Boston, 1973.
[Sch] E.Schenkman, *Group theory*, N.Y., 1965.
[ST] G.Smith, O.Tabachnikova, *Topics in group theory*, Springer Verlag, Berlin et al., 2000, pp. 1–255.
[Za] H.Zassenhaus, *The theory of groups*, Dover Publications, N.Y., 1999, pp. 1–265, (Reprint of the 1958 Chelsea 2nd edition).

Популярная литература

[Bud] F.J.Budden, *The fascination of groups*, C.U.P., Cambridge, 1972.
[Bus] B.P.Burns, *Geometry: a path to groups*, C.U.P., Cambridge, 1987.
[Joy] D.Joyner, *Adventures in group theory*, John Hopkins Univ., Baltimore, 2002, pp. 1–262.
[Mr1] R.Mirman, *Group theory: an intuitive approach*, World Scientific, London et al., 1995.

Конечные группы

[A1] M.Aschbacher, *Finite group theory, 2nd ed.*, C.U.P., Cambridge, 2000, pp. 1–304.

[Bur] W.Burnside, *Theory of groups of finite order, reprint of the 2nd ed.*, Dover, N.Y., 1955.
[Go1] D.Gorenstein, *Finite groups*, Harper & Row, N.Y., 1st ed. 1968; Chelsea, N.Y., 2nd ed. 1980.
[Hu] B.Huppert, *Endliche Gruppen,* Bd. I, Springer, Berlin et al., 1967, pp. 1–793.
[HB] B.Huppert, N.Blackburn, *Finite groups,* vol. II, III, Springer, Berlin et al., 1982, pp. 1–531; pp. 1–454.
[Spe] A.Speiser, *Die Theorie der Gruppen von endlicher Ordnung,* 4te Aufl., Birkhäuser, Basel et al., 1956, pp. 1–271.
[Sz] M.Suzuki, *Group theory,* vol. I, II, Springer Verlag, Berlin et al., 1982, pp. 1–434.
[KSt] H.Kurzweil, B.Stellmacher, *Theorie der endlichen Gruppen: eine Einführung*, Springer Verlag, Berlin et al., 1998, pp. 1–341.
[Wh1] B.A.F.Wehrfritz, *Finite groups: a second course on group theory*, World Scientific, London et al., 1999, pp. 1–123.

Классификация конечных простых групп

[Go2] D.Gorenstein, *The classification of finite simple groups, vol. 1, Groups of non-characteristic 2 type*, Plenum Press, N.Y., 1983, pp. 1–487.
[GLS1] D.Gorenstein, R.Lyons, R.Solomon, *The classification of the finite simple groups,*, Amer. Math. Society, Providence, R.I., 1994, pp. 1–165.
[GLS2] 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, pp. 1–218.
[GLS3] 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, pp. 1–419.
[GLS4] D.Gorenstein, R.Lyons, R.Solomon, *The classification of the finite simple groups, N.2, Part* II*, Ch. 1–4. Uniqueness theorems*, Amer. Math. Society, Providence, R.I., 1999, pp. 1–341.
[GLS5] D.Gorenstein, R.Lyons, R.Solomon, *The classification of the finite simple groups, N.5, Part* III*, Ch. 1–6. The generic case*, Amer. Math. Society, Providence, R.I., 2002, pp. 1–467.

Спорадические группы

[A2] M.Aschbacher, *Sporadic groups*, C.U.P., Cambridge, 1994.
[A3] M.Aschbacher, *3-transposition groups*, C.U.P., Cambridge, 1997.
[Atlas] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson, *An atlas of finite groups*, Claredon Press, Oxford, 1972, pp. 1–284.
[FLM] I.Frenkel, J.Lepowsky, A.Meurman, *Vertex operator algebras and the monster*, Academic Press, Boston et al., 1988, pp. 1–502.
[Gr] R.L.Griess, *Twelve sporadic groups*, Springer Verlag, Berlin et al., 1998, pp. 1–169.

Представления конечных групп

[Col] M.J.Collins, *Representations and characters of finite groups*, C.U.P., Cambridge, 1990, pp. 1–242.
[Dor] L.Dornhoff, *Group representation theory. Parts A,B*, Marcel Dekker, N.Y. et al., 1971; 1972.
[Hil] V.E.Hill, *Groups and characters*, Chappman & Hall, Boca Raton, Fl., 2000, pp. 1–239.
[Isa] I.M.Isaacs, *Character theory of finite groups*, Academic Press, N.Y. et al., 1976.
[JL] D.James, M.Liebeck, *Representations and characters of groups, 2nd ed.*, C.U.P., Cambridge, 2001, pp. 1–458.
[PD] B.Puttaswamaiah, J.D.Dixon, *Modular representations of finite groups*, Academic Press, N.Y. et al., 1977, pp. 1–242.

Группы типа Ли

[C1] R.W.Carter, *Simple groups of Lie type*, Wiley, London et al., 1972, pp. 1–331.
[C2] R.W.Carter, *Finite groups of Lie type: conjugacy classes and complex characters*, Wiley, London et al., 1985, pp. 1–544.
[Hu?] J.Humphreys, *Introduction to Lie algebras and representation theory, 3rd revised printing*, Springer Verlag, Berlin et al., 1980.
[KL] P.B.Kleidman, M.W.Liebeck, *The subgroup structure of the finite classical groups*, C.U.P., Cambridge, 1990, pp. 1–303.
[Lu] G.Lusztig, *Characters of reductive groups over a finite field. Ann. Math. Studies*, vol. 107, Princeton Univ. Press, 1984, pp. 1–384.
[Tim] F.G.Timmesfeld, *Abstract root subgroups and simple groups of Lie type*, Birkhäuser Verlag, Basel, 2001, pp. 1–389.

Алгебраические группы

[Ch] C.Chevalley, *Classification des groupes de Lie algebriques, vol.* I, II, ENS, Paris, 1956-58.
[Ho] G.Hochschild, *Basic theory of algebraic groups and Lie algebras*, Springer, Berlin et al., 1981.
[Sp] T.Springer, *Linear algebraic groups*, Birkhäuser, Boston et al., 1981, pp. 1–304.

Группы перестановок

[BW] N.L.Biggs, A.T.White, *Permutation groups and combinatorial structures*, C.U.P., Cambridge, 1979.
[Cam] P.J.Cameron, *Permutation groups*, C.U.P., Cambridge, 1999, pp. 1–220.
[Kr1] A.Kerber, *Algebraic combinatorics via finite group actions*, Biblographisches Inst., Mannheim, 1991.
[Kr2] A.Kerber, *Applied finite group actions*, Springer Verlag, Berlin et al., 1999, pp. 1–454.
[BW] M.Ch.Klin, R.Pöschel, K.Rosenbaum, *Angewandte Algebra. Einführung in gruppentheoretisch-kombinatorische Methoden*, DVW, Berlin, 1988, pp. 1–208.
[Pas] D.Passman, *Permutation groups*, Academic Press, N.Y. et al., 1968.
[Sag] B.E.Sagan, *The symmetric groups: representations, combinatorial algorithms, and symmetric functions, 2nd ed.*, Springer Verlag, Berlin et al., 2001, pp. 1–238.
[Wie] H.Wielandt, *Finite permutation groups*, Academic Press, N.Y. et al., 1964.

Линейные группы

[Bl] H.R.Blichfeldt, *Finite collineation groups*, Univ. Chicago Press, 1917, pp. 1–193.
[Di] L.E.Dickson, *Linear groups, reprint*, Dover, N.Y., 1958.
[Dix] J.Dixon, *The structure of linear groups*, Van Nostrand – Reinhold, London et al., 1971, pp. 1–183.
[Jo] C Jordan, *Traité des substitutions et des équations algebriques*, Gauthier-Villars, Paris, 1870.
[vdW] B.van der Waerden, *Gruppen von linearen Transformationen*, Springer, Berlin et al., 1935.
[Wh2] B.A.F.Wehrfritz, *Infinite linear groups*, Springer, Berlin et al., 1973, pp. 1–229.
[WSh] B.A.F.Wehrfritz, M.Shirvani, *Skew linear groups*, C.U.P., Cambridge, 1986, pp. 1–253.

Классические группы

[D?] J.Dieudonné, *Sur les groupes classiques*, Hermann, Paris, 1948.
[HOM] A.Hahn, O.T.O'Meara, *The classical groups and K-theory*, Springer, Berlin et al., 1989, pp. 1–576.

Группы Ли

[Ba] A.Baker, *Matrix groups*, Springer Verlag, Berlin et al., 2002, pp. 1–330.
[DK] J.J.Duistermaat, J.A.C.Kolk, *Lie groups*, Springer Verlag, Berlin et al., 2000, pp. 1–344.

[FdV] H.Freudenthal, H. de Vries, *Linear Lie groups*, Academic Press, N.Y. et al., 1969, pp. 1–547.
[Ho] G.Hochschild, *The structure of Lie groups*, Holden Day, 1965, pp. 1–230.
[Hsi] W.-Y.Hsiang, *Lectures on Lie groups*, World Scientific, London et al., 2000, pp. 1–108.
[Kna] A.W.Knapp, *Lie groups beyond an introduction, 2nd ed.*, Birkhäuser, Boston et al., 2002, pp. 1–812.
[Nom] K.Nomizu, *Lie groups and differential geometry. vol.* I, II, N.Y., 1963; 1969.
[SW] A.Sagle, R.Walde, *Introductions to Lie groups and Lie algebras*, Academic Press, N.Y. et al., 1973.
[Var] V.S.Varadarajan, *An introduction to harmonic analysis on semisimple groups*, C.U.P., Cambridge, 1999, pp. 1–316.

Представления групп Ли

[A] M.Atiyah et al.??, *Representation theory of Lie groups*, C.U.P., Cambridge, ???, pp. 1–341.
[Var] V.S.Varadarajan, *Lie groups, Lie algebras and their representations*, Prentice Hall, 1974.
[Wal] N.Wallach, *Harmonic analysis on homogeneous spaces*, N.Y., 1973.
[War] G.Warner, *Harmonic analysis on semi-simple Lie groups vol.* I, II, Berlin, 1972.
[Waw] A.Wawrzyńczyk, *Współczesna teoria funkcji specjalnych*, PAN, Warszawa, 1978, pp. 1–525.

Группы Коксетера

[GB] L.C.Grove, C.T.Benson, *Finite reflection groups, 2nd ed.*, Springer, Berlin et al., 1985.
[Hu4] J.Humphreys, *Reflection groups and Coxeter groups*, C.U.P., Cambridge, 1992.
[Kan] R.Kane, *Reflection groups and invariant theory*, Springer Verlag, Berlin et al., 2001, pp. 1–379.

Топологические группы

[Mau] K.Maurin, *General eigenfuction expansions and unitary representations of topological groups*, PWN, Warszawa, 1968, pp. 1–367.
[Wil] L.Ribes, *Introduction to profinite groups and Galois cohomology*, Queen's Univ., Kingston, Ontario, 1999, pp. 1–316, (reprint of the 1970 original).
[Wil] J.S.Wilson, *Profinite groups*, Claredon Press, Oxford et al., 1998, pp. 1–284.

Группы и геометрии

[Abr] P.Abramenko, *Twin buildings and applications to S-arithmetic groups* Springer Lecture Notes Math., vol. 1641, Berlin et al., 1996.
[Han] F.Buekenhout (ed.), *Handbook of incidence geometry: buildings and foundations*, Elsevier, Amsterdam et al., 1995.
[Pa] A.Pasini, *Diagram geometries*, Claredon Press, Oxford, 1994.
[Ron] M.Ronan, *Lectures on buildings*, Academic Press, N.Y. et al., 1989.
[Ti] J.Tits, *Buildings of spherical type and finite BN-pairs* Springer Lecture Notes Math., vol. 386, Berlin et al., 1974.

Бесконечные группы

[KW] O.Kegel, B.A.F.Wehrfritz, *Locally finite groups*, Amsterdam, 1973, pp. 1–210.
[War] R.B.Warfield, *Nilpotent groups* Springer Lecture Notes Math., vol. 513, Berlin et al., 1976.
[Rob] D.J.S.Robinson, *Finiteness conditions and generalised soluble groups, vol.* I, II, Springer, Berlin et al., 1972.
[Seg] D.Segal, *Polycyclic groups*, C.U.P., Cambridge, 1983.

Группы в геометрии и топологии

[B4] A.Borel, *Seminar on transformation groups. Ann. Math. Studies*, vol. 46, Princeton Univ. Press, 1960.
[Mag] W.Magnus, *Non-Euclidean tesselations and their groups*, Academic Press, N.Y., 1976.
[Whi] A.T.White, *Graphs, groups and surfaces, 2nd ed.*, North Holland, N Amsterdam, 1984.

Геометрическая теория групп

[dlH] P.de la Harpe, *Topic in geometric group theory*, Univ. Chicago Press, Chicago, Il., 2000, pp. 1–310.

Комбинаторная теория групп

[Bau] G.Baumslag, *Topics in combinatorial group theory*, Birkhäuser, Boston et al., 1993.
[Co1] D.E.Cohen, *Combinatorial group theory: a topological approach*, Queen Mary College, London, 1978.
[FR] B.Fine, G.Rosenberger, *Algebraic generalizations of discrete groups*, Marcel Dekker, N.Y. et al., 1999, pp. 1–317.
[S3] J.-P.Serre, *Arbres, amalgames,* SL_2, Astèrisque or Springer, Berlin et al..

Когомологии групп

[AM] A.Adem, R.J.Milgram, *The cohomology of finite groups*, Springer, Berlin et al., 1994.
[AM] A.Babakhanian, *Cohomology of finite groups*, Queen's Univ., Kingston, Ontario, 1999, pp. 1–216, (reprint of the 1969 original).
[Ben] D.Benson, *Representations and cohomology: cohomology of groups and modules*, C.U.P., Cambridge, 1991.
[Co2] D.E.Cohen, *Groups of cohomological dimension one*, Springer, Berlin et al., 1972.
[Gr] C.Gruenberg, *Cohomological topics in group theory* Springer Lecture Notes Math., Berlin et al., 1970.
[Sta] U.Stammbach, *Homology in group theory* Springer Lecture Notes Math., vol. 359, Berlin et al., 1973.

Применения групп в физике, химии и минералогии

[Bar] V.Bargmann, *Group representations in mathematics and physics*, Berlin et al., 1970.
[Dy] F.J.Dyson, *Symmetry groups in nuclear and particle physics*, Benjamin, N.Y., 1966.
[Kim] Sh.K.Kim, *Group theoretical methods and applications to molecules and crystals*, C.U.P., Cambridge, 1999, pp. 1–492.
[MSt] K.Mathiak, P.Stingl, *Gruppentheorie für Chemiker, Physiko-Chemiker und Mineralogen*, Viehweg, Braunschweig, 1968.
[Mr2] R.Mirman, *Point groups, space groups, crystals, molecules*, World Scientific, London et al., 1999, pp. 1–707.
[Wag] M.Wagner, *Gruppentheoretische Methoden in der Physik*, Vieweg & Sohn, Braunschweig, 1998, pp. 1–461.

История теории групп

[Bor] A.Borel, *Essays in the history of Lie groups and algebraic groups*, Amer. Math. Soc., Providence, R.I., 2001, pp. 1–184.
[Gra] J.J.Gray, *Linear differential equations and group theory from Riemann to Poincaré*, Birkhäuser, Basel et al., 2000, pp. 1–338.

Тема 1. ГРУППЫ

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

Michael Doob, A gentle introduction to TEX.

На вопрос “Что такое животное?” лучше всего отвечает прогулка по зоопарку.

Джордж Гретцер[19]

В этой главе мы вводим понятие группы и приводим первые примеры групп. Не предполагается, что начинающий поймет (или просто прочтет) все эти примеры при первом чтении, они служат только для того, чтобы показать, что группы возникают в математике в десятках различных констекстов и по самым разным поводам.

§ 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 задан*[20] *закон композиции* $\mathrm{mult} : G \times G \longrightarrow G$, $(x, y) \mapsto xy$, *обладающий следующими тремя свойствами:*

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**.

---

[19] Г.Гретцер, Общая теория решеток. – Мир., М., 1982, с.1–452, стр.396.

[20] В этом месте у нас с Робертом Шмидтом возникла 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 углы предмета составить представления об остальных трех, не следует учить’. 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.

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**[21]*, 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[22], который доказал разрешимость в радикалах уравнений с абелевой группой Галуа. Абелевы группы обычно записываются аддитивно, так что вместо xy пишется $x + y$, 0 вместо e и $-x$ вместо x^{-1}.

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

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

Обратите внимание на порядок множителей во втором выражении. Если две операции не коммутируют, то он весьма существеннен. 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?

3. 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}.

---

[21] Специалисты по комбинаторной теории групп в этом случае используют обозначение $x \rightleftarrows y$, однако нам оно не кажется настолько более удобным, чем обычная запись $xy = yx$ или $[x, y] = 1$, чтобы оправдать введение специального символа.

[22] **Нильс Хендрик Абель** (05.08.1802, Финдё – 06.04.1829, Кристиания, ныне Осло) – замечательный норвежский математик, основные работы которого относятся к теории алгебраических уравнений, теории рядов, теории алгебраических функций. Наряду с Якоби Абель был одним из основателей теории эллиптических функций. В 1824 году получил полное доказательство теоремы о неразрешимости общего уравнения степени 5 в радикалах (теорема Руффини-Абеля). За это достижение он получил стипендию, которая позволила ему совершить поездку в Германию, Италию и Францию. Вынужденный содержать семью и не имея постоянной должности, Абель зарабатывал на жизнь частными уроками. Умер от чахотки в бедности за несколько дней до того, как ему пришло приглашение на должность профессора в Берлинский Университет. Кроме абелевых групп в нашем курсе встречается трюк Абеля, теорема 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: О.Оре, Замечательный математик Нильс Генрих Абель. – ГИФМЛ, М., 1961, с.1–343.

Поэтому в группах обычно избегают пользоваться знаком h/g для обозначения 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[23]

1. Группа как множество с одной операцией. По словам В.И.Арнольда[24], '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 *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 $(f/f)/(g/h) = h/g$.

А именно, Хиллел Фюрстенберг[25] показал[26], 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:

1) для любых $f, g, h \in G$ выполняется равенство $(f/h)/(g/h) = f/g$,

2) для любых $g, h \in G$ уравнение $g/x = h$ разрешимо.

---

[23] А.И.Мальцев, Алгебраические системы. – Наука, М., 1970, с.1–392; стр.98.

[24] **Владимир Игоревич Арнольд** (род. Москва) – великий русский математик, непревзойденный маэстро теории всякого рода особенностей и катастроф. Ученик Колмогорова Арнольд сразу заявил о себе яркими результатами по тринадцатой проблеме Гильберта. Он открыл совершенно замечательные связи между особенностями дифференцируемых отображений и системами корней. В широких кругах известен своими высказываниями о сущности математики, каждое из которых противоречит всем остальным высказываниям. Если исходить из того, что 'воспитанные люди противоречат другим, мудрые противоречат себе' ('Заветы молодому поколению'), то нет, не было и никогда не будет человека, более воспитанного и мудрого, чем Владимир Игоревич. Вот для примера, несколько откровений: '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'. Арнольд написал несколько блистательных книг, в том числе В.И.Арнольд, Теория катастроф. 2-е изд. – Изд-во Моск. ун-та, М., 1983, с.1–80; В.И.Арнольд, Обыкновенные дифференциальные уравнения. – Наука, М., 1971, с.1–239; В.И.Арнольд, Дополнительные главы теории обыкновенных дифференциальных уравнений. – Наука, М., 1978, с.1–304; В.И.Арнольд, Математические методы классической механики. 2-е изд. – Наука, М., 1979, с.1–431; В.И.Арнольд, А.Авец, Эргодические проблемы классической механики. – РХД, Ижевск, 1999, с.1–281; В.И.Арнольд, А.Н.Варченко, С.М.Гусейн-Заде, Особенности дифференцируемых отображений. Т. I, II. – Наука, М., Т.I. Классификация критических точек, каустик и волновых фронтов. – 1982, с.1–304; т.II. Монодромия и особенности интегралов. – 1984, с.1–335.

[25] **Хиллел Фюрстенберг** () – крупнейший израильский математик американского происхождения. Его основные работы относятся к области ... В ?? году совершил алию.

[26] H.Furstenberg, The inverse operation in groups. – Proc. Amer. Math. Soc., 1955, vol.6, p.991–997.

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, [Swi], 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 $\tau : G \times G \longrightarrow G \times G$, 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 [Bo], [Vo], [Hu1]) 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[27] и ужасный[28], определяет группу[29] 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 $(xy)y^{-1} = x$.

Упражнение. Покажите, что определение Мальцева эквивалентно обычному.

Но 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, что подобное заявление 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

[27] **Анатолий Иванович Мальцев** (27.11.1909, Московская область – 07.07.1967, 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 много замечательных 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: А.И.Мальцев, Основы линейной алгебры. 3-е изд. – Наука, М., 1970, с.1–390; и вполне удачный учебник А.И.Мальцев, Алгоритмы и рекурсивные функции. – Наука, М., 1965, с.1–391. Все основные статьи Мальцева собраны в издании А.И.Мальцев, Избранные труды. т. I, II. – Наука, М., 1976, т.I. Классическая алгебра. – с.1–482; т.II. Математическая логика и (очень) общая теория алгебраических систем. – с.1–388.

[28] 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 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, и те деятели, которых он выкармливал, 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. А причины, по которым сибирская школа пыталась административно-террористическими методами навязать такое понимание всей остальной стране, вообще не постигаются разумом.

[29] ibid., стр.97.

тремя операциями: обычной бинарной операцией умножения mult; 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[30]. На этом пути мы получаем определение **группы в категории**. При этом то, что мы называем просто группой – есть *группа 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**;

• аналитические многообразия и аналитические отображения – в этом случае получатся **аналитические группы** более известные широким народным кругам как **группы Ли**;

• алгебраические многообразия и регулярные отображения – в этом случае получатся **алгебраические группы**.

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 $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ (здесь *для поля* K через K^* обозначено $K^\bullet = K \setminus \{0\}$) образуют группы по умножению, называемые **мультипликативными группами** рациональных, вещественных и комплексных чисел, соответственно.

• **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.

• **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,

[30]На русском языке это можно найти, например, в книге И.Букур, А.Деляну, Введение в теорию категорий и функторов, Мир, М., 1972, с.1–259. – Глава IV, в особенности Теорема 4.1.

$\mathbb{T}$ 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 5 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** (alias **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**[31], 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 $e_1, \ldots, e_n$ в векторном пространстве $V = \mathbb{R}^n$ и рассмотрим множество $L = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$ всевозможных *целочисленных* линейных комбинаций векторов $e_1, \ldots, e_n$. Это множество называется **решеткой** в V с базисом $e_1, \ldots, e_n$. Как абстрактная группа L изоморфна свободной

[31] **Трансляция** – **перенос**, **перемещение**, **смещение**, **передвижение**, **сдвиг**. В дальнейшем в нашем курсе встречаются трансвекции, трансвекция это перенос чего-то относительно чего-то другого, в то время как трансляция есть движение как целое.

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 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 биекция снова является биекцией; тождественное отображение является биекцией и служит нейтральным элементом композиции и, наконец, любая биекция обратима, причем обратное отображение также является биекцией. В § 7 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 § 7.

• **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, знаки подчиняются обычному правилу (т.е., например, $(-i)(-k) = ik$), квадраты всех отличных от ± 1 элементов равны -1, 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, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. 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 Главе III, а также во втором и третьем семестрах.

• **Группа Мебиуса.** Рассмотрим группу **дробно-линейных преобразований** сферы Римана $\overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ ('расширенной комплексной плоскости'). Она состоит из всех преобразований вида: $z \mapsto \dfrac{az+b}{cz+d}$, где $a, b, c, d \in \mathbb{C}$ и $ad - bc \neq 0$. Ясно, что композиция двух дробно-линейных преобразований снова является дробно-линейным преобразованием, а обратное преобразование имеет вид $z \mapsto \dfrac{dz-b}{-cz+a}$ (проверьте!). Получающаяся так группа называется **группой Мебиуса**[32] (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.

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** $ax + b$**.** 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** $ax + b$. 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 $(g, u)(h, v) = (gh, gv+u)$. 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

[32] **Август Фердинанд Мебиус** (1790–1868), немецкий геометр, директор обсерватории и профессор университета в Лейпциге, работы которого проложили путь к теоретико-групповой трактовке геометрии. В нашем курсе Вам встретятся функция Мебиуса, формула обращения Мебиуса, формула Мебиуса-Дедекинда, а в курсе топологии – лист Мебиуса.

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**[33]. 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**[34], которая естественно возникает при рассмотрении коммутационных соотношений в квантовой теории.

• **Группа Рубика.** Пусть теперь Γ – группа внутренних вращений кубика Рубика. В Главе X мы сможем 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. М.Э.Ларсен[35,36] вычислил порядок группы внутренних вращений игрушки, известной как **месть Рубика** (Rubik's revenge), представляющей собой куб $4\times4\times4$. Этот порядок 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 $5\times5\times5$.

§ 5. Простейшие конструкции над группами

В этом параграфе мы начнем конкретизацию рассмотренных в Главе 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 $g,h \in H$ множество 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

[33] **Вильгельм Зейтц**, немецкий физик, наиболее известный своими работами в области физики твердого тела, решетка Вигнера-Зейтца,... Не следует путать с выдающимся алгебраистом **Гари Зейтцем**

[34] **Вернер Гейзенберг** (05.12.1901,), – замечательный немецкий физик, один из создателей квантовой механики. В 1925 году Гейзенберг предложил аппарат матричной механики, который позволил произвести первые квантово-механические вычисления, а в 1927 году сформулировал принцип неопределенности.

[35] M.E.Larsen, Gruppeteori, København, 1981, p.37.

[36] M.E.Larsen, Rubik's revenge: the group theoretical solution, – Amer. Math. Monthly, 1985, June–July, p.381–390.

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 предыдущей главе 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 10 мы детально изучим 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 X. 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 X. 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 [На] и [КаМ] 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^{-1} (в смысле умножения, а не композиции!) равна $f^{-1}(x) = f(x)^{-1}$.

§ 6. 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 Г – правильный многогранник в трехмерном пространстве. Так как любое эвклидово движение, сохраняющее Г, сохраняет и двойственный многогранник, можно ограничиться случаем, когда Г тетраэдр, куб или додекаэдр. Легко убедиться, что порядок группы симметрий Г 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,

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

◦ 3 вращения, на угол π, вокруг 3 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 6 плоскостей, проходящих через ребра,

◦ 6 композиций вращений с отражениями, перемещающих все 4 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, известная также под народным названием eigentliche Würfelgruppe, которое объясняет используемое некоторыми авторами для этой группы обозначение W^+), изоморфную S_4.

◦ тождественное преобразование,

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

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

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

◦ 6 вращений, на угол π, относительно 6 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 можно 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.

∘ 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, каждый 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, [CS]), 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 $e_1, \ldots, e_n$. 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, $e_1, \ldots, e_{n+1} \in \mathbb{R}^{n+1}$ 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 $e_1, \dots, e_{n+1}$). 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 $\pm e_1 \pm \dots \pm e_n$. Однако с точки зрения автоморфизмов несколько удобнее рассматривать не гиперкуб, а гипероктаэдр.

• **Гипероктаэдр.** Вершинами гипероктаэдра в n-мерном пространстве являются $2n$ точек $\pm e_1, \dots, \pm e_n$. Таким образом, группу симметрий гипероктаэдра Oct_n можно представлять себе как группу **означенных перестановок** (signed permutations) базиса $e_1, \dots, e_n$, иными словами, отображений, которые посылают каждый базисный вектор e_i либо в какой-то вектор базиса, либо в вектор противоположный к базисному[37]. Группа Oct_n называется **октаэдральной группой**, сказанное выше означает, что ее можно мыслить как подгруппу в S_{2n}. С другой стороны, в Главе X 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.

§ 7. 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[38]

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[39]. 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.

Классификация сопряженных элементов в $\mathrm{SO}(3,\mathbb{R})$ известна как теорема Эйлера[40]. Следующее рассуждение использует понятие собственного числа и простейшие свойства собственных чисел, которые мы доказываем в 3-м семестре (все эти свойства можно найти в

[37] Детальное обсуждение всех симметрий гиперкуба/гипероктаэдра в связи с расположением гиперплоскостей приведено в статье G.Gordon, The answer is $2^n n!$ What's the Question? – Amer. Math. Monthly, 1999, vol.109, August-September, p.636–645.

[38] И.И.Шафрановский, История кристаллографии, XIX век, – Наука, Л., 1980, с.1–324. – стр.232

[39] **Иоганн Гессель**

[40] **Леонард Эйлер** (15.04.1707, Базель – 18.09.1783, 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,

любом учебнике линейной алгебры, например, в [КМ]). 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. *Следующими группами исчерпываются все конечные подгруппы в* $\mathrm{SO}(3,\mathbb{R})$*:*

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[41,42] и использует идею действия группы на

в том числе ? 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, как *Элементы* Эвклида на построение учебников геометрии. В нашем курсе встречаются круги Эйлера, функция Эйлера, тождество Эйлера, углы Эйлера, формула Эйлера, формулы Эйлера-Фурье, 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.

[41] Ф.Клейн, Лекции об икосаэдре и решении уравнений пятой степени, Наука, М., 1989.

[42] **Христиан Феликс Клейн** (25.04.1849, Дюссельдорф – 22.06.1925, 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: Ф.Клейн, История математики в XIX столетии. – Наука,

множестве и понятие орбиты, которое мы обсуждаем в Главе 6. Это доказательство многократно излагалось в книгах на русском языке, см., например,[43], [W2], Приложение A, и [C], 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.

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 § ? Главы 6 установлено, что $l_i m_i = n$ для всех $i = 1, \dots, s$. Для i-й орбиты имеется $m_i(l_i-1)$ пар вида (g,P). Сравнивая два результата, мы получаем основное равенство

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

Разделив это равенство на n, мы получаем

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

или, что то же самое, $\dfrac{1}{l_1} + \dots + \dfrac{1}{l_s} = s - 2 + \dfrac{2}{n}$. 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, $m_1 + m_2 = \dfrac{n}{l_1} + \dots + \dfrac{1n}{l_s} = 2$. 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.

Если $s = 3$, то уравнение принимает вид $\dfrac{1}{l_1} + \dfrac{1}{l_2} + \dfrac{1}{l_3} = 1 + \dfrac{2}{n}$. 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 $\dfrac{1}{l_2} + \dfrac{1}{l_3} = \dfrac{1}{2} + \dfrac{2}{n}$. Оба числа l_2, l_3 не могут быть ≥ 4, так как в этом случае левая часть $\leq \dfrac{1}{2}$, в то время как правая часть $> \dfrac{1}{2}$. Это значит, что $l_2 = 2$ или 3

Рассмотрим вначале случай, когда $l_1 = l_2 = 2$. Тогда уравнение принимает вид $\dfrac{1}{l_3} = \dfrac{2}{n}$. 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 $O(3,\mathbb{R})$.

М., 1989, с.1–454. Ф.Клейн, Элементарная математика с точки зрения высшей, т.I, Арифметика, алгебра, анализ. т.II, Геометрия. – Наука, М., 1987, с.1–431. с.1–416. 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**'. В нашем курсе упоминаются клейновы группы и модель Клейна геометрии Лобачевского.

[43] Л.Р.Форд, Автоморфные функции, – ОНТИ, М.–Л., 1936.

Теорема Гесселя. *Следующими группами исчерпываются конечные подгруппы в* $O(3,\mathbb{R})$*:*
1) 5 типов конечных подгрупп, содержащихся в $\mathrm{SO}(3,\mathbb{R})$*, а именно,* C_n*,* D_n*,* T^+*,* O^+*,* I^+*.*
2) 5 типов прямых произведений конечных подгрупп в $\mathrm{SO}(3,\mathbb{R})$ *и* C_2*:*

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

3) 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, [W2], Приложение B, или [C], с.400–401, а также десятки учебников на английском языке [Bus], [GB], 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[44]*-Майера.* Пусть f обозначает 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[45].

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 (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

[44]**Дьердь Пойа** (13.12.1887, Будапешт –) – замечательный венгерский математик, основные работы которого относятся к теории групп, комбинаторике, теории чисел, теории вероятностей и теории функций. Наиболее известное достижение Пойа в теории групп – это знаменитая **теория перечисления Пойа**, которая излагается в Главе 15 настоящей книги. С 1914 года работал в ETH в Цюрихе, а в 1946 – 1953 годах преподавал в Стэнфорде. На русский язык переведены несколько совершенно замечательных книг Пойа, в частности Д.Пойа, Г.Сеге, Задачи и теоремы из анализа, т.I, т.II, 3-е изд. – Наука, М., 1978, с.1–391; с.1–431. Д.Пойа, Математика и правдоподобные рассуждения. – ИЛ, М., 1957, с.1–535. Д.Пойа, Как решить задачу. –

[45]Г.Смит, Драгоценные камни, Мир, М., 1980, 1–586. Интересно, что на рис.29 этой книги в связи с описанием кристаллографических классов тот же самый многогранник фигурирует под названием **пентагон-додекаэдра**!

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 $G\le O(n,\mathbb{R},A)$. Осталось заметить, что так как A положительно определена, то группа $O(n,\mathbb{R},A)$ сопряжена с $O(n,\mathbb{R})$.

Однако конечные подгруппы в $O(3,\mathbb{R})$ совсем несложно описать и на пути Клейна[46]. 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, стр.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 стр.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.

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.

§ 8. 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[47]

Большинство профессиональных алгебраистов скорее всего охарактеризуют группы T и

[46] M.Senechal, Finding the finite groups of symmetries of the sphere. – Amer. Math. Monthly, 1990, April, p.329–335.

[47] С.Дали, 50 магических секретов мастерства. – ЭКСМО-Пресс, М., 2002, с.1–271, 45-й секрет на стр.259–260.

O не как группы симметрий правильных многогранников, а как **группы Вейля**[48,49] $W(A_3)$, $W(B_3)$ 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 $1152 = 2^7.3^2$ и группу Вейля $W(H_4)$ некристаллографической системы корней типа H_4, порядка $14400 = 2^6.3^2.5^2$. 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 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, чтобы 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 Коксетера[50,51].

---

[48]**Герман Вейль** (09.11.1885, Эльмсхорн – 09.12.1955, Цюрих) – замечательный немецкий математик, один из классиков, 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 Г.Вейль, Избранные труды, Наука, М., 1984, с.1–511.

[49]М.Г.А.Ньюмен, Герман Вейль. – Успехи Мат. Наук., 1976, т.31, N.4, с.239–250.

[50]H.S.M.Coxeter, Regular polytopes, Methuen, London et al., 1963.

[51]**Гарольд Скотт Макдональд Коксетер** (1907? – 2003) – английский математик, с 1936 работавший в Торонто, Канада, основные работы которого относятся к геометрии

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:

$$\tau = \frac{1+\sqrt{5}}{2} = 2\cos\left(\frac{\pi}{5}\right) = 1.6180339887498948482045868343656381177203091798058...,$$

численное значение найдено при помощи `N[GoldenRatio,50]`.

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**[52,53] (golden ratio, golden section) или **числом Фидия**[54], 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[55] '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 обсужда-

---

и теории групп. 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.

[52]Термин der goldene Schnitt весьма позднего происхождения, он появился в Германии в XIX веке.

[53]Уместна некоторая осторожность, так как в полиграфии, живописи и архитектуре 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 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, Г.Гусман, О книге, М., Книга, 1982, с.1–112.

[54]Д.Э.Кнут, Искусство программирования, Т.1, Основные алгоритмы, 3-е изд. – Вильямс, М.–Спб–Киев, 2000, с.1–712, – стр.49, 111.

[55]**Лука Пачоли** (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, 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.

ется, *например*, в Главе 11 книги Коксетера [Co] и его статье[56], и книге Пидо[57]. Из текстов, написанных не математиками, большое впечатление производит манифест Ле Корбюзье[58].

Начнем со следующего общеизвестного наблюдения (см., например, [C?], с.238–240, или [Ber], т.1, с.487–489). Если разделить ребра октаэдра с вершинами $(\pm\tau^2, 0, 0)$, $(0, \pm\tau^2, 0)$, $(0, 0, \pm\tau^2)$, в отношении $\tau : 1$, то получившиеся 12 вершин являются вершинами правильного икосаэдра.

Теорема. *Следующие 12 точек* $(\pm 1, 0, \pm\tau)$, $(\pm\tau, \pm 1, 0)$, $(0, \pm\tau, \pm 1)$ *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 $\dfrac{2\pi}{5}$ 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* $(\pm 1, \pm 1, \pm 1)$, $(\pm\sigma, \pm\tau, 0)$, $(0, \pm\sigma, \pm\tau)$, $(\pm\tau, 0, \pm\sigma)$ *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[59] 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. 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 1 меньшей размерности. Так как все вершины Γ социологически одинаковы, 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 $n = 3$ *тетраэдр* $\{3, 3\}$, *октаэдр* $\{3, 4\}$, *куб* $\{4, 3\}$, *икосаэдр* $\{3, 5\}$, *додекаэдр* $\{5, 3\}$.

---

[56] H.M.S.Coxeter, The golden ratio, phyllotaxis and Wythoff's game. – Scripta Math., 1953, vol.19, p.135–143.

[57] Д.Пидо, Геометрия и искусство, М., Мир, 1979, с.1–332.

[58] Ле Корбюзье, Модулер, в книге Архитектура XX века, М., Прогресс, 1970, с.233–257.

[59] **Шлефли**

При $n = 4$ многогранники $\{3,3,3\}$, $\{3,3,4\}$, $\{4,3,3\}$, $\{3,4,3\}$, $\{3,3,5\}$, $\{5,3,3\}$.

При $n \geq 5$ 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** 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** 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**. Точнее, 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 V), 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**.

§ 9. 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[60]

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 Глава 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 случае *чисто трансцендентного* расширения группа автоморфизмов называется группой Кремона.

• **Группа Кремона**[61]. Пусть $K(x_1, \ldots, x_n)$ – поле рациональных дробей от n переменных над полем K. Группа автоморфизмов $\mathrm{Aut}_K K(x_1, \ldots, x_n)$ называется **группой Кремона**. Эта группа возникает в алгебраической геометрии как группа бирациональных автоморфизмов n-мерного аффинного (или проективного) пространства.

[60]W.M.Kantor, Some consequences of the classification of finite simple groups. – Contemp. Math., 1985, vol.45, p.159–173.

[61]**Луиджи Кремона** (1830, Павия – 1903) – основоположник итальянской геометрической школы. Был профессором Болонского университета и Миланского Политехнического Института. Основные исследования Кремона относятся к проективной геометрии.

• **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 $\Gamma\mathrm{L}(V)$ 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** $E \subseteq \bigwedge^2(X)$ (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**[62] **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

[62] **Рудольф Липшиц** (14.05.1832, Кенигсберг – 07.10.1903, 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 и Берлине и кратковременной работы в 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.

$\lambda, \mu \in \mathbb{R}_+$, такие, что $\lambda d(x,y) \le d(\varphi(x),\varphi(y)) \le \mu d(x,y)$ для любых двух точек $x, y \in X$. Как обычно, множество всех билипшицевых биекций X на себя образует группу относительно композиции.

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

Задача. Биекция φ называется **антитонной**, если она обращает порядок, т.е. из $x \le y$ вытекает, что $\varphi(x) \ge \varphi(y)$. 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.

§ 10. Группы матриц

В этом параграфе мы рассмотрим некоторые группы матриц степени $n = 2$. В дальнейшем в Главах III, IV и V и в третьем семестре 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 $x\in M(2,K)$ посредством

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

Как мы узнаем в Главе 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 всех 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*.

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

2. Некоторые важнейшие подгруппы. А 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**[63] **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 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

$$\mathrm{Sp}(2,K)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}(2,A)\;\middle|\;\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\begin{pmatrix}\overline{d}&-\overline{b}\\-\overline{c}&\overline{a}\end{pmatrix}\right\}$$

[63] **Арман Борель** – замечательный швейцарский математик, член Бурбаки последние ... лет работающий в Принстоне. Основные работы Бореля относятся к алгебре и топологии, в первую очередь к теории групп Ли и алгебраических групп. В честь него называются борелевские подгруппы, борелевские подалгебры и т.д. На русский язык переведено несколько книг Бореля, в том числе А.Борель, Линейные алгебраические группы. – Не путать с французским аналистом начала XX века Эмилем Борелем.

и **ортогональную группу** как

$$\mathrm{O}(2,K)=\left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\mathrm{GL}(2,A)\,\middle|\,\begin{pmatrix}a&b\\c&d\end{pmatrix}^{-1}=\begin{pmatrix}\overline{d}&\overline{b}\\\overline{c}&\overline{a}\end{pmatrix}\right\}.$$

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 главах, посвященных линейной алгебре.

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

$$\left\{\begin{pmatrix}\pm1&x\\0&1\end{pmatrix},x\in\mathbb{Z}/m\mathbb{Z}\right\}$$

изоморфна группе диэдра.

• Группа кватернионов может быть описана как следующая группа матриц в $\mathrm{SL}(2,\mathbb{C})$

$$\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad\pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\quad\pm\begin{pmatrix}0&i\\i&0\end{pmatrix},\quad\pm\begin{pmatrix}i&0\\0&-i\end{pmatrix}.$$

• Физики обычно реализуют группу треугольника $S_3\cong D_3$ как следующую группу матриц в $\mathrm{GL}(2,\mathbb{R})$

$$\begin{pmatrix}\pm1&0\\0&1\end{pmatrix},\quad\frac{1}{2}\begin{pmatrix}1&\pm\sqrt{3}\\\pm\sqrt{3}&-1\end{pmatrix},\quad\frac{1}{2}\begin{pmatrix}-1&\pm\sqrt{3}\\\mp\sqrt{3}&-1\end{pmatrix},$$

(знаки пробегаются согласованно, так что в этой группе действительно 6 элементов). Сопряжение позволяет сделать все коэффициенты матриц рациональными, т.е. вложить S_3 в $\mathrm{GL}(2,\mathbb{Q})$:

$$\begin{pmatrix}\pm1&0\\0&1\end{pmatrix},\quad\frac{1}{2}\begin{pmatrix}1&\pm1\\\pm3&-1\end{pmatrix},\quad\frac{1}{2}\begin{pmatrix}-1&\pm1\\\mp3&-1\end{pmatrix}.$$

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 $\mathbb{Q}$ и вдумайтесь, что бы это могло означать с точки зрения полей характеристики 2.

§ 11. Группы движений

По знаменитому тезису Феликса Клейна[64], геометрия есть теория групп[65]. 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 можно связать две группы, а именно, **ортогональную группу**

$$O(n,K,f)=\{g\in \mathrm{GL}(n,K)\mid gfg^t=f\},$$

проверьте, что это действительно группа! Решение: $(hg)^t=g^th^t$ и $(g^{-1})^t=(g^t)^{-1}$. Кроме того, часто рассматривается **специальная ортогональная группа**

$$\mathrm{SO}(n,K,f)=\{g\in \mathrm{SL}(n,K)\mid gfg^t=f\}=O(n,K,f)\cap \mathrm{SL}(n,K).$$

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 $e_1,\dots,e_n$ пространства K^n посредством $B(e_i,e_j)=f_{ij}$. Как мы узнаем в 3-м семестре, 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

$$f=\begin{pmatrix}e_p&0\\0&-e_q\end{pmatrix}$$

(это утверждение вытекает из теоремы Лагранжа и закона инерции Сильвестра). Иными словами, в $\mathbb{R}^{p,q}$ скалярное произведение двух векторов $x=(x_1,\dots,x_n)$ и $y=(y_1,\dots,y_n)$ определяется посредством

$$B(x,y)=x_1+\dots x_py_p-x_{p+1}y_{p+1}-\dots-x_ny_n.$$

Ортогональная группа пространства $\mathbb{R}^{p,q}$ обозначается через $O(p,q,\mathbb{R})$. Она состоит из всех матриц, для которых

$$O(p,q,\mathbb{R})=\left\{g\in \mathrm{GL}(n,K)\,\middle|\, g\begin{pmatrix}e_p&0\\0&-e_q\end{pmatrix}g^t=\begin{pmatrix}e_p&0\\0&-e_q\end{pmatrix}\right\}$$

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 $\mathrm{SO}(n,\mathbb{R})=O(n,\mathbb{R})\cap \mathrm{SL}(n,\mathbb{R})$

[64]Клейн определял геометрию так: “Дано многообразие и в нем группа преобразований. Требуется развить теорию инвариантов этой группы” – см. Сравнительное обозрение новейших геометрических исследований (‘Эрлангенская программа’ – ‘Erlanger Programm’) – в кн. Об основаниях геометрии, Гостехиздат, М., 1956, с.399–434.

[65]Впрочем, сегодня принято говорить чуть иначе: теория групп есть геометрия.

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**

$$\mathrm{SO}(2,\mathbb{R}) = \left\{ \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} \;\middle|\; \varphi \in \mathbb{R} \right\}.$$

Группа $O(2,\mathbb{R})$ порождается $\mathrm{SO}(2,\mathbb{R})$ и любым отражением, например, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. В то же время группа **лоренцевых вращений**

$$\mathrm{SO}^+(1,1,\mathbb{R}) = \left\{ \begin{pmatrix} \mathrm{ch}(\varphi) & \mathrm{sh}(\varphi) \\ \mathrm{sh}(\varphi) & \mathrm{ch}(\varphi) \end{pmatrix} \;\middle|\; \varphi \in \mathbb{R} \right\}.$$

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 $O(1,1,\mathbb{R})$, 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

$$\left\{ \begin{pmatrix} \cos(\varphi) & \sin(\varphi) & a \\ -\sin(\varphi) & \cos(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \varphi, a, b \in \mathbb{R} \right\}.$$

Полная группа эвклидовых движений плоскости порождается $O(2,\mathbb{R})$ и группой трансляций. Она изоморфна

$$\left\{ \begin{pmatrix} \cos(\varphi) & \pm\sin(\varphi) & a \\ -\sin(\varphi) & \pm\cos(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix} \;\middle|\; \varphi, a, b \in \mathbb{R} \right\}$$

(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[66]**.** В специальной теории относительности рассматривается 4-мерное **пространство Минковского**[67] $\mathbb{R}^{3,1}$. Как множество оно совпадает с 4-мерным простран-

[66]**Гендрик Антон Лоренц** (18.07.1853 – 04.02.1928) – замечательный голландский физик, один из классиков XIX века, создатель электродинамики движущихся сред и электронной теории, один из творцов специальной теории относительности. Большая часть его жизни связана с Лейденским университетом. После окончания этого университета в 1875 году в 1878–1923 годах он был там профессором, а с 1923 года – 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.

[67]**Герман Минковский** (22.06.1864, Алексотас, при Каунасе – 12.01.1909, 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 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. Работа Минковского по математическим основаниям электродинамики и специальной теории относительности оказала огромное влияние на последующее развитие физики. В нашем курсе упоминяются сложение и умножение по Минковскому, пространство Минковского, функционал Минковского, теорема Минковского-Хассе и другие восходящие к нему понятия и результаты.

ством $\mathbb{R}^4$, 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 $x^2 = B(x, x) = -x_0^2 + x_1^2 + x_2^2 + x_3^2$. 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 3-м семестре, 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**:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\varphi) & \sin(\varphi) & 0 \\ 0 & -\sin(\varphi) & \cos(\varphi) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(\varphi) & 0 & \sin(\varphi) \\ 0 & 0 & 1 & 0 \\ 0 & -\sin(\varphi) & 0 & \cos(\varphi) \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(\varphi) & \sin(\varphi) \\ 0 & 0 & -\sin(\varphi) & \cos(\varphi) \end{pmatrix}.$$

$$\begin{pmatrix} \operatorname{ch}(\varphi) & \operatorname{sh}(\varphi) & 0 & 0 \\ \operatorname{sh}(\varphi) & \operatorname{ch}(\varphi) & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \operatorname{ch}(\varphi) & 0 & \operatorname{sh}(\varphi) & 0 \\ 0 & 1 & 0 & 0 \\ \operatorname{sh}(\varphi) & 0 & \operatorname{ch}(\varphi) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} \operatorname{ch}(\varphi) & 0 & 0 & \operatorname{sh}(\varphi) \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \operatorname{sh}(\varphi) & 0 & 0 & \operatorname{ch}(\varphi) \end{pmatrix}.$$

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 $\mathcal{L}_{+\uparrow}$:

$$\begin{pmatrix} 1 & 0 \\ 0 & e \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & e \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -e \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 \\ 0 & -e \end{pmatrix},$$

где e обозначает единичную матрицу порядка 3. Подгруппа в $\mathcal{L}$, порожденная собственной группой Лоренца $\mathcal{L}_{+\uparrow}$ и $\operatorname{diag}(1, -e)$, обозначается $\mathcal{L}_{\uparrow}$ и называется **ортохронной группой Лоренца**, а подгруппа, порожденная $\mathcal{L}_{+\uparrow}$ и $\operatorname{diag}(-1, -e)$, 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 $\operatorname{diag}(-1, e)$, 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[68] 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 посредством $B(x, y) = x_0y_0 - x_1y_1 - x_2y_2 - x_3y_3$.

[68] **Анри Пуанкаре** (29.04.1854, Нанси – 17.07.1912, Париж) – самый знаменитый и продуктивный среди математиков конца XIX века, автор более 500 работ, в том числе ? книг. Работы Пуанкаре охватывают практически всю математику: теория автоморфных функций, геометрия, топология, теория 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. С 1881 года был лектором, а с 1886 года – профессором Парижского университета (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,

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[69].

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 фактор-группе односвязной группы $\mathrm{SL}(2,\mathbb{C})$ по подгруппе $\{\pm e\}$. В действительности, в релятивистской квантовой механике (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** $\mathcal{P} = \mathcal{L} \leftthreetimes \mathcal{T}$ 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 [Ch], 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.

§ 12. 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, вплоть до понятия тензорного произведения модулей.

1. Группа Брауэра[70]**.** Пусть K – поле. Если A и B – *конечномерные* алгебры над K, то их тензорное произведение $A \otimes B$ как векторных пространств превращается в алгебру,

---

классификация особых точек, теорема Пуанкаре о возвращении etc. Камиль Жордан так отозвался о работе Пуанкаре об особых точках дифференциальных уравнений: 'Она вышя 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, так и философских и научно-популярных, в том числе: А.Пуанкаре, Ценность науки. – СПб, 1906; А.Пуанкаре, Наука и гипотеза. – СПб, 1906; А.Пуанкаре, Наука и метод. – СПб, 1910; А.Пуанкаре, Последние мысли. – Пг, 1923; (Эти книги *в основном* вошли в том А.Пуанкаре, О науке. – Наука, М., 1983, с.1–559); А.Пуанкаре, О кривых, определяемых дифференциальными уравнениями. – М.-Л., 1947; А.Пуанкаре, Лекции по небесной механике. – Наука, М., 1965, с.1–571; А.Пуанкаре, Избранные труды. т.I–III. – Наука, М., т. I: Новые методы небесной механики. – 1971, с.1–771; т. II: Топология, Теория чисел. – 1972, с.1–999; т. III: Математика, теоретическая физика. – 1974, с.1–771. 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.

[69] А.Мессиа, Квантовая механика, т.2, Наука, М., 1979, с.1–583, см. с.366–368.

[70] **Рихард Брауэр** – замечательный немецкий алгебраист, создатель теории модулярных представлений конечных групп

если положить $(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1a_2 \otimes b_1b_2$. 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**[71] 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**[72] 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 поле K алгебраически замкнуто, то $\mathrm{Br}(K(t)) = 1$ известно как **теорема Тзена**[73,74]. 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**[75]. 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**[76]. Это вычисление теснейшим образом связано со следующими двумя ключевыми результатами, каждый из которых весьма небанален, а именно **теоремой Алберта**[77]**–Брауэра–Хассе**[78]**–Нетер**[79] и **законом взаимности**

---

[71]**Веддербарн**

[72]**Фердинанд Георг Фробениус** (26.09.1849 – 03.08.1917, Берлин) – замечательный немецкий алгебраист, основные работы которого относятся к теории гиперкомплексных систем, теории матриц, теории представлений конечных групп. После учебы в Берлине и Геттингене и 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 опубликовнных работ посвящено анализу. Однако потом он почти полностью переключился на теорию алгебр и теорию представлений. В нашем курсе встречаются теорема Фробениуса о гиперкомплексных системах, несколько теорем Фробениуса о группах, эндоморфизм Фробениуса и т.д.

[73]**Тзен** () –

[74]Р.Пирс, Ассоциативные алгебры. – М.Мир, 1986, с.1–541, стр.462–463.

[75]Ж.-П.Серр, Локальная теория полей классов, – в книге [Alg], с.201–249, в особенности см. стр.201–215.

[76]Дж.Тэйт, Глобальная теория полей классов, – в книге [Alg], с.250–309, в особенности см. стр.287–294.

[77]**Алберт** () –

[78]**Хельмут Хассе** (25.08.1898, Кассель –) – замечательный немецкий алгебраист и теоретико-числовик. После обучения в Киле, Геттингене и Марбурге в 1925 году он стал профессором в Халле, откуда снова вернулся в Марбург, а в 1934 году возглавил математический институт в Геттингене. Он доказал несколько центральных результатов, относящихся к теории квадратичных форм, таких как теоремы Минковского-Хассе, Хассе-Витта, Хассе-Артина и т.д. В 1950 году начал преподавать в Гамбурге. В нашем курсе встречаются диаграммы Хассе. На русский переведен его классический учебник по теории чисел.

[79]**Эмми Нетер** (23.03.1882, Эрланген – 14.04.1935, Брин Мор) – гениальный немецкий математик, один из основателей (основательниц?) современной алгебры, оказавшая огромное влияние на развитие математики в XX веке. Вероятно, самая замечательная женщина во всей истории математики. Дочь Макса Нетера, ученица Гильберта. Среди ее учеников –

Артина[80].

2. Группа Пикара[81]**.** 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 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 можно 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,

---

мальчиков, как их называли в Геттингене – Эмиль Артин, Бартельс ван дер Варден, ... В нашем курсе встречаются нетеровы кольца и модули, теорема Нетер об изоморфизме. Отец Эмми Нетер – замечательный алгебраический геометр **Макса Нетера** (24.09.1844, Маннхейм – 13.12.1921, Эрланген). Макс Нетер учился в Гейдельберге, Гиссене и Геттингене, с 1871 года работал в Геттингене, а с 1875 года – в Эрлангене, где с 1888 года он стал профессором. Нетер внес глубокий вклад в теорию алгебраических функций, теорию исключения, теории 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.

[80]**Эмиль Артин** (03.03.1898, Вена – 20.12.1962, Гамбург) – гениальный австрийский математик, внесший фундаментальный вклад в развитие алгебры, топологии и теории чисел. В 1921 году Артин защитил диссертацию в области алгебраической теории чисел под руководством Густава Герглотца. В 1925 году Артин стал профессором в Гамбурге. 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. Трудно описать впечатление, которое производят работы Артина, точнее, чем это сделал Анри Картан: 'Emil Artin fut un mathématicien génial. C'était aussi un artiste et, pour tout dire, un homme complet'. Сын Эмиля Артина **Майкл Артин** тоже стал замечательным алгебраистом и алгебраическим геометром. На русския язык переведена блистательная книга Артина Геометрическая алгебра.

[81]**Шарль Эмиль Пикар** (24.07.1856, Париж – 11.12.1941, Париж) – знаменитый французский математик, основные работы которого относятся к теории функций комплексного переменного и теории дифференциальных уравнений. После окончания Ecole Normale в Париже короткое время преподавал в Тулузе, а потом вернулся в Париж, где был профессором анализа. Теоремы Пикара о распределении значений аналитических функций, теория Пикара-Вессио дифференциальных уравнений. В нашем курсе встречаются группы Пикара в двух различных смыслах. Пикар был зятем Эрмита??? – от него пошла поговорка о том, что 'математические способности передаются от тестя к зятю'.

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 проективных модулей над R. По отношению к операции прямой суммы $(P,Q) \mapsto P \oplus Q$ это множество образует моноид, нейтральным элементом которого является класс 0. В главе 1 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, [M], 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 $K_0(R)\cong\mathbb{Z}$.

4. Группа классов идеалов. Напомним, что если $A,B \trianglelefteq R$ – два идеала кольца 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. [M], 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 ([Alg], 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 $x,y\in R^\bullet$. 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 $\mathrm{Cl}(R)=1$.

§ 13. Группы в топологии

В настоящем пункте 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 обратен пути f *с точностью до гомотопии*, 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**[82] 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[83] 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 $\mathbb{I}^n$. 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

[82] **ван Кампен** ()

[83] **Гуревич** ()

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 $f^{-1} : \mathbb{I}^n :\longrightarrow X$, $t \mapsto f(1-t_1, t_2, \dots, t_n)$. Таким образом, $\pi_n(X, x)$ образует группу, которая называется **n-й гомотопической группой** пространства X в точке x. Замечательное отличие случая $n \ge 2$ от случая $n = 1$ состоит в том, что все группы $\pi_n(X, x)$, $n \ge 2$, 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 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 $n \ge 1$ 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 $i \ge 1$. 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 $i \ne 0, n$. Вот эффектное приложение функториальности групп гомологий, с которого начинается каждый курс алгебраической топологии. Классическая **теорема Брауэра**[84] 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,

[84]**Люйтцен Эгбертус Ян Брауэр (Brouwer)** (27.02.1881, Overschie – 02.12.1966, Амстердам) – 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 интуициони-

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 $g\circ \hookrightarrow\colon \mathbb{S}^{n-1} \hookrightarrow \mathbb{B}^n \longrightarrow \mathbb{S}^{n-1}$ 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 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.

§ 14. Квазигруппы и латинские квадраты

> Нет сомнения, что время так же относится к весу, как бремя к бесу.
>
> Велимир Хлебников, ‘Ка’.

Как мы знаем, ассоциативность произвольной операции трудно усмотреть из таблицы Кэли[85]. 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

стов 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 (Война мышей и лягушек. – М.-Л., 1936). Эта война закончилась оргвыводами в отношении Брауэра, изгнанием его из редакции Mathematische Annalen и пр.

[85] **Артур Кэли** (16.08.1821, Ричмонд – 26.01.1895, Кембридж) – замечательный английский алгебраист, один из самых продуктивных математиков XIX века, наряду с Галуа и Гамильтоном один из основателей современной алгебры, в особенности линейной алгебры и алгебраической геометрии. Юрист по профессии, в 1860-х годах он полностью переключился на математику и был профессором в Кембридже. Его самые знаменитые работы относятся к теории матриц, теории групп, теории инвариантов, проективной геометрии, теории функций и комбинаторике. В 1842 году определил умножение матриц, в 1843 году обобщая конструкцию гамильтоновых кватернионов он построил неассоциативную 8-мерную алгебру с делением над полем вещественных чисел, известную как ‘алгебра Кэли-Грейвса’ (alias ‘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.

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 `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[86]. 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, таблица[87]

$*$	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 ей 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 $y_1v_1 = y_2v_2$.

[86] Д.Дюге, Теоретическая и прикладная статистика, 1972, Ч.II, Гл. IV.

[87] Ф.Кертеси, Введение в конечные геометрии, 1976, § 1.14.

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.

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 $x * y = {}^x y = xyx^{-1}$. Показать, 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?

Тема 2. ПОДГРУППЫ И СМЕЖНЫЕ КЛАССЫ

Теперь мы начинаем систематически конкретизировать для групп основные конструкции общей алгебры. В этой и двух следующих главах мы определим

★ подобъекты,

★ фактор-объекты,

★ морфизмы в категории групп.

В настоящей главе мы определим 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.

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 Главы 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* (Teiler, 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**[88] H.

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).

[88] Заметим, что правильный английский перевод ‘overgroup’, употребление в этом контексте термина ‘supergroup’ производит на понимающего человека совершенно анекдотическое впечатление.

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,

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

– **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 выполнения включения $HH^{-1} \subseteq H$.

3. Первые примеры подгрупп. 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, 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 Главе 7 (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: $\{\pm 1\}$, $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$.

• **Подгруппы 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

$$A_4 = \{e, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

§ 2. Централизаторы м нормализаторы

Сейчас мы введем две конструкции, которые позволят строить много интересных примеров подгрупп в неабелевых группах.

1. 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 в Главе 3 мы докажем гораздо более общий результат. 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

2. 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) $C_H(x) = G_G(x) \cap H$. Справедливы ли аналогичные утверждения для нормализаторов?

3. Примеры централизаторов. Вычислим централизаторы некоторых матриц.

• **Централизатор регулярной полупростой матрицы**. Диагональная матрица $d = \mathrm{diag}(\varepsilon_1, \dots, \varepsilon_n)$ 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

$$C_{\mathrm{GL}(n,K)} \begin{pmatrix} 1 & 1 & \dots & 0 \\ 0 & 1 & \ddots & 0 \\ 0 & 0 & \ddots & 1 \\ 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} a & b & \dots & c \\ 0 & a & \ddots & \vdots \\ 0 & 0 & \ddots & b \\ 0 & 0 & \dots & a \end{pmatrix}.$$

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**. 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. 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, то $C_G(X)$ подгруппа в G.

5. Нормализатор подмножества. Пусть снова $X \subseteq G$ – любое подмножество в G. Определим **нормализатор** X как множество элементов, которые коммутируют с X *в целом*:

$$N_G(X) = \{g \in G \mid gX = Xg\}.$$

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 Главах 5 и 7. 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 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?

6. 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[89,90].

Задача. Проверьте, что $\mathrm{Comm}_G(H)$ – группа, содержащая $N_G(H)$.

§ 3. Порядок элемента и экспонента группы

1. Степени элемента, циклические подгруппы. Если G – любая группа, то мы можем определить степени 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

[89] G.A.Margulis, Discrete subgroups of semisimple Lie groups. Springer, Berlin et al., 1991.

[90] N.A'Campo, M.Burger, Réseaux arithmétiques et commensurateur d'après G.A. Margulis. – Invent. Math., 1994, vol.116, N.1–3, p.1–25.

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 $o(g)$ 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 $\neq 1$ 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[91]**.** *Если $p \in \mathbb{P}$ простое, то $(p-1)! \equiv -1 \pmod p$.*

Доказательство. Примените результат предыдущей задачи к группе $A = (\mathbb{Z}/p\mathbb{Z})^*$.

[91] **сэр Джон Уилсон (sir John Wilson)** (1741, Вестморленд – 1793) – английский юрист, врач и математик-любитель. В математике Уилсон занимался главным образом теорией чисел. Обычно его фамилия *ошибочно* передается по русски как Вильсон (Watson переводится как Ватсон и пр.) Мы сознательно сохраняем это традиционное написание, чтобы отличать сэра Джона Вильсона от одного из ведущих современных спецаилистов по теории бесконечных групп Джона Уилсона (J.S.Wilson), несколько теорем которого упоминаются в Главе 7.

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** группы G. Такого m может не существовать, но если оно существует, то говорят, что группа G имеет **конечную экспоненту**. 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.

§ 4. 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 $\langle X\rangle$ 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 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 здесь 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 $\langle G \setminus H\rangle = G$.

2. Формула произведения. Чему равен порядок произведения двух подмножеств в группе? Для подгрупп ответить на этот вопрос довольно легко и сейчас мы проведем соответствующее рассуждение, так как оно хорошо иллюстрирует, как именно используется тот факт, что какое-то подмножество является подгруппой.

Теорема (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 $\phi : F \times H \longrightarrow FH$, $(f, h) \mapsto fh$. 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.

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 $|X| + |Y| = q + 1 > q = |G|$.

§ 5. 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 пересечение $F \cap H$ тоже является подгруппой в G, которая 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. Этот термин несколько двусмысленен, 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 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, эта 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 § 8.

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[92] **(Ope**[93]**).** Пусть G – конечная группа, $F, H \leq G$. Предположим, что индексы $|G : F|$ и $|G : H|$ взаимно просты. Тогда $FH = HF = G$.

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**[94]. 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[95].

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.

§ 6. 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 $\vee$.

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 $L(D, G)$ обозначается решетка **промежуточных подгрупп** (intermediate subgroups), т.е. подгрупп в G, содержащих D. В этих обозначениях $L(G) = L(1, G)$.

2. Модулярный закон. Самый важный факт о решетке подгрупп состоит в следующем

Теорема (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 $FH = FK$ и $F \cap H = F \cap K$, то $H = K$.*

Доказательство. В самом деле,

$$K = FK \cap K = FH \cap K = (F \cap K)H = (F \cap H)H = H.$$

Стоит, однако, обратить внимание, что здесь речь идет о произведении, а не о порождении подгрупп F и H!

---

[92] O.Ore, Contributions to the theory of groups. – Duke Math. J., 1939, vol.5, p.431–460. стр.436

[93] **Ope** ()

[94] В настоящее время такие группы обычно называются permutable, но перевод этого термина на русский неочевиден, поэтому мы сохраняем оригинальный термин Ope.

[95] R.Schmidt, Subgroup lattices of groups. – de Gruyter, Berlin, 1994, стр.202.

Следствие 2. *Если в условиях теоремы F и H перестановочны, то*

$$\langle F, H\rangle \cap K = \langle F \cap K, H\rangle.$$

3. 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 $F = H$.

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 несколько примеров, много дальнейших примеров встретится нам в Главах 5 и 7:

- Любая подгруппа простого индекса максимальна;
- 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 $K \neq \mathbb{F}_3, \mathbb{F}_5$.

§ 6. 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. $G = \{g^n, n \in \mathbb{Z}\}$. Следующий результат был фактически 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 гомоморфзим 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 $G \cong \mathbb{Z}$, 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 $o(g)$ 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 $\phi(n)$ 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 порядка n в G существует единственная подгруппа порядка d.*

Доказательство. Пусть $d|n$, 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 и, значит, $H = \langle g^m \rangle$ для некоторого m. По теореме порядок подгруппы, порожденной g^m, равен $d = n/\gcd(m, n)$. В частности, $(n/d)|m$. Это значит, что $H = \langle g^m \rangle$ содержится в подгруппе, порожденной $g^{n/d}$, но, так как их порядки совпадают, то $H = \langle g^{n/d} \rangle$.

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 $p \in \mathbb{P}$.

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 $\phi(d)$ 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 $\phi(d)$ образующих.

Заметим, что это следствие дает еще одно доказательство **сумматорной формулы** для функции Эйлера $\sum_{d|n} \phi(d) = n$. В самом деле, каждый элемент $h \in G$ конечной циклической группы порядка n имеет порядок $d|n$, причем число элементов порядка d равно $\phi(d)$. 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 2 можно сформулировать и чуть иначе.

Следствие 4. *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 G существует единственная подгруппа H порядка $(n/d)|n$, а именно, подгруппа, порожденная $g^{n/(n/d)} = g^d$. Ясно, что фактор-группа G/H порождена классом gH, причем $g^d \in H$.

§ 6. 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 этой связи возникают две противоположных проблемы.

Найти группу H, зная какую-то систему ее образующих X. Особенно широко этот способ 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[96]**.** Пусть d – делитель числа 12. Возьмем колоду из d карт, занумерованных $1, \ldots, d$, и применим к ней две перестановки:

- **Переворачивание**, т.е. отображение $i \mapsto d - i$.
- **Тасование Монжа**[97], т.е. отображение $i \mapsto \min(2i, 2d + 1 - 2i)$.

Задача. Докажите (или проверьте экспериментально!), что для $d = 1, 2, 3, 4, 6$ порядок подгруппы в S_d, порожденной переворачиванием и тасованием Монжа,

[96] P.Diaconis, R.L.Graham, W.M.Kantor, The mathematics of perfect shuffles. – Adv. Appl. Math., 1983, vol.4, p.175–196.

[97] **Гаспар Монж** (10.05.1746, Beaune – 28.07.1818, 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. Принимал активное участие во французской революции, в 1892–1893 годах был морским министром. Как друг Наполеона стал директором египетского музея и одной из самых престижных школ 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!

равен 1,2,6,12 и 120, соответственно. Отождествите[98] 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 S_n и A_n. Следующие 5 результатов доказаны в Глава 5.

• Симметрическая группа S_n порождается множеством циклов $(i_1 \dots i_r)$, $i_1 < \dots < i_r$.

• 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 $(ij)(hk)$, $|\{i,j,h,k\}| = 4$.

4. Порождение линейных групп. Следующие результаты доказаны в Главе 7.

• Для поля группа $\mathrm{SL}(n,K)$ порождается множеством элементарных трансвекций $t_{ij}(1) = e + \xi e_{ij}$, $\xi \in K$, $1 \leq i \neq j \leq n$.

• Для поля группа $\mathrm{GL}(n,K)$ порождается множеством элементарных преобразований, состоящим из элементарных трансвекций $t_{ij}(1) = e + \xi e_{ij}$, $\xi \in K$, $1 \leq i \neq j \leq n$, и элементарных псевдоотражений $d_i(\varepsilon) = e + \varepsilon e_{ii}$, $\varepsilon \in K^*$, $1 \leq i \leq n$.

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 10).

• Свободная абелева группа $\mathbb{Z}^n$ конечного ранга.

[98] 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**.

• 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, то группа G бесконечна. Эта группа обозначается D_∞ и называется **бесконечной диэдральной группой**.

А следующие группы не могут быть конечно порожденными:

• Свободная абелева группа $\mathbb{Z}^{\aleph_0}$ счетного ранга;

• Аддитивная группа $\mathbb{Q}^+$ порождена $\{1/n, n \in \mathbb{N}\}$;

• Мультипликативная группа μ_{p^∞} порождается первообразными корнями ζ_{p^n} степеней p^n, $n \in \mathbb{N}$;

• Мультипликативная группа $\mathbb{Q}^*$ 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 для 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 $e_{12} + e_{23} + \dots + e_{n-1,n} + (-1)^n e_{n1}$

§ 7. Смежные классы

В настоящем параграфе мы свяжем с каждой подгруппой $H \le G$ два отношения эквивалентности на G.

1. Смежные классы. Сейчас мы введем одно из ключевых понятий теории групп, которое впервые 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 вставляет дополнительные 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*[99]. 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` (в старых книгах говорится также `Nebengruppe`). Этот термин в большинстве языков образуется от нового корня и является одним их самых трудных для перевода, например, по-английски смежный класс называется `coset` (сомножество), 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 [Ha], Фаддеев[100] [F] и Шафаревич[101] [Sh]. В то же время, под влиянием Ку-

[99]'Which is the master, that's the question' – Humpty Dumpty.

[100]**Дмитрий Константинович Фаддеев** () – выдающийся русский алгебраист, основатель Петербургской алгебраической школы (супербренд **Д.К.**). Основные работы Фаддеева относятся к алгебраической теории чисел, алгебраической геометрии, гомологической алгебре, линейной алгебре, теории колец и теории представлений. Ранние работы Фаддеева относятся к геометрии теории Галуа (бренд **Делоне–Фаддеев**). Гомоологии в группах (бренд **Боревич–Фаддеев**) С моей точки зрения работы Д.К., его вклад в алгебру и его роль в развитие алгебры в нашей стране **драматическим** образом недооценены. Мне конечно, трудно оценивать Фаддеева объективно: *у собаки есть хозяин, у волка есть бог, а у человека есть учитель*. Так вот, Фаддеев был общим учителем всех Петербургских алгебраистов моего поколения. Эта книга представляет собой скромный омаж (или, как теперь принято говорить, tribute) памяти Д.К. Все в этой книге (кроме стиля!) является плодом того понимания математики, которому я обязан школе Д.К. Д.К. был образцом русского интеллектуала и профессионала высочайшего класса. В филармонии я каждый раз встречал Дмитрия Константиновича, во время исполнения он тщательно сверял происходящее с партитурой. Он писал романсы – и слова к ним, на немецком языке. Кроме цитированного во введении учебника [F] и сборника задач (бренд **Фаддеев–Соминский**) Д.К. написал еще несколько книг Д.К.Фаддеев, В.Н.Фаддеева, Вычислительные методы линейной алгебры. – Физматгиз, М.-Л., 1963. (бренд **Фаддеев–Фаддеева**) Многие работы Фаддеева по линейной алгебре написаны им совместно с супругой **Верой Николаевной Фаддеевой**. Их сын **Людвиг Дмитриевич Фаддеев** тоже стал совершенно замечательным математиком, основные работы которого относятся к различным аспектам математической физике и связанным с ней анализу и алгебре: теория рассеяния, квантовые группы и т.д. В ... годах Л.Д.Фаддеев был Президентом Международного Математического Союза.

[101]**Игорь Ростиславович Шафаревич** () – выдающийся русский алгебраист, основатель Московской алгебраической школы. Основные работы Шафаревича относятся к алгебраической теории чисел, алгебраической геометрии. (бренд **Шафаревич–Пятецкий-Шапиро**) (бренд **Кострикин–Шафаревич**) (бренд **Рудаков–Шафаревич**) Кроме цитированного во введении обзора 'Основные понятия алгебры' Шафаревич написал два замеча-

роша[102] [Kur] кафедра алгебры Московского Университета называет *Hx правым* смежным классом, см., например, Кострикин[103] [K1], [K2] и Винберг[104] [Vi2].

2. Разбиение на смежные классы. Сейчас мы покажем, что смежные классы по подгруппе H задают разбиение группы G.

Теорема. *Группа G является дизъюнктным объединением всех различных левых (или правых) смежных классов по подгруппе H.*

тельных учебника: З.И.Боревич, И.Р.Шафаревич, Теория чисел. 3-е изд. – Наука, М., 1985, с.1–503 (супербренд **Боревич–Шафаревич**); И.Р.Шафаревич. – Основы алгебраическая геометрии. 2-е изд., Т.1 и 2. – Наука, М., 1988, с.1–351, 1989, с.1–304. Основные математические работы Шафаревича собраны в третьем томе его трудов: И.Р.Шафаревич. Сочинения в трех томах, т.3. – АО 'Прима В', М., Часть 1: Теория чисел и разное, 1996, с.1–415; Часть 2: Алгебра и алгебраическая геометрия, 1996, с.1–637. Кроме математических работ Шафаревич написал громадное количество философских, исторических, социологических и философских произведений: 'Русофобия', 'Два пути к одному обрыву', ... Эти сочинения вызвали неоднозначную реакцию коллег, как в России, так и на Западе.

[102]**Александр Геннадьевич Курош** (– 18.05.1971, Москва) – известный русский алгебраист, профессор Московского университета, основные работы которого посвящены абстрактной теории групп, абстрактной теории колец и очень общей алгебре. В предвоенные годы им и его учениками получены весьма замечательные теоремы о подгруппах свободных и амальгамированных произведений, теоремы Куроша и Грушко, которые мы упоминаем в Главе 10. Из других работ Куроша наибольшей известностью пользуются его статьи по теории радикалов, **радикал Амицура-Куроша**, обобщенным разрешимым группам (бренд **Курош-Черников**) и написанная им совместно с А.Х.Лифшицем и Е.Г.Шульгейфером обзорная статья по теории категорий (Успехи Мат. Наук, 1960, т.15, с.3–52). Влияние Куроша на развитие алгебры в СССР на определенном этапе было чрезвычайно велико, но с сегодняшних позиций выглядит весьма неоднозначно. Несомненно, Курош был одним из главарей и идейных вдохновителей шайки 'преступных алгебраистов'. Кроме крайне неудачной книжки по теории групп Курош записал еще лекции по общему курсу алгебры для 1-го курса: А.Г.Курош, Курс высшей алгебры. – Наука, М., 1975. В первом издании эти лекции выглядели вполне прилично, но дальше с каждым изданием становились все хуже и хуже. Кроме того, Курош сфабриковал два уже совершенно одиозных программных сочинения в духе товарищества передвижных выставок: А.Г.Курош, Лекции по общей алгебре. 2-е изд. – М., 1973, с.1–396; А.Г.Курош, Общая алгебра. – М., 1973. Впрочем, даже у Александра Геннадиевича можно найти весьма проникновенные суждения, основанные на большом личном опыте: 'в такой науке, как общая алгебра, не нужно большого ума, чтобы создавать новые объекты изучения' ('Общая Алгебра', стр.9).

[103]**Алексей Иванович Кострикин** () – выдающийся русский алгебраист, один из самых блестящих представителей Московской алгебраической школы. Основные работы Кострикина относятся к теории алгебр Ли, теории групп, и теории представлений. Ученик Чудакова и Шафаревича. Работы Кострикина по ослабленной проблеме Бернсайда. Эти работа была блестяще продолжена Ефимом Исааковичем Зельмановым. Кострикин внес совершенно выдающийся вклад в теорию модулярных алгебр Ли. Именно его работы превратили эту область из набора разрозненных примеров в Сформулированная им совместно с Шафаревичем **гипотеза Кострикина-Шафаревича** стала программой работы всех специалистов в этой области на много десятилетий и в дальнейшем блестяще подтвердилась. Работы **Кострикина–Кострикина–Уфнаровского** (супербренд 'отец, сын и святой дух') посвященные решению **проблемы Винни-Пуха** об ортогональных разложениях ('Зачем говорим мы слово $A_5, \dots$') привели к открытию бесконечной серии замечательных решеток в размерностях $p^2 - 1$, первые две из которых – это E_8 и решетка Лича. Книги: Алгебра, Кострикин–Манин, Вокруг Бернсайда. – Наука, М., 1986, с.1–232.

[104]**Эрнест Борисович Винберг** () – выдающийся русский алгебраист, один из самых блестящих представителей Московской алгебраической школы. Основные работы Винберга относятся к теории групп и алгебр Ли, теории алгебраических групп, неэвклидовой геометрии и теории дискретных групп. Кроме цитированных во введении учебников алгебры [Vi1], [Vi2] Эрнест Борисович написал еще несколько замечательных книг, в том числе [Vin] и [VO].

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**. 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. 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.

§ 8. 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. *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. Аксиома выбора утверждает, что для каждого отношения эквивалентности существует трансверсаль.

Определение. *Трансверсаль к отношению сравнимости по модулю H слева/справа называется* **системой представителей** *левых/правых смежных классов G по H.*

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 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

$X = \{x_1, \ldots, x_n\}$ – система представителей левых смежных классов, то группа G представляется в виде дизъюнктного объединения $G = Hx_1 \sqcup \ldots \sqcup Hx_n$.

3. Системы общих представителей. В 1935 году Филипп Холл[105] заинтересовался вопросом, 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. Сформулируем без доказательства следующий классический результат, который можно найти в любой серьезной книжке по комбинаторике, например, в книге[106] Маршалла Холла[107].

Теорема Ф.Холла. *Предположим, что подгруппа $H \leq G$ конечна. Тогда существует система общих представителей левых и правых смежных классов G по H.*

В частности, это всегда так, если сама группа G конечна. Система общих представителей существует и при некоторых других предположениях относительно подгруппы H, например, если ее *индекс* конечен. Точнее, имеет место следующий результат[108].

Теорема Оре. *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.*

§ 9. Теорема Лагранжа

В этом параграфе мы докажем важнейшие равенства, связывающие индексы подгрупп, а в следующем параграфе извлечем из них интересные неравенства.

1. Теорема Лагранжа[109]. Следующий результат, несмотря на свою простоту, исключительно важен.

Теорема Лагранжа. *Если $H \leq G$, то $|G| = |H||G : H|$.*

Доказательство. Как всегда, правильный способ доказательства равенства двух чисел состоит в установлении биекции между некоторыми множествами.

---

[105] **Филипп Холл** () –

[106] М.Холл, Комбинаторика, М. 1970, Гл.V.

[107] **Маршалл Холл** () –

[108] O.Ore, On coset representatives in groups. – Proc. Amer. Math. Soc., 1958, vol.9, p.665–670.

[109] **Джузеппе Лодовико Лагранж** (25.01.1736, Турин – 10.04.1813, Париж) – наряду с Эйлером самый великий математик XVIII века. Часто Лагранжа называют на французский манер 'Жозеф Луи', но в действительности он был итальянцем, который работал 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 работа по механике и астрономии и сыграла ключевую роль в дальнейшем развитии физики и послужила 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 курсе математического анализа встречается остаточный член ряда Тейлора в форме Лагранжа, лагранжиан и т.д.

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[110], 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[111]). *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. Контр-пример 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[112] определил все подгруппы симметрической группы S_5. В частности, он показал, что

---

[110] J.L.Lagrange, Réflexions sur la résolution algébriques des équations. 1771. – Oeuvres, t.3, p.205–421.

[111] **Пьер де Ферма** (17.08.1601, Beaumont de Lomage – 12.01.1665, Castres) – величайший математик XVII века, основатель теории чисел, алгебраической геометрии и дифференциального исчисления. Ферма изучал юриспруденцию и в 1630 году купил себе должность советника парламента Тулузы. 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. В нашем курсе встречаются десятки восходящих к нему понятий: декартовы координаты, дифференцирование, простые числа Ферма, теорема Ферма, кольцо двойных чисел, и т.д. Долгое время самая знаменитая проблема математики, супербренд над супербрендами, shir hash shirim, **большая** alias **последняя** alias **великая теорема Ферма**.

[112] **Паоло Руффини** (23.09.1765, Валентано – 10.05.1822, Модена) итальянский врач и математик-любитель. Первым доказал неразрешимость общего 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 называется теоремой Руффини-Абеля. Однако как раз в части, посвященной группам перестановок, доказательство Руффини совершенно безупречно. Другие его математические работы относятся к теории алгебраических кривых и методам вычислений.

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.

Задача. Докажите, что у группы A_4 нет подгруппы порядка 6.

Решение (T.-L.Shen, [Ro], 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 $F = 1$.

§ 10. Теорема Пуанкаре

1. Индекс пересечения. Сейчас мы выведем из мультипликативности индекса важное следствие.

Теорема. *Если $F, H \leq G$, то $|G : (F \cap H)| \leq |G : F||G : H|$.*

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, $x = y$.

Задача. Докажите, что если $F, H \leq G$, 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) $FH = G$.

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 $H_1, \ldots, H_n$ – подгруппы группы G, имеющие в ней конечный индекс, то их пересечение $H_1 \cap \ldots \cap H_n$ тоже подгруппа конечного индекса в G.*

Сам Пуанкаре формулировал эту теорему следующим образом. 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, то отношение соизмеримости является отношением эквивалентности.

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 $g_1, \dots, g_n$ – трансверсаль к H в G. Тогда все подгруппы H^{g_i} имеют индекс n в G. Тем самым, по теореме Пуанкаре подгруппа $F = H^{g_1} \cap \dots \cap H^{g_n} \trianglelefteq G$ имеет там конечный индекс.

§ 11. 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**[113].

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 $\phi : F \dashrightarrow H$ 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).

[113]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**.

Задача. Проверьте, что две группы H и G в том и только том случае виртуально изоморфны, $H \approx G$, когда в них существуют подгруппы конечного индекса $H' \leq H$, $G' \leq G$ изоморфные в обычном смысле, $H' \cong G'$.

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 $\mathrm{GL}(n, \mathbb{Q})$.

§ 12. Виртуальные свойства

В соответствии с приведенными в предыдущем параграфе определениями, говоря, что группа G **виртуально** обладает каким-то свойством $\mathcal{C}$, мы всегда имеем в виду, что она обладает этим свойством в категории виртуальных групп. Для большинства реально рассматриваемых свойств это означает просто, что группа G имеет подгруппу H *конечного индекса*, обладающую этим свойством $\mathcal{C}$. Если свойство $\mathcal{C}$ наследуется подгруппами группы H, то по теореме Пуанкаре это условие эквивалентно формально более сильному условию, что G содержит *нормальную* подгруппу конечного индекса H, обладающую свойством $\mathcal{C}$. В последнем случае говорят также, что группа G **почти** обладает свойством $\mathcal{C}$.

Перечислим некоторые наиболее часто используемые виртуальные свойства:

• Группа G **виртуально без кручения = почти без кручения**, если в ней есть (нормальная) подгруппа конечного индекса H не имеющая кручения.

• Группа G **виртуально свободная = почти свободная**, если в ней есть свободная (нормальная) подгруппа H конечного индекса.

• Группа G **виртуально абелева = почти абелева**, если в ней есть абелева (нормальная) подгруппа H конечного индекса.

Аналогичный смысл вкладывается в выражения **виртуально нильпотентная**, **виртуально полициклическая**, **виртуально разрешимая**, etc.

Задача. Как Вы думаете, почему в литературе не упоминаются виртуально конечные и виртуально периодические группы?

§ 12. Локальные свойства

В теории групп термин **локальные свойства** употребляется в двух абсолютно различных смыслах. В теории *бесконечных* групп говорят, что группа G **локально** обладает свойством $\mathcal{C}$, если любая ее *конечно порожденная* подгруппа обладает этим свойством. В настоящем параграфе мы обсуждаем локальные свойства только в этом смысле. Если свойство $\mathcal{C}$ наследуется подгруппами группы H, то группа из класса $\mathcal{C}$ автоматически является группой *локально* из класса $\mathcal{C}$. Ясно, что конечная группа, локально обладающая каким-то свойством, на самом деле обладает этим свойством. Поэтому для конечных групп это определение бе ссмысленно[114].

• Группа G называется **локально конечной**, если любая ее конечно порожденная подгруппа H конечная. Любая локально конечная группа является периодической. Обратное, вообще говоря, неверно (**общая проблема Бернсайда**).

• Группа G называется **локально циклической**, если любая ее конечно порожденная подгруппа H циклическая. Примерами (нециклических) локально циклических групп являются квазициклические группы μ_{p^∞} и группа $\mathbb{Q}$.

[114]В теории *конечных* групп локальными принято называть свойства, выражаемые в терминах нормализаторов p-подгрупп.

• Группа G называется **локально свободной**, если любая ее конечно порожденная подгруппа H свободна. Примерами локально свободных групп являются свободные группы (теорема Нильсена–Шрайера!) и группа $\mathbb{Q}$, которая сама отнюдь не является свободной! Класс локально свободных групп замкнут относительно свободного произведения, так что вместе с группой $\mathbb{Q}$ он содержит и свободное произведение $\mathbb{Q} * \mathbb{Q}$.

• Группа G называется **локально нильпотентной**, если любая ее конечно порожденная подгруппа H нильпотентная.

• Группа G называется **локально разрешимой**, если любая ее конечно порожденная подгруппа H разрешимая.

В аналогичном смысле используется термин **локально сверхразрешимая**, etc.

Задача. Как Вы думаете, почему в литературе не упоминаются локально абелевы, локально неабелевы, локально периодические группы, группы локально без кручения?

§ 12. Резидуальные свойства

Говорят, что группа G **резидуально** обладает каким-то свойством $\mathcal{C}$, если пересечение ядер гомоморфизмов $\phi : G \longrightarrow H$ в группы, обладающие свойством $\mathcal{C}$, равно 1. Иными словами, утверждается, что для любого $g \in G$, $g \neq 1$, существует нормальный делитель $F \trianglelefteq G$ такой, что фактор-группа G/F обладает свойством $\mathcal{C}$ и при этом $g \notin F$. В этом случае Некоторые авторы предпочитают говорить, что группа G **аппроксимируется** группами из класса $\mathcal{C}$.

Предостережение. Строго говоря, следовало бы уточнить, что речь здесь идет об аппроксимируемости **относительно равенства**! Кроме того, в сугубой теории бесконечных групп рассматривается аппроксимация относительно других отношений на G, скажем, сопряженности. А именно, группа G **аппроксимируется** группами из класса $\mathcal{C}$ **относительно сопряженности**, если для двух любых несопряженных элементов $x, y \in G$ существует гомоморфизм $\phi : G \longrightarrow H$ в группу, обладающую свойством $\mathcal{C}$, такой, что $\phi(x)$ и $\phi(y)$ не сопряжены в H.

В терминах главы ? это значит, что группа G является *подпрямым произведением* групп из класса $\mathcal{C}$.

• Группа G называется **резидуально конечной = финитно аппроксимируемой**, если пересечение ее нормальных подгрупп конечного индекса равно 1.

Задача. Докажите, что любая подгруппа резидуально конечной группы сама резидуально конечна.

Задача. Докажите, что группа $\mathrm{GL}(n, \mathbb{Z})$ резидуально конечна.

Решение. В самом деле, пересечение главных конгруэнц-подгрупп $\mathrm{GL}(n, \mathbb{Z}, m\mathbb{Z})$, $m \in \mathbb{N}$, равно 1. Осталось заметить, что фактор-группа $\mathrm{GL}(n, \mathbb{Z})/\mathrm{GL}(n, \mathbb{Z}, m\mathbb{Z}) = \mathrm{SL}^{\pm}(n, \mathbb{Z}/m\mathbb{Z})$ конечна.

Задача. Докажите, что свободная группа резидуально конечна.

Решение. Очевидно, достаточно доказать резидуальную конечность свободных групп конечного ранга. По теореме Санова свободная группа конечного ранга вкладывается в $\mathrm{GL}(2, \mathbb{Z})$ и, значит, является резидуально конечной как подгруппа резидуально конечной группы.

§ 12. Двойные смежные классы

Сейчас мы рассмотрим важное обобщение понятие смежного класса введенное в 1894 году Фробениусом и Дедекиндом.

1. Двойные смежные классы. Пусть $F, H \leq G$. Произведение вида

$$FgH = \{fgh \mid f \in F, h \in H\}$$

называется **двойным смежным классом** (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. *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 $X = \{x_1, \dots, x_n\}$ – система представителей смежных классов, то

$$G = Fx_1H \sqcup \ldots \sqcup Fx_nH.$$

Задача. Убедитесь, что в качестве системы представителей двойных смежных классов по модулю (H, F) можно взять $X^{-1} = \{x_1^{-1}, \dots, x_n^{-1}\}$, иными словами,

$$G = Hx_1^{-1}F \sqcup \ldots \sqcup Hx_n^{-1}F.$$

Задача. Убедитесь, что

$$|G : H| = |F : F \cap x_1Hx_1^{-1}| + \ldots + |F : F \cap x_nHx_n^{-1}|.$$

Теорема Лагранжа является частным случаем этого утверждения, получающимся при $H = 1$.

2. Пересечения левых и правых смежных классов. 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 предыдущего пункта 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 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,

$$Fx \cap yH = Fu \cap uH = u(u^{-1}Fu \cap H), \quad Fx \cap zH = Fv \cap vH = v(v^{-1}Fv \cap H).$$

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.

Следствие. $|F| \cdot |H| = |FgH| \cdot |F \cap gHg^{-1}|$.

Тема 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.

Чтобы проиллюстрировать введенные понятия на примере, который нельзя назвать чисто учебным, мы обсуждаем первое реальное приложение теории групп, а именно, классификацию кристаллографических групп. Вначале как следствие доказанной в главе I теоремы Гесселя мы классифицируем 32 кристаллографических класса (классы конечных подгрупп в $\mathrm{GL}(n,\mathbb{Z})$ с точностью до сопряженности в $\mathrm{GL}(n,\mathbb{R})$), а потом формулируем описание одномерных, двумерных и трехмерных кристаллографических групп.

§ 1. Нормальные подгруппы

В этом пункте 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, это *в точности* такие подгруппы в G, отношение сравнимости по модулю которых является конгруэнцией на G.

Определение. *Подгруппа H группы G называется* **нормальной**, *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). 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.

2. Первые примеры нормальных подгрупп. Укажем несколько очевидных примеров нормальных делителей[115]. В дальнейшем, когда мы научимся строить нормальные делители из гомоморфизмов и сопряженных классов, возникнет много других, более интересных примеров.

• **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 $H = 1$ 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.

• **Подгруппы индекса 2.** 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 $x \neq H$, то $Hx \neq H$ и $xH \neq H$, и, значит, $Hx = G \setminus H = xH$. Важнейшим примером этой ситуации является **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 $g^2 \in H$.

Этот пример легко обобщить.

Задача. Пусть p – наименьшее простое, делящее порядок группы G. Тогда любая подгруппа $H \leq G$ индекса p нормальна в G.

Решение. 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 § 12 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 $xH = Hx$.

[115]Алексей Степанов отметил явное противоречие этой фразы с декларацией, что термин **нормальная подгруппа** превратился 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**.

• **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.** Группа G называется **гамильтоновой**, если все ее подгруппы нормальны (иногда при этом еще требуется, чтобы 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, тоже нормальны.

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 $C_G(X) \trianglelefteq N_G(X)$

В случае, когда $H \leq G$ есть подгруппа в G, фактор-группа $N_G(H)/C_G(H)$ называется **группой Вейля** группы H. 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 $N_G(D)/C_G(D) \cong S_n$.

§ 2. Не каждая подгруппа нормальна

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:

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Тогда, как легко видеть, $H \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} H$, 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 этой ситуации 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, за исключением случая $n = 2$, когда каждый элемент имеет период 2, и, поэтому, равенство $\pi(i) = 2$ равносильно равенству $\pi(2) = i$, это совсем не одно и то же.

3. Стабилизатор точки в $\mathrm{GL}(n, K)$**.** Рассмотрим 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

$$\{g \in \mathrm{GL}(n, K) \mid g_{*1} = v\}, \qquad v \in K^n \setminus \{0\}.$$

Ясно, что в общем случае это совсем не одно и то же, для этого 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.

§ 3. 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**[116] 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*[117]

$$g^G = \{xgx^{-1} \mid x \in G\}$$

и называется **классом сопряженных элементов** *группы G с представителем g.*

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**. 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. Главу 4).

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 своих 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.

---

[116]Роберт Шмидт заметил, что по-русски лучше говорить `сопряженный с`. С моей точки зрения возможны оба варианта, однако даже по-английски я предпочитаю говорить `conjugate to`, а не `conjugate with`. Обратите внимание, что в любом случае `conjugate`, а не `conjugated`, как *ошибочно* пишут почти все русские математики.

[117]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.

3. Очевидные примеры описания сопряженных классов. Описание классов сопряженных элементов является одним из основных вопросов, на которые мы должны ответить, чтобы понять строение группы G. Вот несколько очевидных примеров.

• Класс элемента $x \in G$ в том и только том случае одноэлементен, когда x централен. В частности, группа G тогда и только тогда абелева, когда все ее сопряженные классы одноэлементны.

• В группе кватернионов Q два центральных элемента ± 1, а три других сопряженных класса имеют вид $\{\pm i\}$, $\{\pm j\}$, $\{\pm k\}$.

• Пусть $G = D_n$ – диэдральная группа. В этом случае классы сопряженных элементов описываются по разному, в зависимости от четности n. Проще всего убедиться в этом представляя себе G как группу симметрий правильного n-угольника. Группа D_n содержит n вращений на углы $2\pi m/n$, $m = 0, \dots, n-1$, и n отражений. Если n нечетно, то все отражения сопряжены в G: 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 семестре III. 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 $O(n, \mathbb{R})$.

?. Классы сопряженности группы $\mathrm{Isom}(\mathbb{R}^3)$**.**

§ 4. 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. 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. [Sch], 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.

В действительности, на порядок $|C|$ класса сопряженных элементов конечной группы имеются и другие нетривиальные арифметические ограничения. Сформулируем один из наиболее известных классических результатов в этом направлении.

Теорема Бернсайда. *Порядок $|C|$ класса сопряженных элементов конечной группы не может быть примарным числом.*

Обычное доказательство этого результата использует теорию представлений. Из этого результата, в частности, сразу вытекает такое знаменитое следствие, утверждающее, что конечная группа, порядок которой делится лишь на два различных простых числа, разрешима.

***pq*-Теорема Бернсайда.** *Пусть $p, q \in \mathbb{P}$. Тогда группа порядка $p^m q^n$ разрешима.*

2. Классовое уравнение. Пусть теперь $Z = \{x_1, \ldots, x_m\}$ – 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** (class number) группы G, а равенство $n = n_1 + \ldots + n_m$ – **классовым уравнением** (class equation). Набор $(n_1, \ldots, n_m)$ 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 $G = \langle g_1, \ldots, g_m \rangle$.

3. Теорема Ландау. Сейчас мы с другой стороны взглянем на вопрос о количестве классов сопряженных элементов. Следующий результат доказанный Эдмундом Ландау[118] в 1903 году иллюстрирует использование классового уравнения.

[118]**Эдмунд Ландау** (1877–1938) — знаменитый немецкий математик. Подавляющее

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 $1 - \dfrac{1}{l_{m-k}} - \ldots - \dfrac{1}{l_m} > 0$ существует наименьшее, и, значит, найдется $q \in \mathbb{N}$ такое, что $\dfrac{1}{q} \leq \dfrac{m-k-1}{l_{m-k-1}}$ или, что то же самое, $l_{m-k-1} \leq q(m-k-1)$. Таким образом, доказательство теоремы завершается по индукции.

Сделаем для иллюстрации явно еще один шаг:

$$1 - \frac{1}{l_{m-1}} - \frac{1}{l_m} = \frac{1}{l_1} + \ldots + \frac{1}{l_{m-2}} \leq \frac{m-2}{l_{m-2}}.$$

Так как $m \geq 3$, то $l_{m-1} \geq 3$ (в самом деле, если $l_m = 2$, это так потому, что $1 - \dfrac{1}{l_m} - \dfrac{1}{l_{m-1}} > 0$, а если $l_m \geq 3$, то просто потому, что $l_{m-1} \geq l_m$). Это значит, что левая часть последнего равенства $\geq \dfrac{1}{6}$ 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?

большинство из его 254 статей относятся 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'. Ландау происходил из банкирской семьи и в математическом фольклоре известны десятки 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.

4. Сопряженность и коммутирование. Ясно, что два класса сопряженных элементов C и D, вообще говоря, не могут 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!

Задача. Доказать, что порядок коммутанта группы G не меньше порядка любого из ее сопряженных классов.

5. 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.

§ 5. Порождение нормальных подгрупп

> "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, часть III, IX.

Теперь у нас все готово для того, чтобы описать нормальные подгруппы в терминах сопряженных, а не смежных классов.

1. Сопряженные подгруппы. 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 $(xhx^{-1})^{-1} = xh^{-1}x^{-1} \in xHx^{-1}$.

Число подгрупп в G, сопряженных с H, равно $|G : N_G(H)|$.

Задача. Пусть $H \leq G$ — подгруппа *конечной* группы G. Докажите, что объединение всех подгрупп в G, сопряженных с H, не может равняться G.

Предостережение. Как уже упоминалось, можно построить бесконечную группу G, все неединичные элементы которой сопряжены. Такая группа G является объединением нетривиальных циклических подгрупп, которые все сопряжены.

2. Сопряженность и нормальные подгруппы. Таким образом, 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 $xHx^{-1} \leq H$, конечно, 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, $H = x(x^{-1}Hx)x^{-1} \leq xHx^{-1} \leq H$.

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.

• 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.

3. 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.

4. Лемма Дицмана. Доказательство следующей леммы[119] 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

$$g = x_1\dots x_l = xx_1^x\dots x_{i-1}^x x_{i+1}\dots x_l$$

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.*

5. Коммутаторы и коммутант. Сейчас мы построим *важнейший* пример нормальной подгруппы, к изучению которого мы вернемся во втором семестре.

[119] А.П.Дицман, О p-группах. – Докл. АН СССР, 1937, т.15, с.71–76.

Определение. Коммутатором *элементов* $x, y \in G$ *называется*

$$[x, y] = xyx^{-1}y^{-1}.$$

Подгруппа в G*, порожденная всеми коммутаторами, называется* **коммутантом** G *и обозначается* $[G, G]$*:*

$$[G, G] = \langle [x, y], x, y \in G \rangle.$$

В старых книгах 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.

§ 6. 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* $\equiv = \equiv_H$ *по нормальной подгруппе 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). А именно, 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 не имеет места, 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[120] и Гельдер[121].

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 (употребляется также термин Restklassengruppe и, иногда, Quotientengruppe). Обратите внимание, что в большин-

[120]**Камиль Жордан** (05.01.1838, Лион – 20.01.1922, 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.

[121]**Людвиг Отто Гельдер** (Hölder) (22.12.1859, Штуттгарт – 29.08.1937, 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. Защитил диссертацию в Тюбингене в 1882 году, под руководством дю Буа-Ремона. С 1899 года был профессором в Лейпциге. В нашем курсе встречается десяток теорем Гельдера (описание автоморфизмов S_n, классификация групп порядков pq и p^3 и т.д.), теорема Жордана-Гельдера, неравенство Гельдера и т.д. Крупные специалисты по истории математики часто путают Гельдера ст. с его сыном **Эрнстом Отто Гельдером** (02.04.1901, Лейпциг –), тоже достаточно замечательным 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 доказал в 1889 году Гельдер ст.

стве 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.*

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 $x^{-1}H$.

3. Первые примеры фактор-групп. Приведем несколько очевидных примеров фактор-групп.

• **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 $G/H = \{\{\pm\lambda\}, \lambda \in \mathbb{R}_+\} \cong \mathbb{R}_+$. В действительности 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 Co^*.** 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 $\mathrm{Co}^* = \mathbb{R}_{>0} \times \mathbb{T}$.

• **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 § ?.

• Группа $S_3 \cong S_4/V$ является фактор-группой S_4 по модулю четверной группы V.

4. 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^ma, для некоторых $m \in \mathbb{Z}$, $a \in C(G)$. Ясно, что два любых элемента такого вида коммутируют: $(x^ma)(x^nb) = x^{m+n}ab = (x^nb)(x^ma)$.

5. Теорема о соответствии. Пусть $H \trianglelefteq G$. Сейчас мы построим изоморфизм между решетками $L(G,H)$ и $L(G/H,1)$.

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 и нормальные подгруппы, иными словами, для любых $H \le F, K \le G$ имеем*

i) $F \le K \iff F/H \le K/H$;

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 $H \le F \le G$, $H \trianglelefteq G$, влечет $H \trianglelefteq F$, то F/H – подгруппа в G/H. Предположим, что $H \le F, K \le G$ – 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 $L \le G/H$ – подгруппа в G/H, то $F = \pi^{-1}(L) \ge H$ 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.

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.

§ 7. Примеры нормальных подгрупп и фактор-групп в линейных группах

1. Очевидные примеры. Следующие примеры проверяются 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 Главе ?.

• **Треугольные матрицы по модулю унитреугольных.** Группа $U = U(n, K)$ верхних унитреугольных матриц является нормальным делителем в группе $B = \mathrm{B}(n, K)$ 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 огромную 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 $G = \mathrm{GL}(n, R)$ – 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 $\mathrm{PGL}(2, \mathrm{Co})$. Еще один пример, который будут 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 и для коммутативного кольца R проективная линейная группа $\mathrm{PGL}(n, R)$ **ошибочно** определяется как $\mathrm{GL}(n, R)/R^*$. Это грубейшее заблуждение! В действительности, элементы $\mathrm{PGL}(n, R)$ тоже представляются как классы матриц, но не над самим кольцом R, а над некоторым его расширением. Причины, по которым $\mathrm{PGL}(n, K)$ совпадает с $\mathrm{GL}(n, K)/K^*$, слишком глубоки, чтобы обсуждать их здесь.

Аналогично, **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 $\mathrm{PSL}(2,3) \cong A_4$.

Задача. Докажите, что $\mathrm{PGL}(2,\mathrm{Co}) \cong \mathrm{PSL}(2,\mathrm{Co})$. Верно ли, что $\mathrm{PGL}(2,\mathbb{R}) \cong \mathrm{PSL}(2,\mathbb{R})$?

4. Клейновы и фуксовы группы. Дискретная подгруппа в $\mathrm{PSL}(2,\mathbb{R})$ называется **фуксовой группой**, а дискретная подгруппа в $\mathrm{PSL}(2,\mathrm{Co})$ называется **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 § ?.

§ 8. 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[122], которые вскользь упоминались в Главе I. 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**[123]

$$\mathrm{Lip} = \{a + bi + cj + dk \mid a,b,c,d \in \mathbb{Z}\}.$$

Однако в действительности интересующие нас группы будут группами единиц чуть больших колец[124], самым известным из которых является кольцо Hurw **целых гурвицевых кватернионов**[125]:

$$\mathrm{Hurw} = \mathrm{Lip} \coprod \tfrac{1}{2}(1+i+j+k) + \mathrm{Lip},$$

состоящее из кватернионов, все координаты которых либо одновременно целые, либо одновременно полуцелые.

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

$$T^\star = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}$$

---

[122] P.Du Val, Homographies, quaternions and rotations. – Oxford, 1964, p.1–116; § 20.

[123] R.Lipschitz, Untersuchungen über die Summen von Quadraten. – Bonn, 1886, S.1–147.

[124] M.-F.Vigneras, Arithmetique des algebres des quaternions. – Lect. Notes Math., 1980, vol.800.

[125] A.Hurwitz, Über die Zahlentheorie der Quaternionen. – Nachrichten Ges. Wiss. Göttingen., Math.–Phys. Kl., 1896, N.4, S.313–340; Math. Werke, Bd.2, Basel, 1933, S.303–330.

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 облегчить установление соответствия с другими работами, где рассматриваются бинарные группы многогранников, мы считаем, что перестановки умножаются **слева направо**. Обычно в настоящей книге — например, в Главе V — 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 ясно, 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:

$$\omega \mapsto (234), \quad \omega^i \mapsto (143), \quad \omega^j \mapsto (124), \quad \omega^k \mapsto (132),$$

$$\overline{\omega} \mapsto (243), \quad \overline{\omega}^i \mapsto (134), \quad \overline{\omega}^j \mapsto (142), \quad \overline{\omega}^k \mapsto (123).$$

§ 8. Бинарные группы многогранников, 2ND INSTALMENT: группа $O^\star$

Продолжим издеваться над кватернионами. Для этого введем элемент $\theta = (1 + i)/\sqrt{2}$. Этот элемент замечателен тем, что вместе с Hurw порождает еще одно эвклидово подкольцо[126] 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

$$O^\star = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k),$$
$$\frac{1}{\sqrt{2}}(\pm 1 \pm i), \frac{1}{\sqrt{2}}(\pm 1 \pm j), \frac{1}{\sqrt{2}}(\pm 1 \pm k), \frac{1}{\sqrt{2}}(\pm i \pm j), \frac{1}{\sqrt{2}}(\pm i \pm k), \frac{1}{\sqrt{2}}(\pm j \pm k)\}$$

[126] С.В.Стахов, Евклидовы подкольца в теле кватернионов, связанные с правильными многогранниками. – Канд. Дисс., Ленингр. Ун-т, 1985, с.1–141.

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.

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.

Ответ. 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

$$\frac{1}{\sqrt{2}}(1+i) \mapsto (1423), \quad \frac{1}{\sqrt{2}}(1+j) \mapsto (1234), \quad \frac{1}{\sqrt{2}}(1+k) \mapsto (1342),$$
$$\frac{1}{\sqrt{2}}(1-i) \mapsto (1324), \quad \frac{1}{\sqrt{2}}(1-j) \mapsto (1432), \quad \frac{1}{\sqrt{2}}(1-k) \mapsto (1243).$$

§ 8. 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 § ? Главы I. 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 $\pm1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm1 \pm i \pm j \pm k)$, образующие группу $T^\star$,

• 96 кватернионов, получающихся из $\dfrac{1}{2}(\pm i \pm \sigma j \pm \tau k)$ **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**. Громадную 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 $\zeta = \dfrac{1}{2}(\sigma + i + \tau j)$, 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 $\dfrac{1}{2}(\pm i \pm \sigma j \pm \tau k)$ **нечетными** перестановками $1, i, j, k$,

образуют группу.

Решение. Достаточно повторить то же рассуждение с заменой ζ на $\xi = \dfrac{1}{2}(\sigma + \tau i + j)$. 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.

Ответ. Сейчас мы явным образом построим изоморфизм, продолжающий построенный в § ? изоморфизм $T^\star/\{\pm1\} \cong A_4$. Единственное отличие приводимых нами формул от формул из статьи Роберта Уилсона[127] 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, $\dfrac{1}{2}$ $\dfrac{\sigma}{2}$ и $\dfrac{\tau}{2}$. 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:

$$\begin{array}{lll}
\frac{1}{2}(i + \sigma j + \tau k) \mapsto (14)(35), & \frac{1}{2}(\tau i + j + \sigma k) \mapsto (13)(45), & \frac{1}{2}(\sigma i + \tau j + k) \mapsto (15)(34),\\
\frac{1}{2}(i - \sigma j - \tau k) \mapsto (14)(25), & \frac{1}{2}(-\tau i + j + \sigma k) \mapsto (15)(24), & \frac{1}{2}(-\sigma i + \tau j + k) \mapsto (12)(45),\\
\frac{1}{2}(i - \sigma j + \tau k) \mapsto (15)(23), & \frac{1}{2}(-\tau i + j - \sigma k) \mapsto (13)(25), & \frac{1}{2}(\sigma i - \tau j + k) \mapsto (12)(45),\\
\frac{1}{2}(i + \sigma j - \tau k) \mapsto (23)(45), & \frac{1}{2}(\tau i + j - \sigma k) \mapsto (24)(35), & \frac{1}{2}(-\sigma i - \tau j + k) \mapsto (25)(34).
\end{array}$$

Общее количество 3-циклов в группе A_5 равно $2C_5^3 = 20$. Из них восемь 3-циклов, не затрагивающих 5, уже задействованы, так что у нас снова остается ровно 12 штук 3-циклов,

[127] R.A.Wilson, The geometry of Hall–Janko group as a quaternionic reflection group. – Geom. Dedic., 1986, vol.20, p.157–173.

которые и будут образами тех 12 элементов $I^\star \setminus T^\star$, у которых коэффициент при 1 равен $\frac{1}{2}$, 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 $\frac{\sigma}{2}$ и 12 икосианов, у которых этот коэффициент равен $\frac{\tau}{2}$. 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:

$$\frac{1}{2}(-\sigma+j+\tau k)\mapsto(13524),\quad \frac{1}{2}(-\sigma+\tau i+k)\mapsto(13452),\quad \frac{1}{2}(-\sigma+i+\tau j)\mapsto(15234),$$
$$\frac{1}{2}(-\sigma-j-\tau k)\mapsto(14253),\quad \frac{1}{2}(-\sigma-\tau i-k)\mapsto(12543),\quad \frac{1}{2}(-\sigma-i-\tau j)\mapsto(14325),$$
$$\frac{1}{2}(-\sigma+j-\tau k)\mapsto(15423),\quad \frac{1}{2}(-\sigma-\tau i+k)\mapsto(12435),\quad \frac{1}{2}(-\sigma+i-\tau j)\mapsto(14532),$$
$$\frac{1}{2}(-\sigma-j+\tau k)\mapsto(13245),\quad \frac{1}{2}(-\sigma+\tau i-k)\mapsto(15342),\quad \frac{1}{2}(-\sigma-i+\tau j)\mapsto(12354).$$

А вот и последняя буква имени:

$$\frac{1}{2}(-\tau+\sigma j+k)\mapsto(12534),\quad \frac{1}{2}(-\tau+i+\sigma k)\mapsto(13254),\quad \frac{1}{2}(-\tau+\sigma i+j)\mapsto(13425),$$
$$\frac{1}{2}(-\tau-\sigma j-k)\mapsto(14352),\quad \frac{1}{2}(-\tau-i-\sigma k)\mapsto(14523),\quad \frac{1}{2}(-\tau-\sigma i-j)\mapsto(15243),$$
$$\frac{1}{2}(-\tau+\sigma j-k)\mapsto(12345),\quad \frac{1}{2}(-\tau-i+\sigma k)\mapsto(15324),\quad \frac{1}{2}(-\tau+\sigma i-j)\mapsto(13542),$$
$$\frac{1}{2}(-\tau-\sigma j+k)\mapsto(15432),\quad \frac{1}{2}(-\tau+i-\sigma k)\mapsto(14235),\quad \frac{1}{2}(-\tau-\sigma i+j)\mapsto(12453).$$

§ 8. Решетка Лича и группа Холла–Янко

Рассмотрим кватернион $h=\omega+\sigma=\frac{1}{2}(-\sqrt{5}+i+j+k)$. Ясно, что $h\overline{h}=1$.

$$L=\{(x,y,z)\mid x,y,z\in \mathrm{Icos}, x\equiv y\equiv z \mod h, x+y+z\equiv 0 \mod \overline{h}\}$$

Рассмотрим следующую диагональную подгруппу G_0 в $\mathrm{GL}(3,\mathbb{H})$:

$$G_0=\{\mathrm{diag}(f,g,h)\mid f,g,h\in Q, fgh=\pm 1\}$$

после чего породим подгруппу $G=\langle G_0,\omega e\rangle$, группой G_0 и матрицей $\omega e=\mathrm{diag}(\omega,\omega,\omega)$, Ясно, что $|G_0|=2^7=128$, а $|G|=2^7.3=384$.

§ 8. 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:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}$$

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 берется 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 $x_i y_j$, без которых `Mathematica` может ненароком не обратить внимания на равенство двух матриц и принять их за различные[128]; `Flatten[blabla,1]` делает из получающегося двумерного списка матриц $x_i y_j$ 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:

[128]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.

```
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[129]:

```
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}
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.

§ 8. Классификация конечных простых групп

Одно из самых замечательных достижений математики за всю ее историю — Классификация конечных простых групп.

- Циклические группы простого порядка;
- Знакопеременные группы A_n, $n \geq 5$;
- Конечные простые группы типа Ли;
- 26 спорадических групп.

Вычисления в этих группах легко осуществляются в Mathematica. Так как

§ 8. Порядки простых групп, меньших 1 000 000

Имеется ровно 56 (неабелевых) простых групп, порядки которых меньше 1 000 000. Это сразу вытекает из теоремы классификации, но может быть установлено и элементарными методами[130,131], использующими лишь ранние классификационные результаты. Большая часть этих групп являются проективными специальными группами $\mathrm{PSL}(2, q)$ степени 2. Пять из них — знакопеременные группы A_5, A_6, A_7, A_8, A_9, три из которых изоморфны группам $\mathrm{PSL}(n, q)$. Пять групп — спорадические:

• Три маленькие **группы Матье** M_{11}, M_{12}, M_{22}. Группа $M_{21} \cong \mathrm{PSL}(3, 4)$ не является спорадической, а группа M_{10} не является простой, она содержит $\mathrm{PSL}(2, 9)$ в качестве подгруппы индекса 2. Порядки двух старших групп Матье M_{23} и M_{24} несколько больше одного миллиона, они равны 10 200 960 и 244 823 040, соответственно.

• Две младшие **группы Янко** J_1 и J_2. **Вторая группа Янко** часто называется также **группой Холла–Янко** и обозначается HJ. Что касается первой группы Янко J_1, то она близко дружит с $G_2(11)$ а ее порядок равен

$$175\,560 = 11(11+1)(11^3-1) = 19 \cdot 20 \cdot 21 \cdot 22 = 55 \cdot 56 \cdot 57.$$

[129]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".`

[130]M.Hall, A search for simple groups of order less than one million. – In: Computational Problems in Abstract Algebra, Pergamon Press, Oxford et al., 1970, p.137–168.

[131]М.Холл, Построение конечных простых групп. – В кн.: Вычисления в Алгебре и Теории Чисел, М., Мир, 1976, с.95–128.

Порядки всех остальных спорадических групп гораздо больше, единственными спорадическими группами, кроме перечисленных, порядок которых меньше одного *миллиарда*, являются **группа Хигмена–Симса**, порядка 44 352 000, **третья группа Янко** J_3, порядка 50 232 960, и **группа Маклафлина** Mc, порядка 898 128 000.

Все остальные группы, с *единственным* исключением, являются группами типа Ли, классических серий PSL_2, PSL_3, PSL_4, PSp_4, PSU_3 и PSU_4. Единственным исключением является группа Судзуки $\mathrm{Sz}(2^3)$.

Таблица ?. Конечные простые группы порядка $< 1\,000\,000$

$60 = 2^2 \cdot 3 \cdot 5$,	$A_5 \cong \mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5)$,
$168 = 2^3 \cdot 3 \cdot 7$,	$\mathrm{PSL}(2,7)$,
$360 = 2^3 \cdot 3^2 \cdot 5$,	$A_6 \cong \mathrm{PSL}(2,9)$,
$504 = 2^3 \cdot 3^2 \cdot 7$,	$\mathrm{PSL}(2,8)$,
$660 = 2^2 \cdot 3 \cdot 5 \cdot 11$,	$\mathrm{PSL}(2,11)$,
$1092 = 2^2 \cdot 3 \cdot 7 \cdot 13$,	$\mathrm{PSL}(2,13)$,
$2448 = 2^4 \cdot 3^2 \cdot 17$,	$\mathrm{PSL}(2,17)$,
$2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$,	A_7,
$3420 = 2^2 \cdot 3^2 \cdot 5 \cdot 19$,	$\mathrm{PSL}(2,19)$,
$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$,	$\mathrm{PSL}(2,16)$,
$5616 = 2^4 \cdot 3^3 \cdot 13$,	$\mathrm{PSL}(3,3)$,
$6048 = 2^5 \cdot 3^3 \cdot 7$,	$\mathrm{PSU}(3,3^2)$,
$6072 = 2^3 \cdot 3 \cdot 11 \cdot 23$,	$\mathrm{PSL}(2,23)$,
$7800 = 2^3 \cdot 3 \cdot 5^2 \cdot 13$,	$\mathrm{PSL}(2,25)$,
$7920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$,	группа Матье M_{11},
$9828 = 2^2 \cdot 3^3 \cdot 7 \cdot 13$,	$\mathrm{PSL}(2,27)$,
$12180 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 29$,	$\mathrm{PSL}(2,29)$,
$14880 = 2^5 \cdot 3 \cdot 5 \cdot 31$,	$\mathrm{PSL}(2,31)$,
$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$,	$A_8 \cong \mathrm{PSL}(4,2)$,
$20160 = 2^6 \cdot 3^2 \cdot 5 \cdot 7$,	$M_{21} \cong \mathrm{PSL}(3,4)$,
$25308 = 2^2 \cdot 3^2 \cdot 19 \cdot 37$,	$\mathrm{PSL}(2,37)$,
$25920 = 2^6 \cdot 3^4 \cdot 5$,	$\mathrm{PSp}(4,3) \cong \mathrm{PSU}(4,2^2)$,
$29120 = 2^6 \cdot 5 \cdot 7 \cdot 13$,	группа Судзуки $\mathrm{Sz}(2^3)$,
$32736 = 2^5 \cdot 3 \cdot 11 \cdot 31$,	$\mathrm{PSL}(2,32)$,
$34440 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 41$,	$\mathrm{PSL}(2,41)$,
$39732 = 2^2 \cdot 3 \cdot 7 \cdot 11 \cdot 43$,	$\mathrm{PSL}(2,43)$,
$51888 = 2^4 \cdot 3 \cdot 23 \cdot 47$,	$\mathrm{PSL}(2,47)$,
$58800 = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2$,	$\mathrm{PSL}(2,49)$,
$62400 = 2^6 \cdot 3 \cdot 5^2 \cdot 13$,	$\mathrm{PSU}(3,4^2)$,
$74412 = 2^2 \cdot 3^3 \cdot 13 \cdot 53$,	$\mathrm{PSL}(2,53)$,
$95040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$,	группа Матье M_{12},
$102660 = 2^2 \cdot 3 \cdot 5 \cdot 29 \cdot 59$,	$\mathrm{PSL}(2,59)$,
$113460 = 2^2 \cdot 3 \cdot 5 \cdot 31 \cdot 61$,	$\mathrm{PSL}(2,61)$,
$126000 = 2^4 \cdot 3^2 \cdot 5^3 \cdot 7$,	$\mathrm{PSU}(3,5^2)$,
$150348 = 2^2 \cdot 3 \cdot 11 \cdot 17 \cdot 67$,	$\mathrm{PSL}(2,67)$,
$175560 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$,	группа Янко J_1,
$178920 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 71$,	$\mathrm{PSL}(2,71)$,

$181440 = 2^6 \cdot 3^4 \cdot 5 \cdot 7,$	$A_9,$
$194472 = 2^3 \cdot 3^2 \cdot 37 \cdot 73,$	$\mathrm{PSL}(2, 73),$
$246480 = 2^4 \cdot 3 \cdot 5 \cdot 13 \cdot 79,$	$\mathrm{PSL}(2, 79),$
$262080 = 2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13,$	$\mathrm{PSL}(2, 64),$
$265680 = 2^4 \cdot 3^4 \cdot 5 \cdot 41,$	$\mathrm{PSL}(2, 81),$
$285852 = 2^2 \cdot 3 \cdot 7 \cdot 41 \cdot 83,$	$\mathrm{PSL}(2, 83),$
$352440 = 2^3 \cdot 3^2 \cdot 5 \cdot 11 \cdot 89,$	$\mathrm{PSL}(2, 89),$
$372000 = 2^5 \cdot 3 \cdot 5^3 \cdot 31,$	$\mathrm{PSL}(3, 5),$
$443520 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11,$	группа Матье $M_{22},$
$456288 = 2^5 \cdot 3 \cdot 7^2 \cdot 97,$	$\mathrm{PSL}(2, 97),$
$515100 = 2^2 \cdot 3 \cdot 5^2 \cdot 17 \cdot 101,$	$\mathrm{PSL}(2, 101),$
$546312 = 2^3 \cdot 3 \cdot 13 \cdot 17 \cdot 103,$	$\mathrm{PSL}(2, 103),$
$604800 = 2^7 \cdot 3^3 \cdot 5^2 \cdot 7,$	группа Холла–Янко $J_2 = \mathrm{HJ},$
$612468 = 2^2 \cdot 3^3 \cdot 53 \cdot 107,$	$\mathrm{PSL}(2, 107),$
$647460 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 109,$	$\mathrm{PSL}(2, 109),$
$721392 = 2^4 \cdot 3 \cdot 7 \cdot 19 \cdot 113,$	$\mathrm{PSL}(2, 113),$
$885720 = 2^3 \cdot 3 \cdot 5 \cdot 11^2 \cdot 61,$	$\mathrm{PSL}(2, 121),$
$976500 = 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 31,$	$\mathrm{PSL}(2, 125),$
$979200 = 2^8 \cdot 3^2 \cdot 5^2 \cdot 17,$	$\mathrm{PSp}(4, 4),$

Порядок следующей группы $\mathrm{PSL}(2, 127)$ чуть больше миллиона, он равен $1024128 = 2^7 \cdot 3^2 \cdot 7 \cdot 127$. Легко сделать несколько численных наблюдений. Во-первых, порядки всех групп делятся на 4. Группа Судзуки является *единственной* группой в этом списке, порядок которой не делится на 3. Обе эти закономерности носят общий характер, в частности, порядок всех простых групп, кроме групп Судзуки, делится на 12. В этом списке порядок 20160 фигурирует *дважды*, в самом деле, легко проверить, что группы $\mathrm{PSL}(4, 2)$ и $\mathrm{PSL}(3, 4)$ не изоморфны. Все остальные группы однозначно определяются своим порядком.

§ 8. Группы типа Ли

Основную массу конечных простых групп слставляют группы типа Ли. Группы типа Ли делятся на классические группы, которые были известны в XIX веке, и исключительные группы, которые были открыты только в XX веке.

Таблица ?. Конечные классические группы

группа типа Ли	**классическое обозначение**	**порядок**
$A_l(q)$	$\mathrm{PSL}(l+1, q)$	$\dfrac{1}{\gcd(l+1, q-1)} q^{l(l+1)/2} \prod_{i=1}^{l} (q^{i+1} - 1),$
$B_l(q)$	$\mathrm{P\Omega}(2l+1, q)$	$\dfrac{1}{\gcd(2, q-1)} q^{l^2} \prod_{i=1}^{l} (q^{2i} - 1),$
$C_l(q)$	$\mathrm{PSp}(2l, q)$	$\dfrac{1}{\gcd(2, q-1)} q^{l^2} \prod_{i=1}^{l} (q^{2i} - 1),$
$D_l(q)$	$\mathrm{P\Omega}^+(2l, q)$	$\dfrac{1}{\gcd(4, q^l-1)} q^{l(l-1)} (q^l - 1) \prod_{i=1}^{l-1} (q^{2i} - 1),$
${}^2A_l(q^2)$	$\mathrm{PSU}(l+1, q)$	$\dfrac{1}{\gcd(l+1, q+1)} q^{l(l+1)/2} \prod_{i=1}^{l} (q^{i+1} - (-1)^{i+1}),$

${}^2D_l(q^2)$	$\mathrm{P}\Omega^-(2l,q)$	$\dfrac{1}{\gcd(4,q^l+1)}q^{l(l-1)}(q^l+1)\prod_{i=1}^{l-1}(q^{2i}-1),$

Таблица ?. Конечные исключительные группы типа Ли

группа типа Ли	**порядок**
$E_6(q)$	$\dfrac{1}{\gcd(3,q-1)}q^{36}(q^{12}-1)(q^9-1)(q^8-1)(q^6-1)(q^5-1)(q^2-1),$
$E_7(q)$	$\dfrac{1}{\gcd(2,q-1)}q^{63}(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^{10}-1)(q^8-1)(q^6-1)(q^2-1),$
$E_8(q)$	$q^{120}(q^{30}-1)(q^{24}-1)(q^{20}-1)(q^{18}-1)(q^{14}-1)(q^{12}-1)(q^8-1)(q^2-1),$
$F_4(q)$	$q^{24}(q^{12}-1)(q^8-1)(q^6-1)(q^2-1),$
$G_2(q)$	$q^6(q^6-1)(q^2-1),$
${}^2E_6(q^2)$	$\dfrac{1}{\gcd(3,q+1)}q^{36}(q^{12}-1)(q^9+1)(q^8-1)(q^6-1)(q^5+1)(q^2-1),$
${}^3D_4(q^3)$	$q^{12}(q^8+q^4+1)(q^6-1)(q^2-1),$
${}^2B_2(q)$, $q=2^{2m+1}$,	$q^2(q^2+1)(q-1),$
${}^2G_2(q)$, $q=3^{2m+1}$,	$q^3(q^3+1)(q-1),$
${}^2F_4(q)$, $q=2^{2m+1}$,	$q^{12}(q^6+1)(q^4-1)(q^3+1)(q-1),$

§ 8. Спорадические группы

В настоящем параграфе мы перечислим 26 спорадических групп, которые не входят ни в одну из бесконечных серий.

Таблица ?. Спорадические группы

группа	**обозначение**	**порядок**
Матье	M_{11}	$2^4\cdot 3^2\cdot 5\cdot 11,$
Матье	M_{12}	$2^6\cdot 3^3\cdot 5\cdot 11,$
Матье	M_{22}	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 11,$
Матье	M_{23}	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 11\cdot 23,$
Матье	M_{24}	$2^{10}\cdot 3^3\cdot 5\cdot 7\cdot 11\cdot 23,$
Янко	J_1	$2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 19,$
Холла–Янко	$J_2=\mathrm{HJ}$	$2^7\cdot 3^3\cdot 5\cdot 7,$
Янко	J_3	$2^4\cdot 3^5\cdot 5\cdot 17\cdot 19,$
Янко	J_4	$2^{21}\cdot 3^3\cdot 5\cdot 7\cdot 11^3\cdot 23\cdot 29\cdot 31\cdot 37\cdot 43,$
Хигмана–Симса	HS	$2^9\cdot 3^2\cdot 5^3\cdot 7\cdot 11,$
Маклафлина	Mc	$2^7\cdot 3^6\cdot 5^3\cdot 7\cdot 11,$
Судзуки	Suz	$2^{13}\cdot 3^7\cdot 5^2\cdot 7\cdot 11\cdot 13,$
Рудвалиса	Ru	$2^{14}\cdot 3^3\cdot 5^3\cdot 7\cdot 13\cdot 29,$
Хельда	He	$2^{10}\cdot 3^3\cdot 5^2\cdot 7^3\cdot 17,$
Лайонса	Ly	$2^8\cdot 3^7\cdot 5^6\cdot 7\cdot 11\cdot 31\cdot 37\cdot 67,$

О'Нана–Симса	ON	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$,
Конвея	Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$,
Конвея	Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$,
Конвея	Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$,
Фишера	Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$,
Фишера	Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$,
Фишера	Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$,
Харада–Нортона	$F_5 = \mathrm{HN}$	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$,
Томпсона	$F_3 = \mathrm{Th}$	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$,
Baby Monster	$F_2 = \mathrm{BM}$	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$,
Big Monster = Friendly Giant = Фишер–Грайсс	$F_1 = \mathrm{FG}$	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$

§ 8. Так ли велик Большой Монстр?

С точки зрения обывателя Большой Монстр является чудовищно большой группой. В самом деле, его порядок имеет 54 цифры и равен

$$|\,\mathrm{FG}\,| = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000$$

Наименьшее линейное представление FG над полем комплексных чисел имеет степень 196 883. Для умножения двух матриц такого порядка совсем недавно нужно было около года.

Однако по стандартам теории групп типа Ли Большой Монстр более, чем скромная группа. Вот, для сравнения, порядки первых пяти групп самой маленькой из старших исключительных групп — группы Шевалле типа E_6:

$$|E_6(2)| = 214\,841\,575\,522\,005\,575\,270\,400$$

$$|E_6(3)| = 14\,515\,406\,695\,082\,926\,420\,056\,516\,790\,429\,286\,400$$

$$|E_6(4)| = 85\,528\,710\,781\,342\,640\,103\,833\,619\,055\,142\,765\,466\,746\,880\,000$$

$$|E_6(5)| = 3\,175\,144\,122\,737\,732\,284\,276\,405\,334\,472\,656\,250\,000\,000\,000\,000\,000\,000$$

$$|E_6(7)| = 810\,331\,385\,160\,483\,128\,876\,506\,215\,285\,626\,370\,257\,098\,745\,230\,053\,452\,725\,616\,640\,000$$

Видно, что уже $E_6(5)$ почти в 4 раза больше, чем FG, а $E_6(7)$ больше, чем FG уже на 12 порядков. Еще быстрее FG проигрывает соревнование с группами Шевалле типа E_7:

$$|E_7(2)| = 7\,997\,476\,042\,075\,799\,759\,100\,487\,262\,680\,802\,918\,400$$

$$|E_7(3)| = 2\,542\,750\,473\,636\,273\,484\,480\,959\,502\,278\,043\,289\,108\,758\,407\,541\,532\,509\,234\,790\,400$$

Таким образом, уже вторая группа $E_7(3)$ больше FG на 10 порядков. Порядок самой маленькой группы Шевалле типа E_8 имеет уже 75 цифр:

$$|E_8(2)| = 337\,804\,753\,143\,634\,806\,261\,388\,190\,614\,085\,595\,079\,991\,692\,242\,467\,651\,576\,160\,959\,909\,068\,800\,000$$

Тем самым, уже самая маленькая из групп этого типа, $E_8(2)$, больше FG на 21 порядок! Тем не менее, с точки зрения профессионала, $E_8(2)$ не очень большая группа. Нет ни одного *естественного* вопроса про эту группу, на который мы не знали бы ответа. Мы знаем ее классы сопряженных элементов, автоморфизмы, максимальные подгруппы, комплексные представления, и многое другое.

Но в действительности $E_8(2)$ просто крохотная группа, по сравнению с $\mathrm{GL}(248, 2)$, порядок которой содержит 18515 цифр. А ведь никому не придет в голову называть $\mathrm{GL}(248, 2)$ большой группой!

§ 8. 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 $B(A) \leq Z(A)$.

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 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: $\varphi(Z(A)) \leq Z(B)$, $\varphi(B(A)) \leq B(B)$ (проверьте!). Тем самым φ индукцирует гомоморфизм групп гомологий

$$\varphi_* : H(A) \longrightarrow H(B), \quad x + B(A) \mapsto \varphi(x) + B(B).$$

§ 9. Расширения групп

В этом параграфе мы обсудим, в какой степени группа G определяется своей нормальной подгруппой и фактор-группой по этой нормальной подгруппе и введем одну из ключевых конструкций всей теории групп. Мы вернемся к детальному изучению этой конструкции в Гл. X, в связи с произведениями, но понятие расширения настолько важно, что нам удобно начать пользоваться им уже сейчас.

Определение. *Группа G называется* **расширением** *F при помощи H, если в G есть изоморфная H нормальная подгруппа, фактор-группа по которой изоморфна F.*

Произвольное расширение F при помощи H обозначается $G = H.F$, обратите внимание, что группа H обязана стоять здесь на первом месте! Понятие расширения было введено Отто Шрайером в 1926 году[132]. В этих работах Шрайер впервые поставил задачу классификации **всех** групп G, у которых есть изоморфная H нормальная подгруппа, фактор-группа по которой изоморфна F. По

[132] O.Schreier, Über die Erweiterungen von Gruppen. I. – Monatschrift f. Math. u. Phys., 1926, Bd.34, S.165–180; II. – Abh. Math. Sem. Hamburg, 1926, Bd.4, S.321–346.

крайней мере одна такая группа **всегда** существует, это прямое произведение $H \times F$. Однако, как мы сейчас убедимся, в общем случае может существовать **много** неизоморфных расширений F при помощи H. Каждый пример, когда мы могли вычислить фактор-группу, является примером расширения:

• Как четверная группа V, так и циклическая группа C_4 имеют вид $C_2.C_2$;

• Как группа треугольника S_3, так и циклическая группа C_6 имеют вид $C_3.C_2$

В действительности специалисты по теории групп пишут просто n вместо C_n, так что здесь можно было бы написать 2.2 или 3.2, соответственно. Последний пример допускает широкие обобщения.

• Для любого n имеем $D_n = n.2$.

• Для любого $n \geq 2$ имеем $S_n = A_n.2$.

• Для любого поля K характеристики $\neq 2$ имеем $\mathrm{SL}(2,K) = 2.\,\mathrm{PSL}(2,K)$

С учетом изоморфизма $A_5 \cong \mathrm{PSL}(2,5)$ весьма поучительно сравнить эти два примера в случае $n = 5$, $K = \mathbb{F}_5$. Первый из них превращается в $S_5 = A_5.2$, а второй – в $\mathrm{SL}(2,5) = 2.A_5$. Иными словами, в группе S_5 есть подгруппа A_5 фактор-группа по которой изоморфна C_2, а в $\mathrm{SL}(2,5)$ есть подгруппа C_2, фактор-группа по которой изоморфна A_5. Невооруженным глазом видно, что строение S_5 и $\mathrm{SL}(2,5)$ совершенно различно. Например, S_5 – группа без центра, в то время как $\mathrm{SL}(2,5)$ имеет центр порядка 2. В то же время, группа $\mathrm{SL}(2,5)$ совершенна, в то время как коммутант S_5 равен A_5 и имеет там индекс 2. А вот пример, который мы видели в § ?.

• $S_4 = V.S_3$, специалисты по теории конечных групп обычно пишут $S_4 = 2^2.S_3$. Кстати, почему не $4.S_3$?

• Каждая подгруппа группы кватернионов Q нормальна. Поэтому Q представляется в виде $Q = 4.2$ или $Q = 2.2^2$.

• Для конечного поля $K = \mathbb{F}_p$ имеем $\mathrm{Aff}(n,p) = p^n.\,\mathrm{GL}(n,p)$.

Пусть $i : H \longrightarrow G$ – изоморфизм H в G, а $\pi : G/i(H) \longrightarrow F$ – изоморфизм $G/i(H)$ на F. Профессионалы обычно объединяют изоморфизмы i и π в одну картинку и изображают расширения посредством **короткой точной последовательности**:

$$1 \longrightarrow H \xrightarrow{\ i\ } G \xrightarrow{\ \pi\ } F \longrightarrow 1$$

Точность этой диаграммы означает, что ядро каждого следующего гомоморфизма совпадает с образом предыдущего. Тем самым, точность в члене H означает, что $\mathrm{Ker}(i) = 1$, точность в члене G – что $\mathrm{Ker}(\pi) = \mathrm{Im}(i)$ и, наконец, точность в члене F – что $\mathrm{Im}(\pi) = F$. Группа H называется **ядром** расширения.

Предостережение. В некоторых книгах, в том числе [Kur], [KM] то, что мы называем расширением F при помощи H, **ошибочно** называется расширением H при помощи F. Расширение группы F это не такая надгруппа F, в которой F нормальна, а ее **накрывающая группа**, т.е. такая группа G, у которой есть фактор-группа, изоморфная F.

С принципиальной точки зрения полностью изучен случай расширений, в которых группа H абелева, такие расширения называются **расширениями с**

абелевым ядром. В этом случае ответ дается классической (абелевой) гомологической алгеброй. Еще проще устроены **центральные расширения**, ядро которых содержится в центре $H \leq C(G)$. В приложениях теории расширений в кристаллографии и теории конечных группа особенно часто возникает случай **расширений с циклическим ядром**, для которых H циклическая.

Обратите внимание, что группы H и F входят в $G = H.F$ абсолютно неравноправно. В группе G есть подгруппа, изоморфная H, но, вообще говоря, **нет** подгруппы, изоморфно проецирующейся на F. Это мотивирует введение следующего ключевого определения.

Определение. *Расширение $G = H.F$ называется* **расщепляющимся**, *если оно допускает* **расщепляющий гомоморфизм** (*splitting homomorphism, известный также как* **сечение**), *т.е. если существует такой гомоморфизм $\sigma : F \longrightarrow G$, что $\pi\sigma = \mathrm{id}_F$.*

Таким образом, *расщепляющееся* расширение группы F содержит подгруппу, изоморфную F. В случае расщепляющихся расширений F отождествляется с $\sigma(F)$ и рассматривается как подгруппа в G. Однако, как правило, эта подгруппа не является нормальной! Расщепляющееся расширение F при помощи H называется **полупрямым произведением** нормального делителя (ядра, kernel) H и **дополнительной подгруппы** (alias, **дополнения**, complement) F и обозначается $H \leftthreetimes F$ или $F \rightthreetimes H$. Обратите внимание, что здесь ядро может стоять как на первом, так и на втором месте, так как на него указывает хвостик значка $\leftthreetimes$ (`leftthreetimes`) или $\rightthreetimes$ (`rightthreetimes`). Конструкция полупрямых произведений детально изучается в Главе X, где приведено и много примеров.

В полупрямое произведение $H \leftthreetimes F$ группы H и F все еще входят неравноправно, так как H является там нормальной подгруппой, а F – нет. Если же мы потребуем, чтобы F тоже было нормальной подгруппой, то $G = H \times F$ есть прямое произведение H и F.

§ 10. Точечные группы, 1st instalment: сингонии и кристаллографические классы

В § ? мы классифицировали все **точечные группы**, т.е. все конечные подгруппы $O(3,\mathbb{R})$ или, что то же самое, все конечные подгруппы в $\mathrm{GL}(3,\mathbb{R})$, *с точностью до сопряженности в* $\mathrm{GL}(3,\mathbb{R})$. Как мы убедились, конечные подгруппы в $O(3,\mathbb{R})$, устроены чрезвычайно просто. *Единственная* реальная сложность при использовании этих групп состоит в несогласованности обозначений между различными книгами. Двумя наиболее часто используемыми системами обозначений точечных групп, являются **система Шенфлиса** и так называемая **международная система** (IUCr, система Германа–Могена). При этом геометры, химики и большинство физиков отдают предпочтение системе Шенфлиса, но кристаллографы и специалисты по физике твердого тела пользуются международной системой. Перечислим

элемент симметрии:	Система Шенфлиса:	IUCr:
поворотная ось порядка n	C_n	n
зеркальная ось порядка $n = 2l$	S_n	$\overline{n}$ или $\overline{l}$
вертикальное зеркало	σ_v или σ_d	m
горизонтальное зеркало	σ_h	$1/m$
точка инверсии	i	$\overline{1}$

Для того, чтобы облегчить задачу начинающему, во многих старых работах по геометрии и комбинаторной теории групп используется система, которую мы называем C & M (потому

что наиболее известная книга, где она встречается, это [CM]).

точечная группа:	Система Шенфлиса:	IUCr:	система C & M
C_n	C_n	n	$[n]^+$
D_n	D_n	$n22$	$[2,n]^+$
T^+	T	23	$[3,3]^+$
O^+	O или W	432	$[3,4]^+$
I^+	Y	$-$	$[3,5]^+$
$C_n \times C_2$	C_{nh}	n/m	$[2,n^+]$
$D_n \times C_2$	D_{nh}	n/mmm	$[2,n]$
$T^+ \times C_2$	T_h	n	$[3^+,4]$
O	O_h или W_h	$m3m2/m$	$[3,4]$
I	Y_h	$-$	$[3,5]$
$C_{2n}C_n$	S_{2n}	$\overline{2n}$	$-$
D_nC_n	C_{nv}	nmm	$[n]$
$D_{2n}D_n$	D_{nd}	$\overline{2n}m2$	$[2^+,2n]$
T	T_d	$\overline{4}3m$	$[3,3]$

Теперь мы будем интересоваться не всеми конечными подгруппами в $\mathrm{GL}(3,\mathbb{R})$, а только теми из них, которые оставляют на месте некоторую решетку $L = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_n$ в V. Иными словами, это значит, что нас интересуют конечные подгруппы, сопряженные с некоторой подгруппой в $\mathrm{GL}(3,\mathbb{Z})$. Легко доказывается следующий результат:

Лемма. *Группа, стабилизирующая некоторую решетку, может содержать только повороты порядков 1,2,3,4 и 6.*

Назовем конечную подгруппу в $\mathrm{GL}(n,\mathbb{R})$ **кристаллографической точечной группой**, если она сопряжена с некоторой подгруппой в $\mathrm{GL}(n,\mathbb{Z})$, или, что то же самое, если она содержит только поворотные оси порядков 1,2,3,4 и 6. Классы сопряженности кристаллографических точечных групп в $\mathrm{GL}(n,\mathbb{R})$ называются **кристаллографическими классами** (Kristallklasse). Ясно, что для $n = 2$ имеется ровно 10 кристаллографических классов[133], а именно, $C_1, C_2, C_3, C_4, C_6, D_1, D_2, D_3, D_4, D_6$. Сейчас мы перечислим все 32 кристаллографических класса для $n = 3$. Как мы уже упоминали, впервые это было сделано Гесселем в 1830 году, но его работа в то время осталась незамеченной, так что этот результат передоказывали Аксель Вильгельмович Гадолин[134] (в 1869 году) и Леонард Зонке[135] (в 1879 году), а потом Федоров, Пьер Кюри, Миннигероде, Шенфлис, Вульф, ...

Группа $G \leq \mathrm{GL}(n,\mathbb{R})$, являющаяся полной группой симметрии некоторой решетки, называется **подгруппой Браве**. Всякая максимальная конечная подгруппа группы $\mathrm{GL}(n,\mathbb{Z})$ является подгруппой Браве, но обратное, вообще говоря, не имеет места. Наименьшая подгруппа Браве, содержащая кристаллографическую точечную группу G, *рассматриваемая с точностью до сопряженности в* $\mathrm{GL}(n,\mathbb{R})$, называется **голоэдрией** (или, если быть совсем точным, **геометрической голоэдрией**) группы G. Говорят, что две группы H и G относятся к одной и той же **сингонии** (alias, **кристаллографической системе**, Kristallsystem), если их голоэдрии совпадают. Кристаллографический класс, обладающий максимальной возможной симметрией (т.е. класс, совпадающий со своей собственной голоэдрией) называется **голоэдрическим классом**.

[133]Герман Вейль в книге [W2] приписывает первую явную формулировку этого результата Леонардо да Винчи: "Будучи выраженным в современных абстрактных терминах его результат, в сущности, совпадает с приведенной нами выше таблицей возможных групп вращений (собственных и несобственных) для случая двух измерений" – стр.92.

[134]Гадолин (1828–1892) был не профессиональным кристаллографом, а офицером-артиллеристом, к открытию 32 кристаллографических классов он пришел при подготовке к лекциям по физике в Артиллерийской Академии!

[135]Отец Зонке (1842–1897) был профессором математики, так что свое имя он получил в честь Леонарда Эйлера.

При $n = 3$ существует 7 сингоний, которые имеют традиционные кристаллографические названия[136]: **триклинная** (кристаллы, не имеющие ни осей, ни плоскостей симметрии), **моноклинная** (кристаллы, имеющие одну двойную ось, или одну плоскость симметрии), **ромбическая** (кристаллы, имеющие три взаимно перпендикулярные двойные оси, иногда ромбическая сингония называется еще **орторомбической**), **тригональная** (кристаллы, имеющие одну тройную ось), **тетрагональная** (кристаллы, имеющие одну четверную ось – т.е. ось 4-го порядка), **гексагональная** (кристаллы, имеющие одну ось 6-го порядка) и **кубическая** (кристаллы, имеющие 4 тройные и 3 четверные оси).

Теорема. *При $n = 3$ имеется ровно 32 кристаллографических класса, которые следующим образом разбиваются по сингониям:*

сингония:	голоэдрия:	кристаллографический класс:
триклинная	C_i	$C_1 \times C_2, C_1$
моноклинная	C_{2h}	$C_2 \times C_2, C_2, C_2C_1$
ромбическая	D_{2h}	$D_2 \times C_2, D_2, D_2C_2$
тригональная	D_{3d}	$D_3 \times C_2, D_3, D_3C_3, C_3 \times C_2, C_3$
тетрагональная	D_{4h}	$D_4 \times C_2, D_4, D_4C_4, D_4D_2, C_4 \times C_2, C_4, C_4C_2$
гексагональная	D_{6h}	$D_6 \times C_2, D_6, D_6C_6, D_6D_3, C_6 \times C_2, C_6, C_6C_3$
кубическая	O_h	$O, O^+, T, T^+ \times C_2, T$

Каждый из 32-х кристаллографических классов тоже имеет традиционное кристаллографическое название[137]. Скажем, класс C_1 называется моноэдрическим, класс $C_1 \times C_2$ – пинакоидальным, класс C_2 – сфеноидальным, класс C_2C_2 – доматическим, класс $C_2 \times C_2$ – призматическим и т.д. вплоть до тритетраэдрического класса T^+, дидокаэдрического класса $T^+ \times C_2$, триоктаэдрического класса O^+, гексатетраэдрического класса T и, наконец, гексаоктаэдрического класса O.

§ 11. Точечные группы, 2nd instalment: типы Браве и арифметические классы

Мы продолжаем интересоваться кристаллографическими точечными группами, т.е. конечными подгруппами в $\mathrm{GL}(3, \mathbb{Z})$. Однако теперь нас интересуют классы сопряженности кристаллографических точечных групп не в $\mathrm{GL}(n, \mathbb{R})$, а в самой группе $\mathrm{GL}(n, \mathbb{Z})$. Эти классы называются **арифметическими классами**. Имеется ровно 13 класса при $n = 2$ и 72 класса при $n = 3$ и 710 классов при $n = 4$.

Аналогом сингонии для арифметических классов является понятие типа Браве. Наименьшая подгруппа Браве, содержащая кристаллографическую точечную группу G, рассматриваемая с точностью до сопряженности в $\mathrm{GL}(n, \mathbb{Z})$, называется **арифметической голоэдрией** группы G. Говорят, что две группы H и G относятся к одному и тому же **типу Браве**, если их *арифметические* голоэдрии совпадают. При $n = 2$ имеется 5 типов Браве, при $n = 3$ – 14, а при $n = 4$ – уже 64.

§ 12. n-мерная кристаллография

Подгруппа $G \leq \mathrm{Isom}(\mathbb{R}^n)$ группы движений эвклидова пространства $V = \mathbb{R}^n$ называется **кристаллографической**, если она дискретна, а фактор по ней V/G компактен. Подгруппа $G \leq \mathrm{Isom}(\mathbb{R}^n)$ группы движений эвклидова пространства является **федоровской**, если, *кроме того*, в G существует n-мерная подгруппа трансляций.

Когда Федоров принес свою работу Чебышеву, тот даже не стал ее смотреть и сказал буквально следующее: 'это не может *сегодня* интересовать математиков'. Ирония истории состоит в том, что после того, как была обнаружена связь теории решеток с алгебраической

[136]См., например, Э.Уиттекер, Кристаллография, Мир, М., 1983, таблица 3.1 на стр.34. или Г.Смит, Драгоценные камни, Мир, М., 1980, с.1–586, описание сингоний на с.29–34.

[137]См., например, Т.Пенкаля, Очерки кристаллохимии. – Химия, Л., 1974, с.1–496, Таблица 3.3 'названия и обозначения 32 классов симметрии' на ст.49–51.

теорией чисел и теорией квадратичных форм изучение федоровских групп их аналогиов и обобщений стало одним из основных направлений для детей, внуков, правнуков и праправнуков Чебышева: Коркина, Золотарева, Маркова, Делоне, Фаддеева, Венкова, ...

Первая теорема Бибербаха[138]**.** *Все кристаллографические группы являются федоровскими. Точнее, все параллельные переносы, содержащиеся в кристаллографической группе G образуют нормальную подгруппу $H \trianglelefteq G$ конечного индекса в G.*

Вторая теорема Бибербаха. *Две кристаллографические группы в том и только том случае изоморфны как абстрактные группы, когда они либо сопряжены в* $\mathrm{Isom}^+(\mathbb{R}^n)$*, либо энантиоморфны.*

Вопрос о конечности числа классов кристаллографических групп в n-мерном эвклидовом пространстве составлял первую половину 18-й проблемы Гильберта[139] и представлялся самому Гильберту весьма трудным. Однако Бибербах положительно решил его уже в 1910–1912 годах.

Третья теорема Бибербаха. *Для каждого n существует конечное число классов изоморфизма кристаллографических подгрупп в группе* $\mathrm{Isom}(\mathbb{R}^n)$.

На русском языке доказательство теорем Бибербаха и Жордана можно найти, например, в книге [Wo], с.122–128.

В 1948 году Ганс Цассенхауз показал, как классифицировать n-мерные федоровские группы, зная конечные подгруппы в $\mathrm{GL}(n,\mathbb{Z})$. Все федоровские группы в размерности 4 были фактически классифицированы в 1971 году в работах Вондрачека, Нойбюзера и Бюлова.

§ 13. Одномерная кристаллография

В чисто одномерном мире существуют только две бесконечные кристаллографические группы, а именно, группа $\mathbb{Z}$, порожденная одной трансляцией и группа D_∞, порожденная двумя центральными симметрии. Однако можно рассмотреть группы симметрий в пространстве n измерений, допускающие трансляции лишь в одном направлении.

1. Группы симметрии бордюров. Двумерный объект, допускающий трансляцию лишь в одном направлении, называется **бордюром**. По английски в этом контексте принято говорить о симметрии **фризов**, frieze[140]. Кроме архитектуры эти группы часто встречаются в прикладном искусстве: книжная миниатюра, керамика, вышивки, инкрустации, резьба, татуировки. Имеется всего 7 видов симметрии бордюров и классифицировать их совсем просто (см., например, [C?], таблица на странице 83 или [Spe], с.81–82).

Теорема. *С точностью до сопряженности в* $\mathrm{Isom}(\mathbb{R}^2)$ *имеется ровно 7 групп симметрии бордюров, перечисленных в следующей таблице*

бордюр:	группа:	образующие:	IUCr:
ГГГГГГГГ	$\mathbb{Z}$	одна трансляция	?
ГLГLГLГL	$\mathbb{Z}$	одна скользящая симметрия	?
DDDDDDDD	$\mathbb{Z} \times C_2$	трансляция и горизонтальное отражение	?
NNNNNNNN	D_∞	два полуповорота	?
VVVVVVVV	D_∞	два вертикальных отражения	?
ΛVΛVΛVΛV	D_∞	отражение и полуповорот	?
HHHHHHHH	$D_\infty \times C_2$	три отражения	?

Группа ?, порожденная двумя полуповоротами, известна как **группа симметрий меандра**.

---

[138]**Людвиг Бибербах** (1886 –) –

[139]Проблемы Гильберта, – Наука, М., 1969, с.1–239с. – см. стр.50–51

[140]В классической архитектуре фризом называется среднее членение антаблемента, ограниченное снизу архитравом, а сверху карнизом. Фризы часто покрывались периодически повторяющимися рисунками или рельефами. Впрочем, с таким же основанием можно говорить о симметрии карнизов.

2. Группы симметрии стержней. Трехмерный объект, допускающий трансляцию лишь в одном направлении, называется **стержнем**. Симметрия стержней описывает симметрию объектов в физике, химии, биологии, ширина и толщина которых малы по сравнению с длиной, таких как молекулярные цепи (скажем, ДНК), стебли растений, пучки света. В быту мы встречаемся с этой симметрией рассматривая нити, шнуры, канаты, нитки бус, трубы, (коленчатые) валы, (якорные) цепи и т.д. Полная классификация всех 75 групп симметрии стержней была осуществлена в 1929-м году Е.Александером[141]. На русском языке все группы симметрии стержней перечислены, например, в [ShK], таблица 6. Стержни с осями симметрии не выше второго порядка называются **лентами**, отличие ленты от бордюра состоит в том, что ленту можно перевернуть. Иными словами, у ленты *две* стороны, которые могут преобразовываться друг в друга. Симметрия лент подробно описана в книге Шпейзера [Spe].

§ 14. Двумерная кристаллография

1. Группы симметрии орнаментов. Плоские кристаллографические группы были впервые полностью классифицированы в 1891 году Е.С.Федоровым в работе 'Симметрия на плоскости', их оказалось ровно 17. Интересно отметить, что еще в 1869 году Камиль Жордан перечислил 16 из этих групп, а 17-я группа была открыта в 1874 году Зонке, но он пропустил три других. Независимо, но много позже эти группы классифицировали Пойа и Ниггли[142,143]. Часто утверждается, что все 17 кристаллографических групп были использованы в орнаментах Альгамбры[144,145], но в действительности там использованы лишь 13 групп[146]. Интересно, что в книге[147] воспроизводятся 14 из 17 плоских кристаллографических групп (все, кроме pm, p3 и pg).

Дорис Шаттшнейдер[148] отмечает, что Морис Эшер[149] скопировал полный текст работы Пойи в своей рабочей тетради. Диаграммы из статьи Пойа, наряду с орнаментами, которые он скопировал в Альгамбре, стали основным источником, на основе которого он смог развить

---

[141]E.Alexander, Systematik der eindimensionalen Raumgruppen. – Z. Kristallographie, 1929, Bd.70, S.367–382.

[142]G.Pólya, Über die Analoge der Kristallsymmetrie in der Ebene – Z. Kristallographie, 1924, Bd.60, S.278–282.

[143]P.Niggli, Die Flächensymmetrien homogener Diskontinuen. – Z. Kristallographie, 1924, Bd.60, S.283–298.

[144]Альгамбра, (от арабского аль-Хамра – красная) – построенный в XIII–XIV веках дворцовый комплекс мавританских правителей Гранадского эмирата, расположенный на восточной окраине современной Гранады, один из самых удивительных памятников поздней мавританской архитектуры.

[145]В [CM], с.54 говорится буквально следующее: 'Все 17 таких групп были открыты эмпирически Мурсом в **его** украшениях Альгамбры в Гренаде' (перевод В.А.Чуркина под редакцией Ю.И.Мерзлякова). Кроме того, что это утверждение неверно по существу, здесь содержится две курьезных ошибки. Прежде всего, Гренадой раньше назывался один из Антильских островов, а Альгамбра расположена все-таки в Гранаде. Чуть сложнее установить личность великого художника Мурса. Для этого достаточно представить, что в английском оригинале написано 'by Moors'.

[146]Там **не** используются группы p2, p3m1, pg и pgg. Интересно отметить, что орнаменты с группой p2 очень часто встречаются в декорации египетских гробниц и саркофагов, и позже, уже после арабского завоевания, воспроизводились в мозаиках, а орнаменты с группой p3m1 типичны для оформления персидских манускриптов. В то же время специалисты считают, что группы pg и pgg вообще никогда не использовались в исламском искусстве.

[147]D.S.Dye, A grammar of Chinese lattice. – Harvard Univ. Press, Cambridge, Mass., 1937 (reprinted by Dover under the title 'Chinese lattice design', 1974.)

[148]D.Schattschneider, The plane symmetry groups: their recognition and notation. – Amer. Math. Monthly, 1978, June–July, p.439–450.

[149]**Морис Эшер** (1898–1972) – замечательный голландский график, широко использовавший в своих работах геометрические и топологические мотивы, в частности, почти все плоские кристаллографические группы, правильные многогранники, модель Пуанкаре геометрии Лобачевского, и т.д.

свой геометрический стиль. Мы видим эти группы вокруг себя в повторяющемся рисунке обоев (по-английски плоские кристаллографические группы обычно и называются просто wallpaper groups), паркетных и кафельных полов и т.д.

2. Алгоритм распознавания обойных групп. Следующий алгоритм хорошо известен. Он описан, в частности, в[150]. Для того, чтобы определить группу требуется ответить самое большее на 5 вопросов.

Старт:

Допускает ли картинка хотя бы одно отражение?

- **Да:** допускает ли картинка вращения?
  - ⋆ **Да:** каков наименьший угол поворота?
    - ∘ π**:** допускает ли картинка отражения в двух направлениях?
      - ◇ **Да:** Лежат ли все центры вращений на зеркалах?
        - ∗ **Да: pmm**
        - ∗ **Нет: cmm**
      - ◇ **Нет: pmg**
    - ∘ $2\pi/3$**:** Лежат ли все центры вращений на зеркалах?
      - ◇ **Да: p3m1**
      - ◇ **Нет: p31m**
    - ∘ $\pi/2$**:** Существуют ли два зеркала под углом $\pi/4$?
      - ◇ **Да: p4m**
      - ◇ **Нет: p4g**
    - ∘ $\pi/3$**: p6m**
  - ⋆ **Нет:** имеется ли скользящее отражение не лежащее на зеркале?
    - ∘ **Да: cm**
    - ∘ **Нет: pm**
- **Нет:** допускает ли картинка вращения?
  - ⋆ **Да:** каков наименьший угол поворота?
    - ∘ π**:** имеется ли скользящее отражение?
      - ◇ **Да: pgg**
      - ◇ **Нет: p2**
    - ∘ $2\pi/3$**: p3**
    - ∘ $\pi/2$**: p4**
    - ∘ $\pi/3$**: p6**
  - ⋆ **Нет:** имеется ли скользящее отражение?
    - ∘ **Да: pg**
    - ∘ **Нет: p1**

Финиш

Применяйте этот алгоритм к рисункам Эшера, обоям, кафельным полам, пока не достигните полного автоматизма и не будете в состоянии распознавать обойные группы с первого взгляда.

3. Группы симметрии слоев. Трехмерный объект, допускающий трансляцию в двух направлениях, называется **слоем**. Симметрия слоев описывает симметрию объектов в физике, химии и биологии, толщина которых мала по сравнению с двумя другими измерениями, таких как эпитаксиальные пленки, мембраны, поверхности раздела, оболочки, жидкие кристаллы, и т.д. В быту мы встречаемся с этой симметрией рассматривая экраны, ширмы,

[150]Washburn, Crowe, Symmetries of culture, Table 5.1.

решетки[151], ограды, (двусторонние) вывески, кружева и т.д. Полная классификация всех 80 групп симметрии слоев была осуществлена в 1929-м году Е.Александером и К.Германном[152]. На русском языке все группы симметрии слоев перечислены, например, в [ShK], таблица 11.

§ 15. Трехмерная кристаллография

[151]Не в строгом математическом смысле, который обсуждался выше, а такие, как решетка Летнего Сада.

[152]E.Alexander, K.Hermann, Die 80 zweidimensionalen Raumgruppen. – Z. Kristallographie, 1929, Bd.69, S.285–299; Bd.70, S.328–345.

Тема 4. ГОМОМОРФИЗМЫ ГРУПП

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. Сознательно использование гомоморфизмов групп начал Непер, но название появилось 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. 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 G и 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 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. Тех, кто хочет ознакомиться с работами классиков, стоит предостеречь, что следуя Жордану в XIX веке изоморфизмами называли *эпиморфизмы*[153]. То, что мы называем изоморфизмом, при этом называлось **голоэдрическим изоморфизмом** (isomorphisme holoédrique, einstufiger Isomorphismus, holohedral isomorphism), а эпиморфизмы, не являющиеся изоморфизмами, назывались **мероэдрическими**[154] **изоморфизмами** (isomorphisme meriédrique, mehrstufiger Isomorphismus, merohedral isomorphism). Однако уже в 1904 году де Сегье пользовался современной терминологией[155].

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 раз и понималась как изучение алгебраических систем **с точностью до изоморфизма**. Вот несколько очевидных изоморфизмов, которые подробнее обсуждаются в следующем параграфе: $\mathbb{R}_+ \cong \mathbb{R}^+$, $\mathbb{C}^+ \cong (\mathbb{R}^+)^2$, $\mathbb{C}^* \cong \mathbb{T} \times \mathbb{R}_+$, $\mathbb{Z}/m\mathbb{Z} \cong \mu_n$. Однако в действительности понятие изоморфности является *чрезвычайно* тонким. Так, например, можно показать (это будет сделано в Главе IV), что $\mathbb{C}^* \cong \mathbb{T}$, хотя этот изоморфизм отнюдь не очевиден.

Задача. Даны 6 рациональных дробей

$$x,\ \frac{1}{x},\ 1-x,\ \frac{x}{x-1},\ \frac{x-1}{x},\ \frac{1}{1-x}.$$

Убедитесь, что относительно композиции эти 6 дробей образуют группу. Проверьте, что эта группа изоморфна S_3.

Задача (основная теорема арифметики). Докажите, что $\mathbb{Q}^*_{>0} \cong \mathbb{Z}[x]^+$.

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 подробно изучается 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*

[153]См., например, А.Пуанкаре, Избранные труды, т.III, М., Наука, 1974, с.1–771, страницы 9–10 (оригинал опубликован в 1882 году).

[154]Вариант: **мериэдрическими**.

[155]J.-A.de Séguier, Theorie des groupes finis. Eléments de la théorie des groupes abstraits. – Gauthier-Villars, Paris, 1904.

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?

3. Классы сопряженных гомоморфизмов. 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 логарифм с натуральным основанием e:

$$\begin{aligned} &\exp : \mathbb{R}^+ \longrightarrow \mathbb{R}_+, \qquad x \mapsto e^x, \\ &\log : \mathbb{R}_+ \longrightarrow \mathbb{R}^+, \qquad x \mapsto \log_e(x). \end{aligned}$$

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 $\mathbb{R}_+ \longrightarrow \mathbb{R}^+$, $x \mapsto \log_a(x)$, являются гомоморфизмами между аддитивной и мультипликативной структурами $\mathbb{R}$. Как мы вскоре увидим, никаких других таких *непрерывных* гомоморфизмов нет.

• **Знак и абсолютная величина.** Отображение $|\ | : \mathbb{R}^* \longrightarrow \mathbb{R}_+$, $x \mapsto |x|$, 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 и $|xy| = |x||y|$ 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: $|\ |:\mathbb{C}^*\longrightarrow\mathbb{R}_+$ 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 § ?. 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 Главе 5 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 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, возникающие в абелевой группе. В следующих примерах существенно, что группа G абелева.

• **Обращение в абелевой группе.** Пусть теперь G аддитивно записанная абелева группа. В этом случае 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, $n \geq 3$?

Задача[156]**.** Докажите, что количество 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 – такая группа, 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, $g \in G$, $gx^n g^{-1} = (gxg^{-1})^n$, 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. Рассмотрим $\varphi, \psi \in \mathrm{Hom}(G, H)$, где группа H абелева. 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 его обратный 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** $x \mapsto x^t$,

[156] J.A.Gallian, J.Van Buskirk, The number of homomorphisms from $\mathbb{Z}_m$ into $\mathbb{Z}_n$. – Amer. Math. Monthly, 1984, vol.91, p.196–197. В действительности, в этой работе вычисляется количество **кольцевых** гомоморфизмов $\mathbb{Z}/m\mathbb{Z}$ в $\mathbb{Z}/n\mathbb{Z}$, где ответ уже не столь очевиден.

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 возникают в произвольных группах, но второй из них интересен только только для неабелевых групп.

• 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, $g^{m+n} = g^m g^n$. 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 ${}^g x$ 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'.

• **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 § ? 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 $N_G(H) = HC_G(H)$.

5. Группы с одним или двумя автоморфизмами. Следующая задача предполагает знакомство с векторными пространствами (а при чем здесь векторные пространства?). Она замечательна тем, что для ее решения требуются

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. 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. Характеристические подгруппы

Нормальная подгруппа – это подгруппа, устойчивая под действием **внутренних** автоморфизмов. Сейчас мы усилим это понятие. Однако, как замечает по этому поводу Лао-цзы, 'прежде, чем построить высокую башню, вначале копают глубокую яму'.

1. Субнормальные подгруппы. 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 $F \not\trianglelefteq G$. Это оправдывает введение следующего класса подгрупп.

Определение. *Говорят, что подгруппа $F \trianglelefteq G$* **субнормальна** *в G и пишут $F \trianglelefteq\trianglelefteq G$, если существует ряд подгрупп*

$$F = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_d = G$$

в котором каждая подгруппа является нормальной 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.

Задача (Виландт[157]) 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,

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_s = G.$$

[157]H.Wielandt, Eine Verallgemeinerung der invarianten Untergruppen. – Math. Zeitschrift, 1939, Bd.45, S.209–244.

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. 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** $\varphi \in \mathrm{End}(G)$

В старых книгах характеристические подгруппы называются **автоморфно допустимыми**, а вполне характеристические – **эндоморфно допустимыми**. По определению любая вполне характеристическая 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. *1) Характеристическая подгруппа нормальной подгруппы является нормальной подгруппой.*

2) Характеристическая подгруппа характеристической подгруппы является характеристической подгруппой.

3) Вполне характеристическая подгруппа вполне характеристической подгруппы является вполне характеристической подгруппой.

Доказательство. Докажем для иллюстрации 1), доказательство двух других пунктов 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 $F \trianglelefteq G$.

3. Примеры характеристических подгрупп. Приведем несколько очевидных примеров характеристических подгрупп.

• Коммутант $[G, G]$ группы G является вполне характеристической подгруппой;

• Подгруппа G^n, порожденная n-ми степенями элементов группы G, является вполне характеристической;

Это примеры так называемых **вербальных** подгрупп, порожденных значениями некоторых слов в группе G: в первом случае слова $[x, y]$, а во втором – слова x^n. А вот несколько примеров характеристических, но, вообще говоря, не вполне характеристических подгрупп:

• Пересечение всех подгрупп индекса n;

• Пересечение всех подгрупп индекса $\leq n$;

- Пересечение всех нормальных подгрупп индекса n;
- Пересечение всех нормальных подгрупп индекса $\leq n$.

4. 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. Достаточно построить группу, центр которой не является вполне характеристической подгруппой.

Задача. Докажите, что пересечение (вполне) отмеченных подгрупп есть (вполне) отмеченная подгруппа.

5. 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[158,159] 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.

§ 5. 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)[160].

---

[158]B.H.Neumann, A two-generator group isomorphic to a proper factor group. – J. London Math. Soc., 1950, vol.25, p.247–248.

[159]G.Higman, A finitely related group with an isomorphic proper factor group. – J. London Math. Soc., 1951, vol.26, p.59–61.

[160]В теории алгебр Ли алгебры без характеристических идеалов называются **дифференциально простыми**, поэтому некоторые специалисты предпочитают говорить об **автоморфно простых** группах.

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, то $F \cap H_j = H_j$. Это значит, что $H_j \leq F$ и, так как группа $\mathrm{Aut}(G)$ транзитивно действует на факторах $H_1, \ldots, H_s$, то $H_i \leq F$ 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 $F = H$. Так как по условию подгруппа H не может быть характеристической, то существует гомоморфизм $\varphi \in \mathrm{Aut}(G)$ такой, что $\varphi(H) \neq H$. Пусть $H_1 = H, H_2 \ldots, H_s$, где $s \geq 2$, – множество всех различных подгрупп, в которые H переходит под действием $\mathrm{Aut}(G)$. Ясно, что подгруппа $H_1 \ldots H_s$ 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 $H_2, \ldots, H_s$. Тем самым, любой нормальный делитель группы H автоматически является нормальным делителем в G. В силу минимальности H это значит, что H обязана быть простой группой. Пересечение $H \cap H_2 \ldots H_s$ содержится в центре H и, значит, мы имеем следующую альтернативу, либо $H \leq H_2 \ldots H_s$, либо $H \cap H_2 \ldots H_s = 1$. В первом случае H абелева, $H \leq C(G)$ и, так как $C(G)$ является характеристической подгруппой, то $C(G) = G$. 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 $H_i \cap H_1 \ldots \widehat{H}_i \ldots H_s = 1$. Но это и означает, что $G = H_1 \times \ldots \times H_s$.

Замечание. В действительности в этой теореме конечность группы использовалась лишь для того, чтобы гарантировать существование е G минимального нормального делителя. Именно в такой форме и сформулирован этот результат в [Sch], стр.62, но приведенные там доказательства содержат пробелы.

§ 6. 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 того, определить **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 Главе 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, [KM], с.57–58

по поводу доказательства);

- $\mathrm{End}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p$;
- $\mathrm{End}(\mathbb{Z}^n) \cong M(n,\mathbb{Z})$;
- $\mathrm{End}(E_{p^n}) \cong M(n,\mathbb{F}_p)$.

Первые почти всех этих утверждений очевидны: для этого достаточно заметить, что эндоморфизм циклической группы полностью определяется своим значением на образующей, которое моэжет 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 через $\mathrm{Aut}(G)$ обозначается группа всех автоморфизмов группы G 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 примера непосредственно вытекают из соответствующих примеров предыдущего пункта.

- $\mathrm{Aut}(\mathbb{Z}^+) \cong C_2$;
- $\mathrm{Aut}(C_n) \cong (\mathbb{Z}/n\mathbb{Z})^*$;
- $\mathrm{Aut}(\mu_{p^\infty}) \cong \mathbb{Z}_p^*$;
- $\mathrm{Aut}(\mathbb{Z}_p^+) \cong \mathbb{Z}_p^*$;
- $\mathrm{Aut}(\mathbb{Z}^n) \cong \mathrm{GL}(n,\mathbb{Z})$;
- $\mathrm{Aut}(E_{p^n}) \cong \mathrm{GL}(n,p)$.

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 Главе VI. 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. А именно, для $p = 2$ имеем $\mathrm{Aut}(C_2) = 1$, $\mathrm{Aut}(C_4) \cong C_2$ и $\mathrm{Aut}(C_{2^m}) \cong C_2 \cong C_{2^{m-1}}$, в то время как для нечетного p всегда $\mathrm{Aut}(C_{p^m}) \cong C_{(p-1)p^{m-1}}$.

Обратите внимание, что $\mathrm{Aut}(C_3) \cong \mathrm{Aut}(C_4) \cong C_2$. Можно доказать[161], что для данной конечной группы H существует не более конечного числа неизоморфных конечных групп G таких, что $\mathrm{Aut}(G) \cong H$. При этом далеко не всякая группа может быть представлена как группа автоморфизмов. Так, например, легко доказать (это одна из задач следующего параграфа!), что не существует группы G — конечной или бесконечной — для которой $\mathrm{Aut}(G) \cong C_{2l+1}$ есть циклическая группа нечетного порядка. Не реализуются как группы автоморфизмов также и симметрическая группа S_6 (это как раз то исключение, которое возникает в теореме Гельдера!), ни одна из нетривиальных знакопеременных

[161] H.K.Iyer, Rocky Mountain J. Math., 1979, vol.9, N.4, p.653–670.

групп A_n, кроме $A_8 \cong \mathrm{PSL}(4,2)$, и 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?

• В § ? мы проверим, что $\mathrm{Aut}(S_n) = S_n$ при $n \neq 2, 6$ (теорема Гельдера).

• В третьем семестре мы вычислим группу $\mathrm{Aut}(\mathrm{GL}(n,K))$ и покажем, что каждый автоморфизм $\mathrm{GL}(n,R)$ является произведением внутреннего и полевого автоморфизмов и, возможно, контраградиента (теорема Шрайера – ван дер Вардена).

Задача. Докажите, что $\mathrm{Aut}(D_3) \cong D_3$ и $\mathrm{Aut}(D_4) \cong D_4$. Какая гипотеза у Вас возникла? А теперь вычислите $\mathrm{Aut}(D_n)$.

Решение. Эта 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, то $\varphi(y) = x^j y$ 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[162], позволяет проверить, что $\mathrm{Aut}(D_n) \cong C_{\varphi(n)} \leftthreetimes C_n$, 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.

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 $\mathrm{GL}(n,p)$.*

§ 7. Строение группы автоморфизмов

В настоящем параграфе мы обсудим некоторые аспекты строения группы $\mathrm{Aut}(G)$, которые впервые начал рассматривать в 1893 году О.Гельдер.

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.

[162] G.L.Walls, Automorphism groups. – Amer. Math. Monthly, 1986, June–July, p.459–462. Теорема A.

Теорема. *Подгруппа* $\mathrm{Inn}(G) \cong G/C(G)$ *нормальна в* $\mathrm{Aut}(G)$.

Доказательство. Первое 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 $C(G)$. Для доказательства второго утверждения заметим, что следующее 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.

Следствие. *Группа без центра* G *изоморфно вкладывается в группу* $\mathrm{Aut}(G)$.

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. Вычислить 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.

Автоморфизм $\varphi \in \mathrm{Aut}(G)$ называется **центральным**, если $g^{-1}\varphi(g) \in C(G)$ для всех $g \in G$.

Задача. Показать, что для того, чтобы автоморфизм φ группы G был перестановочен со всеми внутренними автоморфизмами, необходимо и достаточно, чтобы он был центральным.

В частности, если $C(G) = 1$, то $C_{\mathrm{Aut}(G)}(\mathrm{Inn}(G)) = 1$. В общем случае можно утверждать, что центральные автоморфизмы образуют подгруппу в $\mathrm{Aut}(G)$. Это утверждение 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 $\mathrm{IAut}(G) \trianglelefteq \mathrm{Aut}(G)$.

2. Группа автоморфизмов неабелевой простой группы. Следующий цикл задач взят со страницы 131 Бурбаки, Алгебра, т.I.

Задача. Пусть G – неабелева простая группа. Показать, 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* $\mathrm{Aut}(G) \cong \mathrm{Aut}(\mathrm{Aut}(G))$.

3. 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).

§ 8. Матричные гомоморфизмы

Следующие примеры предполагают знакомство с умножением матриц.

• **Однопараметрические мультипликативные 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 аддитивные подгруппы.** Следующий 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

$$\begin{pmatrix} x_{11}x_{22}-x_{12}x_{21} & x_{11}x_{23}-x_{13}x_{21} & x_{11}x_{24}-x_{14}x_{21} & x_{12}x_{23}-x_{13}x_{22} & x_{12}x_{24}-x_{14}x_{22} & x_{13}x_{24}-x_{14}x_{23} \\ x_{11}x_{32}-x_{12}x_{31} & x_{11}x_{33}-x_{13}x_{31} & x_{11}x_{34}-x_{14}x_{31} & x_{12}x_{33}-x_{13}x_{32} & x_{12}x_{34}-x_{14}x_{32} & x_{13}x_{34}-x_{14}x_{33} \\ x_{11}x_{42}-x_{12}x_{41} & x_{11}x_{43}-x_{13}x_{41} & x_{11}x_{44}-x_{14}x_{41} & x_{12}x_{43}-x_{13}x_{42} & x_{12}x_{44}-x_{14}x_{42} & x_{13}x_{44}-x_{14}x_{43} \\ x_{21}x_{32}-x_{22}x_{31} & x_{21}x_{33}-x_{23}x_{31} & x_{21}x_{34}-x_{24}x_{31} & x_{22}x_{33}-x_{23}x_{32} & x_{22}x_{34}-x_{24}x_{32} & x_{23}x_{34}-x_{24}x_{33} \\ x_{21}x_{42}-x_{22}x_{41} & x_{21}x_{43}-x_{23}x_{41} & x_{21}x_{44}-x_{24}x_{41} & x_{22}x_{43}-x_{23}x_{42} & x_{22}x_{44}-x_{24}x_{42} & x_{23}x_{44}-x_{24}x_{43} \\ x_{31}x_{42}-x_{32}x_{41} & x_{31}x_{43}-x_{33}x_{41} & x_{31}x_{44}-x_{34}x_{41} & x_{32}x_{43}-x_{33}x_{42} & x_{32}x_{44}-x_{34}x_{42} & x_{33}x_{44}-x_{34}x_{43} \end{pmatrix}$$

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. Матрица $S^m(x)$ называется **m-й симметрической степенью** матрицы x. **Теорема Бине-Коши для перманентов**[163], утверждает, что отображение S^m является гомоморфизмом группы $\mathrm{GL}(n,R)$ в группу $\mathrm{GL}(C^m_{m+n-1},R)$, а именно, $S^m(xy) = S^m(x)S^m(y)$.

[163] Х.Минк, Перманенты, Мир, М., 1982, с.1–213, теорема 1.3 на с.30

§ 9. 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 $\varphi(m/n) = c(m/n)$.

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[164]. 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 $\mathbb{R}$ 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 $\mathbb{R}_+$ 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 $\mathbb{R}_+ \longrightarrow \mathbb{R}_+$, $x \mapsto x^c$, где $c \in \mathbb{R}$, являются единственными* **непрерывными** *эндоморфизмами $\mathbb{R}_+$.*

Следствие 2. *Отображения $\mathbb{R}^+ \longrightarrow \mathbb{R}^*$, $x \mapsto c^x$, где $c \in \mathbb{R}_+$, являются единственными* **непрерывными** *гомоморфизмами $\mathbb{R}^+$ в $\mathbb{R}^*$.*

---

[164] G.Hamel, Eine Basis aller Zahlen und die unstetige Lösungen der Funktionalgleichung $f(x+y) = f(x) + f(y)$. – Math. Ann., 1905, Bd.60, S.459–462.

Следствие 3. *Отображения* $\mathbb{R}_+ \longrightarrow \mathbb{R}^+$, $x \mapsto \log_c(x)$, *где* $c \in \mathbb{R}_+$, $c \neq 1$, *являются единственными* **непрерывными** *гомоморфизмами* $\mathbb{R}_+$ *в* $\mathbb{R}^+$.

В книжке Фихтенгольца все эти четыре утверждения трактуются как независимые теоремы, с четырьмя разными (не слишком короткими) доказательствами!

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 Главах ? и ? если поле K бесконечно, этого вопроса не возникает. Следующий результат моментально вытекает также из леммы Дедекинда-Артина, 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 принципу несущественности алгебраических неравенств $f(xy)$ 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.

§ 10. Образ и ядро гомоморфизма

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, а именно, 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. Верно ли, что уравнитель $\mathrm{Eq}(f, g)$ двух любых гомоморфизмов $f, g : H \longrightarrow G$ всегда является подгруппой в G?

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 $\mathrm{Ker}(I) = C(G)$.

• Пусть $\mathrm{sgn} : S_n \longrightarrow S_n$ – знак перестановки, тогда $\mathrm{Ker}(\mathrm{sgn}) = A_n$.

• Пусть $\det : \mathrm{GL}(n, K) \longrightarrow K^*$ – определитель, тогда $\mathrm{Ker}(\det) = \mathrm{SL}(n, K)$.

§ 11. Теорема о гомоморфизме

Сейчас мы покажем, что факторизация отображений согласована со структурой группы. Следующая теорема является одним из наиболее типичных и характерных результатов общей алгебры.

Теорема о гомоморфизме. *Пусть* $\varphi : H \longrightarrow G$ *– гомоморфизм групп. Тогда*

$$\mathrm{Im}(\varphi) \cong H/\mathrm{Ker}(\varphi).$$

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 $\sim = \sim_\varphi$ определяемой условием $x \sim y \Longleftrightarrow \varphi(x) = \varphi(y)$.

Покажем, прежде всего, что в случае, когда φ является гомоморфизмом, слои являются в точности смежными классами по $\mathrm{Ker}(\varphi)$. 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 теорему 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: $\operatorname{Inn}(G) = G/C(G)$.

§ 12. 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, [Pen], 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, профессионалы чаще ссылаются на него как **теорему Нетер об изоморфизме**[165].

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 § ?, приведем другое доказательство. А именно, 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 G – группа, $H \trianglelefteq G$ – нормальная подгруппа в G, $F \leq G$ – произвольная подгруппа. Тогда $H \cap F \trianglelefteq F$ и имеет место изоморфизм*

$$F/F \cap H = FH/H.$$

Доказательство. Рассмотрим гомоморфизм $\varphi : F \longrightarrow FH \longrightarrow FH/H$, $f \mapsto fH$, являющийся композицией вложения и канонической проекции. Так как любой правый смежный класс FH по H представляется в виде $(fh)H = fH$ для некоторых $f \in F$, $h \in H$, то φ сюръективен. Ясно, что $f \in F$ в том и только том случае лежит в $\mathrm{Ker}(\varphi)$, когда $f \in H$. Таким образом, $\mathrm{Ker}(\varphi) = F \cap H$ и для завершения доказательства осталось лишь сослаться на теорему о гомоморфизме.

Задача. Пусть $f : G \longrightarrow G'$ – гомоморфизм групп, $H \leq G$. Покажите, что

$$|G : H| = |\,\mathrm{Ker}(f) : \mathrm{Ker}(f|H)| \cdot |\,\mathrm{Im}(f) : \mathrm{Im}(f|H)|.$$

Указание. Если группа G конечна, то это просто теорема о гомоморфизме + теорема Лагранжа. В общем случае придется рассмотреть группу $F = H\,\mathrm{Ker}(f)$ и воспользоваться теоремой Нетер.

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

$$(gF)^{-1}(hF)(gF) = (g^{-1}hg)F.$$

[165]**Эмми Нетер** (23.03.1882, Эрланген – 14.04.1935, Брин Мор) – один из основателей современной алгебры, оказавшая огромное влияние на развитие математики в XX веке. Вероятно, самая замечательная женщина во всей истории математики. Дочь замечательного алгебраического геометра Макса Нетера, ученица Гильберта. Среди ее учеников Эмиль Артин, Бартельс ван дер Варден, ... В нашем курсе встречаются нетеровы кольца, теорема Нетер об изоморфизме.

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**[166].

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 $F \leq H = \mathrm{Ker}(\pi)$, то 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.

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.

[166] **Вальтер фон Дик** (1856–1934) –

Тема 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 мало-помалу ясно, в ней непременно следует разобраться, прежде чем мы сможем постичь науку композиции звонов и их исполнения.
>
> C.A.W.Troyte, Change Ringing.

Сейчас мы разберем *ключевой* пример группы: **симметрическую группу конечного множества**. Эта группа играет совершенно особую роль во всей теории.

• **история**: теория групп возникла в работах Лагранжа, Руффини, Абеля, Галуа и Коши[167]. 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[168] и других классиков теория групп развивалась *в первую очередь* как теория групп перестановок. Лишь на рубеже XIX и XX

[167]**Огюстен Луи Коши** (21.08.1789, Париж – 23.05.1857, 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. 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. 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, ... После июльской революции 1830 года из-за своих крайних клерикально-монархических взглядов вынужден был покинуть Францию и 8 лет жил за границей, главным образом в Турине и Праге. После возвращения во Францию в 1838 он 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.

[168]**Джордж Абрам Миллер** (1863–1951) – известный специалист в области теории групп. Все 359 статей, включенных в его собранит сочинений, 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' ([ChM], стр.212).

веков Молин[169], Фробениус, Бернсайд[170], Диксон[171], Шур[172] и Блихфельд[173] превратили теорию групп в теорию матричных групп.

• **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 в группах (даже вычисления с матрицами!) реализованы именно как вычисления в группах перестановок.

• **приложения**: значительная часть приложений теории групп как в самой математике (теория колец, алгебры Ли, коммутативная алгебра, полилинейная алгебра, комбинаторика, геометрия, теория вероятностей), так и за ее пределами (теория твердого тела, квантовая химия, теория 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 нас интересуют главным образом перестановки конечных множеств, в дальнейшем мы можем считать, что $X = \underline{n} = \{1, \dots, n\}$ – множество первых n натуральных чисел.

---

[169] **Молин** (1861–1941) –

[170] **Бернсайд** (1852–1927) – замечательный английский алгебраист. Бернсайд был профессором Королевского Морского колледжа в Гринвиче и сомнительно, чтобы там ему довелось когда-нибудь читать курс по теории групп. Не было у Бернсайда и прямых учеников. Влияние Бернсайда обязано, главным образом его замечательной книге W.Burnside, Theory of groups of finite order. – Dover Repreint of the 1911 edition, N.Y., 1955.

[171] **Леонард Юджин Диксон** (1874–1954) –

[172] **Исайа Шур** (10.01.1875, Могилев – 10.01.1941, Тель Авив) – великий белорусский алгебраист, работавший в Германии и Израиле. Основные работы Шура относятся к теории групп, в первую очередь теории представлений и теории линейных групп, теории матриц, алгебраитческой теории чисел и теории степенных рядов. Шур учился в Берлине и в 1901 защитил диссертацию под руководством Фробениуса. Однако только в 1921 году он стал профессором, а в 1935 году вынужден был эмигрировать. В нашем курсе встречаются лемма Шура, мультипликатор Шура, теоремы Шура о линейных группах и большое количество теорем Шура в теории матриц.

[173] **Блихфельд** () –

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. 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[174]. 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'), 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 ('пермутационное представление', 'пермутационные игры' и т.д.). Тем не менее, в учебной литературе на русском языке архаизм 'подстановка' оказался удивительно живучим.

2. Полная запись перестановки. Обычно перестановки изображаются следующим образом. В первой строке изображаются элементы множества $\underline{n}$ в естественном порядке, а во второй строке – их образы 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 $\mathrm{id} = \begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix}$.

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

[174] L.Novy, Origins of modern algebra, Academia, Praha, 1973, p.1–252, см. pages 206–208.

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[175].

§ 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 $k \in \mathbb{Z}$.

[175] A.T.White, Ringing the cosets. – Amer. Math. Monthly, 1987, October, p.721–746.

Лемма. *Отношение $\sim$ является отношением эквивалентности.*

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 $\underline{n}/\sigma = \{X_1, \ldots, X_m\}$. Орбиты, содержащие более одного элемента, будут называться **нетривиальными**.

Задача. Докажите, что орбита элемента i совпадает с его **траекторией** $\{i, \pi(i), \pi^2(i), \ldots\}$.

Решение. *Обратимое* преобразование *конечного* множества имеет конечный порядок.

2. Фикс и подвижные элементы. С каждой перестановкой $\pi \in S_n$ можно связать два подмножества в $\underline{n}$, а именно, множества

$$\mathrm{Fix}(\pi) = \{i \in \underline{n} \mid \pi(i) = i\}, \qquad \mathrm{Mob}(\pi) = \{i \in \underline{n} \mid \pi(i) \neq i\}$$

стабильных alias **неподвижных** точек и **мобильных** alias **подвижных** 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 $i_1, \ldots, i_l \in \underline{n}$ – набор попарно различных символов. Тогда через $(i_1 \ldots i_l)$, обозначается цикл длины l с носителем $\{i_1, \ldots, i_l\}$, под действием которого

$$i_1 \mapsto i_2 \mapsto i_3 \mapsto \ldots \mapsto i_l \mapsto i_1,$$

а все остальные элементы множества $\underline{n}$ остаются на месте. Один и тот же цикл может быть записан по разному

$$(i_1 i_2 \ldots i_l) = (i_2 \ldots i_l i_1) = \ldots = (i_l i_1 \ldots i_{l-1}).$$

Обратный к циклу $(i_1 \ldots i_l)$ равен $(i_l \ldots i_1)$.

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 взаимно-обратных длинных цикла:

$$\texttt{RotateRight} = (123\ldots n), \qquad \texttt{RotateLeft} = (n, n-1, n-2, \ldots 1).$$

Задача. Найдите количество длинных циклов в S_n.

Решение. Запись длинного цикла имеет вид $(\pi(1), \ldots, \pi(n))$ 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. 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 $(i_1, \ldots, i_l)$ и $(j_1, \ldots, j_m)$ независимы, если $\{i_1, \ldots, i_l\} \cap \{j_1, \ldots, j_m\} = \varnothing$. Следующий результат, известный как **разложение на независимые циклы** (Zyklenzerlegung), несмотря на свою простоту лежит в основе всей теории групп перестановок.

Теорема. *Каждая перестановка может быть представлена как произведение попарно независимых истинных циклов. Такое представление единственно с точностью до перестановки сомножителей.*

Доказательство. Существование: пусть $X_1, \ldots, X_s$ 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 $\pi_1, \ldots, \pi_s$, независимы. Так как каждый элемент лежит в какой-то орбите, то $\pi = \pi_1 \ldots \pi_l$.

Единственность: пусть $\pi = \pi_1 \ldots \pi_l$ 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 $\pi = \pi_1 \ldots \pi_l$ есть разложение перестановки π на независимые циклы, то $o(\pi) = \mathrm{lcm}(o(\pi_1), \ldots, o(\pi_l))$.*

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 $\sigma(i) = j$. Продолжая действовать таким образом, мы 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).

§ 4. 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**[176] и сейчас мы совсем коротко напомним их определение.

1. Числа Стирлинга первого рода. Для этого 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 $\left[{n \atop m} \right]$, $m, n \in \mathbb{N}_0$. Таким образом, по определению

$$[x]^n = \sum_{m=0}^{n} \left[{n \atop m} \right] x^m.$$

[176] **Джеймс Стирлинг** (1692, St.Ninians – 05.12.1770, Leadhills) – шотландский математик, основные работы которого относятся к теории рядов, интерполяции и теории алгебраических кривых. Как приверженец Стюарт Стирлинг вынужден был эмигрировать и в 1714 – 1725 годах жил в Венеции. Позже он вернулся в Шотландию, где занимался горным делом.

Заменяя здесь x на $-x$ мы видим, что $[-x]_n = (-1)^n[x]^n$, так что

$$[x]_n = \sum_{m=0}^{n} (-1)^{n-m} \left[{n \atop m} \right] x^m.$$

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 $(-1)^{n-m}\left[{n \atop m} \right]$, который при этом обозначается через s_{nm} или $s(n,m)$. Классическое определение удобнее в том смысле, что при этом 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[177]. Кроме того, мы пользуемся пропагандируемым Кнутом обозначением Йована Карамата[178,179], достоинство которого состоит в том, что оно подчеркивает аналогию с биномиальными коэффициентами.

Числа Стирлинга первого рода можно определить граничными условиями $\left[{n \atop 0} \right] = \delta_{n0}$, $\left[{n \atop m} \right] = 0$ при $m > n$ и **треугольным рекуррентным соотношением** аналогичным тому, при помощи которого определяются биномиальные коэффициенты:

$$\left[{n \atop m} \right] = (n-1)\left[{n-1 \atop m} \right] + \left[{n-1 \atop m-1} \right].$$

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

[177]**Дональд Кнут** – выдающийся математик, программист и типограф. После окончания Калифорнийского Технологического Института Кнут нработает в Стенфордском университете, в настоящее время выдающимся профессором (distinguished professor). Его первые работы относятся к алгебре и теории чисел, до сих пор он время от времени публикует статьи, посвященные теории чисел, комбинаторике и математическим обозначениям. В начале 1960-х годов Кнут увлекся программированием. Как известно, именно алгебраисты становятся лучшими программистами, именно работы в этой области принесли Кнуту мировую известность. Уникальным явлением в мировой литературе стала серия книг под общим названием 'Искусство программирования'. Три первых тома этой книги имеются в русском переводе: Д.Кнут, Искусство программирования, т.I–III. – Вильямс, М.–СПб.–Киев, 2000, т.I. Основные алгоритмы. – с.1–712; т.II. Получисленные алгоритмы. – с.1–828; т.III. Сортировка и поиск. – с.1–822. 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. Д.Е.Кнут, Все про TEX. – АО RDTEX, Протвино, 1993, с.1–575. Всего Кнут является автором 19 книг, из которых еще некоторые переведены на русский язык, в том числе Р.Грехем, Д.Кнут, О.Паташник, Конкретная математика. – Мир, М., 1998, с.1–703. Из книг, пока не переведенных на русский язык, начинающему можно порекомендовать Surreal numbers, содержащую изложение теории сверхвещественных ('сюрреалистических') чисел Конвея.

[178]D.E.Knuth, Two notes on notation. – Amer. Math. Monthly, 1992, vol.99, p.403–422.

[179]A.E.Fekete, *Apropos* two notes on notation. – Amer. Math. Monthly, 1994, October, p.771–778.

Число Стирлинга $\left[\begin{smallmatrix} n \\ m \end{smallmatrix}\right]$ расположено здесь на пересечении n-й строки и m-го столбца, причем как нумерация строк, так и нумерация столбцов 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 $\left[\begin{smallmatrix} n \\ n \end{smallmatrix}\right] = 1$, а $\left[\begin{smallmatrix} n \\ 1 \end{smallmatrix}\right] = (n-1)!$.

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 $\left\{\begin{smallmatrix} n \\ m \end{smallmatrix}\right\}$, $m, n \in \mathbb{N}_0$. В большинстве классических книг по комбинаторике используется обозначение S_{nm} или $S(n,m)$. Таким образом, по определению

$$x^n = \sum_{m=0}^{n} \left\{\begin{smallmatrix} n \\ m \end{smallmatrix}\right\} [x]_m.$$

Как и выше, пользуясь тем, что $[-x]_n = (-1)^n [x]^n$, мы видим, что

$$x^n = \sum_{m=0}^{n} (-1)^{n-m} \left\{\begin{smallmatrix} n \\ m \end{smallmatrix}\right\} [x]^m.$$

По самому определению, имеют место формулы

$$\sum_i (-1)^{n-i} \left[\begin{smallmatrix} n \\ i \end{smallmatrix}\right] \left\{\begin{smallmatrix} i \\ m \end{smallmatrix}\right\} = \delta_{mn} = \sum_i (-1)^{n-i} \left\{\begin{smallmatrix} n \\ i \end{smallmatrix}\right\} \left[\begin{smallmatrix} i \\ m \end{smallmatrix}\right],$$

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 $\left\{\begin{smallmatrix} n \\ 0 \end{smallmatrix}\right\} = \delta_{n0}$, $\left\{\begin{smallmatrix} n \\ m \end{smallmatrix}\right\} = 0$ при $m > n$, что и числа Стирлинга первого рода, а **треугольное рекуррентное соотношение** для них принимает вид:

$$\left\{\begin{smallmatrix} n \\ m \end{smallmatrix}\right\} = m \left\{\begin{smallmatrix} n-1 \\ m \end{smallmatrix}\right\} + \left\{\begin{smallmatrix} n-1 \\ m-1 \end{smallmatrix}\right\}.$$

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 $\left[{n \atop m} \right]$.*

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 $x(n,m) = \left[{n \atop m} \right]$, 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:

Либо n образует для n отдельную орбиту. Убирая эту орбиту мы получаем перестановку $\sigma \in S_n$ с $m-1$ орбитой, так что количество таких перестановок равно $x(n-1,m-1)$.

Либо 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, $\left[{4 \atop 2} \right] = 11$, 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 $\left\{ {n \atop m} \right\}$ 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 $\left\{ {n \atop m} \right\} \leq \left[{n \atop m} \right]$. При этом в случае, когда имеется хотя бы одна трехэлементная орбита имеется более такой одной перестановки. Тем самым, как правило, $\left\{ {n \atop m} \right\} < \left[{n \atop m} \right]$.

§ 5. Классы сопряженности симметрической группы

В этом параграфе мы опишем классы сопряженности группы S_n.

1. Цикленный тип перестановки. Пусть $\pi \in S_n$ и $\underline{n}/\pi = \{X_1, \dots, X_t\}$. Обозначим через $n_i = |X_i|$ порядок орбиты X_i.

Определение. Цикленным типом *перестановки* $\pi \in S_n$ *называют набор* $[n_1, \dots, n_t]$ *порядков ее орбит.*

Обычно этот набор записывают как тупель $(n_1, \dots, n_t)$, 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 $(n_1, \dots, n_t)$ 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 $X_1, \dots, X_t$ – орбиты σ, то $\rho(X_1), \dots, \rho(X_t)$ – 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

$$\pi = (i_{11} \dots i_{1l}) \dots (i_{t1} \dots i_{tm}),$$

$$\sigma = (j_{11} \dots j_{1l}) \dots (j_{t1} \dots j_{tm}),$$

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 это 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**.

§ 6. Порождение симметрической группы 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*

$$S_n = \langle s_1, \dots, s_{n-1} \rangle.$$

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:

$$w_{ij} = s_i \dots s_{j-2} s_{j-1} s_{j-2} \dots s_i.$$

Теорема полностью доказана.

Задача. Докажите, что группа S_n порождается $n-1$ транспозицией (12), (13), ..., $(1n)$.

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 $(123\dots n)$.

Задача. Верно ли, что группа S_n порождается длинным циклом $(123\dots n)$ и *любой* транспозицией? Найдите необходимое и достаточное условие для того, чтобы S_n порождалось длинным циклом $(123\dots n)$ и транспозицией $(1m)$.

Решение. Так как группа $H = \langle (123\dots n), (1m)\rangle$ 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 $\{1, 1+d, \dots, n-d+1\}$, $\{2, 2+d, \dots, n-d+2\}$, ..., $\{d, 2d, \dots, n\}$. Ясно, что как $(123\dots n)$, 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[180], 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 $(23\dots n)$.

§ 7. 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**[181] перестановки σ.

[180] W.Johnson, M.Silver, A model for permutations, Amer. Math. Monthly, 1974, May, p.503–506.

[181] **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).

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* $X_1, \ldots, X_m$ *перестановки* σ.

Достоинством этого определения (см., например, Ленг [упражнение 9 на стр. 70]) является то, что, с одной стороны, легко доказать его совпадение с обычным определением в терминах транспозиций (к которому мы вернемся в следующем параграфе), 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* $\tau_1, \ldots, \tau_l$ – *транспозиции. Тогда* $\operatorname{sgn}(\tau_1 \ldots \tau_l) = (-1)^l$.

Доказательство. Индукция по l. Случай $l \leq 1$ очевиден. Для индукционного перехода достаточно показать, что знаки $\tau_2 \ldots \tau_l$ и $\tau_1 \ldots \tau_l$ **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

$$(pq)(pi_2 \ldots i_r)(qj_2 \ldots j_s) = (pi_2 \ldots i_r qj_2 \ldots j_s)$$

так что в этом случае две орбиты сливаются в одну.

Если p, q лежат в одной орбите, то

$$(pq)(pi_2 \ldots i_r qj_2 \ldots j_s) = (pi_2 \ldots i_r)(qj_2 \ldots j_s),$$

так что в этом случае одна орбита распадается на две.

Проанализировав приведенное выше 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 $m \geq 1$, то декремент принимает наибольшее значение на множестве длинных циклов: длинные циклы и только они требуют для своего выражения $n-1$ транспозиции.

§ 8. Знак перестановки
2nd 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 предыдущего параграфа и дадим другое определение знака.

Определение. *Положим* $\operatorname{sgn}(\sigma) = (-1)^l$, *если* σ *можно представить как произведение* l *транспозиций* $\sigma = \tau_1 \dots \tau_l$.

Как мы знаем, из предыдущего параграфа, 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 кратной индукции, сейчас мы проведем *еще одно* доказательство корректности, не зависящее от результатов предыдущего параграфа.

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 $\varphi = \text{sgn}$.

Следствие. *Знакопеременная группа A_n является единственной подгруппой индекса 2 в S_n, $n \geq 2$.*

§ 9. 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 $\text{inv}(\sigma)$ 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 пару $(\sigma(i), \sigma(j))$. Дональд Кнут[182] утверждает, что понятие инверсии ввел в 1750 году Г.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[183], когда они одновременно (и, наскольк-

[182] Д.Э.Кнут, Искусство программирования. Том 3. Сортировка и поиск, 2е изд., Вильямс, М.–СПб–Киев, 2000, 1–822.

[183] **Габриэль Крамер** (31.07.1704, Женева – 04.01.1752, Bagnols при Nismes) – известный 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.

ко 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 века до нашей эры.

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[184] это определение обладает одним 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,

$$(-1)^{\mathrm{inv}(\pi\sigma)} = \prod_{1\le i<j\le n} \frac{\pi\sigma(i)-\pi\sigma(j)}{i-j} = \prod_{1\le i<j\le n} \frac{\pi\sigma(i)-\pi\sigma(j)}{\sigma(i)-\sigma(j)} \prod_{1\le i<j\le n} \frac{\sigma(i)-\sigma(j)}{i-j} = (-1)^{\mathrm{inv}(\pi)}(-1)^{\mathrm{inv}(\sigma)}.$$

[184]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!

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.

§ 10. Знакопеременная группа

Знак позволяет нам определить важнейшую подгруппу в S_n.

1. Знакопеременная группа. Теперь мы в состоянии высказать самое сокровенное, что можно высказать об отображении групп.

Теорема. *Отображение* $\mathrm{sgn} : S_n \longrightarrow \{\pm 1\}$ *является гомоморфизмом.*

Доказательство. Если π можно представить как произведение l транспозиций, а σ можно представить как произведения m транспозиций, то, конкатенируя эти представления, мы выразим $\pi\sigma$ как произведение $l+m$ транспозиций. Таким образом, $\mathrm{sgn}(\pi\sigma) = (-1)^{l+m} = \mathrm{sgn}(\pi)\,\mathrm{sgn}(\sigma)$.

Назовем перестановку **четной**, если $\mathrm{sgn}(\sigma) = 1$, и **нечетной**, если $\mathrm{sgn}(\sigma) = -1$. 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). 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 $(ij)(hk)$ 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. Транзитивность

В настоящем параграфе мы совсем коротко обсудим свойства транзитивности групп перестановок. На русском языке дальнейшие детали и ссылки можно найти, например, в статье[185].

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, обозначим их общий порядок через m. Как мы убедились в предыдущей задаче, $|G| = mn$. Но, так как 1 принадлежит всем группам G_i, то $|G_1 \cup \dots \cup G_n| \leq n(m-1)+1 < |G|$. Это значит, что найдется перестановка $\pi \in G$, которая не принадлежит ни одной группе G_i.

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.

[185] П.Дж.Камерон, Конечные группы подстановок и конечные простые группы. – Успехи Мат. наук, 1983, т.38, N.3, с.135–157

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. 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 $4! = 24$, то 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.

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[186]**.** *При $n \geq 5$ группа S_n не содержит никаких подгрупп H таких, что $2 < |G : H| < n$. 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[187] основывалось на следующем предположении, которое он проверил для всех $n < 1500000$, но доказательством которого в общем случае он не владел.

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[188,189]. Однако тем временем Серре нашел доказательство теоремы Бертрана, не опирающееся на постулат Бертрана[190].

§ 12. 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 $x_1, \ldots, x_m \in X$ и любых попарно различных $y_1, \ldots, y_m \in X$ существует $\pi \in G$ такое, что $\pi(x_i) = y_i$ для всех $i = 1, \ldots, m$. Группа $G \leq S_n$ называется **кратно транзитивной**, если она m-транзитивна для какого-то $m \geq 2$.

---

[186] **Жозеф Бертран** (11.03.1822 – 03.04.1900, Париж) – известный французский математик, основные работы которого относятся к теории вероятностей и дифференциальной геометрии.

[187] 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, 1845, vol.30, p.123–140.

[188] P.L.Tschebycheff, Mémoire sur les nombres premiers. – J. Math. pures appl., 1852, vol.17, p.366–390.

[189] Сегодня постулат Бертрана обычно формулируется в чуть более слабой форме, как существование простого p между n и $2n$, причем обычно воспроизводится доказательство Эрдеша: P.Erdös, Beweis eines Satzes von Tschebyscheff. – Acta Reg. Univ. Hungar., 1932, Bd.5, S.194–198.

[190] 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, vol.15, p.1–44.

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[191] открыл пять совершенно удивительных групп M_{11}, M_{12}, M_{22}, M_{23}, M_{24}, обладающих высокой степенью транзитивности. Именно, группы M_{12} и M_{24} 5-кратно транзитивны. В действительности, это единственные 5-кратно транзитивные группы, кроме S_n и A_n.

$$\begin{aligned} M_{11} &\qquad 2^4 \cdot 3^2 \cdot 5 \cdot 11 = 7920, \\ M_{12} &\qquad 2^6 \cdot 3^3 \cdot 5 \cdot 11 = 95040, \\ M_{22} &\qquad 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 = 443520, \\ M_{23} &\qquad 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 10200960, \\ M_{24} &\qquad 2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23 = 244823040. \end{aligned}$$

Как проще всего убедиться в том, что группы Матье M_{12} и M_{24} не могут быть 6 транзитивными?

3. Кратная однородность. Подгруппа $G \leq S_n$ 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[192].

Теорема Ливингстона-Вагнера. *Если подгруппа $G \leq S_n$ является m-однородной для некоторого $m \leq n/2$, то она является и $m-1$-однородной.*

§ 13. Примитивность

1. Примитивные группы. Группа $G \leq S_n$ называется **импримитивной**, если множество $X = \underline{n}$ можно представить в виде $X = X_1 \sqcup \dots \sqcup X_t$, где $1 < t < n$, притом так, что каждый элемент $g \in G$ переставляет классы $X_1, \dots, X_t$ 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 $\{X_1, \dots, X_t\}$ называется **системой импримитивности** группы G, а сами классы $X_1, \dots, X_t$ – **блоками импримитивности**. В противном случае, когда такое разбиение

[191] **Эмиль Матье** ()

[192] D.Livingston, A.Wagner, Transitivity of finite permutation groups on unordered sets. – Math. Z., 1965, Bd. 90, S. 393–403.

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, bla-bla-bla.

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.

§ 14. Простота знакопеременной группы

> 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 уравнениея 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.

§ 15. 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[193].

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

[193] O.Hölder, Bildung zusammengesetzter Gruppen. – Math. Ann., 1895, Bd. 46, p.321–422.

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 $s_1, \dots, s_{n-1}$, то нам достаточно доказать существование такой перестановки $\pi \in S_n$, что

$$\varphi(s_1) = \pi s_1 \pi^{-1}, \dots, \varphi(s_{n-1}) = \pi s_{n-1} \pi^{-1}.$$

В действительности, технически несколько удобнее доказывать существование такого $\pi \in S_n$, что $I_\pi\varphi(s_h) = s_h$ для всех $h = 1, \dots, n-1$. 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 $I_\pi\varphi(s_1) = s_1, \dots, I_\pi\varphi(s_r) = s_r$ 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 несколько 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[194,195,196,197,198] 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:

$$\begin{aligned}
(12) &\mapsto (12)(35)(46),\\
(13) &\mapsto (13)(24)(56),\\
(14) &\mapsto (14)(25)(36),\\
(15) &\mapsto (15)(26)(34),\\
(16) &\mapsto (16)(23)(45)
\end{aligned}$$

и показывает, что действительно существует автоморфизм S_6 (по сравнению с работой[196] мы для большей симметрии переставили 5 и 6).

---

[194]H.A.Bender, A new method for the determination of the group of isomorphisms of the symmetric group of degree n. – Amer. Math. Monthly, 1924, vol.31, p.287–289.

[195]E.Witt, Die 5-transitiven Gruppen von Mathieu. – Abh. Math. Sem. Univ. Hamburg, 1938, Db. 12, S.256–264.

[196]D.W.Miller, On a theorem of Hölder. – Amer. Math. Monthly, 1958, vol.65, p.252–254.

[197]G.Janusz, J.J.Rotman, Outer automorphisms of S_6. – Amer. Math. Monthly, 1982, vol.89, p.407–410.

[198]T.A.Fournelle, Symmetries of the cube and outer automorphisms of S_6. – Amer. Math. Monthly, 1993, April, p.377–380.

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[199] 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[200]. Наша формула слегка отличается от формулы, приведенной в книгах [O'Meara] и [Isom], 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 $(e_1,e_3) = (e_2,e_4) = 1$.

§ 16. 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,

[199] T.Y.Lam, D.B.Leep, Combinatorial structure of the automorphisms of S_6. – Expositio Math., 1993.

[200] R.E.Solazzi, Four-dimensional symplectic groups. – J. Algebra, 1977, vol.49, N.1, p.225–237.

`Permutations[Range[n]]`

генерирует все элементы симметрической группы S_n степени n в лексикографическом порядке, в сокращенной записи.

`Reverse` – перестановка $\begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$.

`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[`$\{x_1,\dots,x_n\}$`]` генерирует перестановку с данным разложением на циклы.

`Inversions[`x`]` возвращает число инверсий перестановки x.

`Signature[`x`]` возвращает знак перестановки x.

Тема 6. ДЕЙСТВИЯ ГРУПП

Как уже неоднократно отмечалось, в подавляющем большинстве приложений группа возникает не как абстрактная группа, а как группа преобразований, т.е. как группа действующая на множестве. 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.

§ 1. Действие группы на множестве

В настоящем параграфе мы применим определения из § ? к случаю, когда $M = G$ является группой. Специфика групповых действия состоит в том, что элементы группы осуществляют *обратимые* преобразования множества X.

1. Действие группы на множестве. Так как любая группа является моноидом, все определения предыдущего параграфа сохраняют силу для случая, когда $M = G$ является группой. 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, $\theta_g\theta_{g^{-1}} = \theta_{gg^{-1}} = \theta_1 = \mathrm{id}_X$.

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.

3. Естественное действие симметрической группы. Следующий пример играет такую же роль для групповых действий, как действие моноида эндоморфизмов для действий моноидов. А именно, группа S_X действует на множестве X обычным образом, как $\pi x = \pi(x)$ для любого $\pi \in S_X$ и любого $x \in X$.

4. 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. 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, для правые действия G на X и взаимно однозначно соответствуют *антигомоморфизмами* G в S_X. Гомоморфизм G в симметрическую группу S_X часто называется также **перестановочным представлением** группы G на множестве X.

5. 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.

§ 2. Теорема Кэли

В этом параграфе мы покажем, что *каждая* группа может рассматриваться как подгруппа группы перестановок.

1. Теорема Кэли. В § ? мы рассматривали таблицу Кэли конечной квазигруппы G. При этом мы заметили, 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 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, $L_g(x) = gx$ (от английского 'left' – 'левый').

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 английского 'right' – 'правый').

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. ?, 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.

§ 3. Действие группы 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: $L_gR_h = R_hL_g$ для всех $h, g \in G$. В самом деле, $(L_gR_h)(x) = g(xh) = (gx)h = (R_hL_g)(x)$.

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, $G \times G \longrightarrow S_G$, $(h, g) \mapsto L_hR_{g^{-1}}$. Конечно, в общем случае это представление не является точным, так как, если $h = g \in C(G)$ – центральный элемент, то $L_gR_{g^{-1}} = \mathrm{id}_G$

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 $I_g = L_gR_{g^{-1}}$. 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 пермутационным 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, $(x)\sin$).

§ 4. 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:

$$C_{\mathrm{Hol}(G)}(L(G)) = R(G), \qquad C_{\mathrm{Hol}(G)}(R(G)) = L(G).$$

§ 5. 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 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.

§ 6. Произведение, копроизведение и расслоенное произведение G-множеств

?. Копроизведение G-множеств.

?. Прямое произведение G-множеств.

?. Действие на m-ках.

?. Расслоенное произведение G-множеств.

§ 7. 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.
$\mathrm{Map}(X,Y)^G = \mathrm{Map}_G(X,Y)$.

§ 8. Классификация транзитивных G-множеств

Задача (аргумент Фраттини). Пусть X – конечное G-множество, $H \leq G$ 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 $H\backslash G/H$.

§ 9. 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 трансзитивным**, 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. Аффинное пространство становится изоморфным векторному пространству **после того**, как в нем выбрано начало координат – ПРОРАБОТАТЬ!!

§ 10. Действие на смежных классах

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.

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?

§ 11. 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

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : \; z \mapsto \frac{az + b}{cz + d}.$$

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[201], что H можно мыслить себе как модель **плоскости Лобачевского**[202]. 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**[203]. 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 $\mathrm{im}\left(\dfrac{az + b}{cz + d}\right) > 0$.

2. Действие $\mathrm{PSL}(2, \mathbb{C})$ на трехмерном пространстве Лобачевского. Построить действие в этом случае чуть сложнее. А именно, рассмотрим следующую модель трехмерного

[201] Например, из рисунков Мориса Эшера.

[202] Буква H является первой буквой слова 'hyperbolic' – гиперболический, в англоязычной литературе геометрию Лобачевского принято называть гиперболической геометрией.

[203] 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.

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:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} : \; u + vi + wj \mapsto \frac{(a(u+vi)+b)\overline{(c(u+vi)+d)} + a\overline{c}w^2 + wj}{|c(u+vi)+d|^2 + |c|^2 t^2}.$$

Задача. Проверьте, что эта формула действительно определяет действие $\mathrm{PSL}(2, \mathbb{C})$ на H.

§ 12. 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, [Ha], 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. [Ha], упражнение 2.2 на стр. 385–386). Как мы узнаем в Главе 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

$$(x, y, z) \mapsto \left(\frac{y-1}{y-x}, \frac{1}{x}, \frac{z-1}{z-x} \right).$$

Одноэлементные орбиты возникают в золотом сечении и корнях 5-й степени из 1.

§ 13. 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 локашльный 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.

Тема 7. ЛИНЕЙНЫЕ ГРУППЫ

I believe in a heliocentric view of the Universe, with linear groups playing the role of the Sun

John Thompson

Чтение этой главы предполагает знакомство с основными понятиями, обсуждаемыми в книгах III и IV настоящего учебника, в первую очередь, с кольцами и (свободными) модулями, и некоторыми их простейшими свойствами, а также такими понятиями, как, скажем, гомоморфизм, идеал и фактор-кольцо. Кроме того, предполагается, что читатель легко умножает (блочные) матрицы.

1. Линейные группы

§ 1. Линейные группы

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, 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*: $u\mapsto gu$. 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 $v\in{}^nR$.

3. Проективная линейная группа. Пусть $A=\mathrm{Cent}(R)$ центр кольца R. Тогда матрица λe, $\lambda\in A^*$ называется **скалярной**.

Задача. Докажите, что центр $C(n,R)$ полной линейной группы $\mathrm{GL}(n,R)$ совпадает с множеством всех скалярных преобразований.

Указание. Для этого полезно знать достаточный запас обратимых матриц. Вернитесь к этой задаче после чтения § ?.

Класс матрицы $g\in\mathrm{GL}(n,R)$ в фактор-группе $\mathrm{GL}(n,R)/C(n,R)$ группы $\mathrm{GL}(n,R)$ по центру обычно обозначается через $[g]$. При этом в случае, когда в обозначении g использованы круглые скобки, в обозначении для $[g]$ они опускаются, так что вместо $[(g_{ij})]$ пишут просто $[g_{ij}]$. По определению, $[hg]=[h][g]$, $[g^{-1}]=[g]^{-1}$ и $[\lambda g]=[g]$ для любого $\lambda\in\mathrm{Cent}(R)$.

В случае, когда $R=K$ *поле*, фактор-группа $\mathrm{GL}(n,K)/C(n,K)$ обозначается $\mathrm{PGL}(n,K)$ и называется **проективной специальной линейной группой** степени n над K. Обозначение PGL является сокращением от `Projective General Linear Group`.

Предостережение. Некоторые наивные писатели, не знакомые с первыми группами когомологий, беззастенчиво называют $\mathrm{GL}(n,R)/C(n,R)$ проективной линейной группой и в случае колец, но это безнадежно неверно!!! В действительности, даже для коммутативных колец группа $\mathrm{PGL}(n,R)$, которую естественно понимать, как группу автоморфизмов проективного пространства, почти всегда заметно больше, чем просто фактор-группа $\mathrm{GL}(n,R)$ по центру!

Дело в том, что эпиморфизмы алгебраических групп как правило не сюръективны на точках.

4. Специальная линейная группа. Пусть снова R коммутативно. В этом случае в группе $\mathrm{GL}(n,R)$ можно выделить в терминах определителя исключительно важную группу

$$\mathrm{SL}(n,R)=\{x\in M(n,R)\mid \det(x)=1\}$$

состоящую из всех матриц с определителем 1. Группа $\mathrm{SL}(n,R)$ называется **специальной линейной группой** степени n над R. Обозначение SL является сокращением от `Special Linear Group`. В случае, когда $R=\mathbb{R}$ – поле вещественных чисел, группа $\mathrm{SL}(n,\mathbb{R})$ естественно истолковывается геометрически как подгруппа в $\mathrm{GL}(n,\mathbb{R})$, состоящая из преобразований, сохраняющих *ориентированный* объем.

Кроме $\mathrm{SL}(n,R)$ встречается, хотя и заметно реже, другие группы, определенные в терминах значений определителя, скажем

$$\mathrm{SL}^{\pm}(n,R)=\{x\in M(n,R)\mid \det(x)=\pm 1\}.$$

В случае $R=\mathbb{R}$ группа группа $\mathrm{SL}^{\pm}(n,\mathbb{R})$ истолковывается как подгруппа в $\mathrm{GL}(n,\mathbb{R})$, состоящая из преобразований, сохраняющих объем (но не ориентацию!). В этом случае часто рассматривается и группа

$$\mathrm{GL}^{+}(n,\mathbb{R})=\{x\in M(n,\mathbb{R})\mid \det(x)>0\}$$

линейных преобразований, сохраняющих ориентацию (но не объем!)

5. Проективная специальная линейная группа. Центр $\mathrm{SC}(n,R)$ специальной линейной группы $\mathrm{SL}(n,R)$ совпадает с пересечением $C(n,R)\cap\mathrm{SL}(n,R)$. Он состоит из всех скалярных матриц λe, где $\lambda\in R$ таково, что $\lambda^n=1$.

В случае, когда $R=K$ – поле, фактор-группа $\mathrm{SL}(n,K)/\mathrm{SC}(n,K)$ часто обозначается через $\mathrm{PSL}(n,K)$ и называется **проективной специальной линейной группой**. Обозначение PSL является сокращением от `Projective Special Linear Group`.

Предостережение. Все, что сказано выше о проективное полной линейной группе с еще большим драматизмом применимо к проективной специальной линейной группе. В действительности, группа $\mathrm{SL}(n,K)/\mathrm{SC}(n,K)$ как правило не совпадает с настоящей $\mathrm{PSL}(n,K)$ уже для случая поля!

§ 2. Линейные группы над конечным полем

1. Линейные группы над конечными полями. Если $q=p^m$, $p\in\mathbb{P}$, примарное число, то существует единственное конечное поле $K=\mathbb{F}_q$ из q элементов. Мы используем обычные сокращения $\mathrm{GL}(n,K)=\mathrm{GL}(n,q)$, $C(n,K)=C(n,q)$, $\mathrm{PGL}(n,K)=\mathrm{PGL}(n,q)$, $\mathrm{SL}(n,K)=\mathrm{SL}(n,q)$, etc.

Теорема. *Порядок полной линейной группы* $\mathrm{GL}(n,q)$ *степени* n *над полем* $\mathbb{F}_q$ *равен*

$$|\mathrm{GL}(n,q)|=(q^n-1)(q^n-q)\dots(q^n-q^{n-1}).$$

Доказательство. В книге V мы обсуждаем основной принцип линейной алгебры над полем, состоящий в том, что *любой* подмодуль свободного модуля дополняем, так что, в частности, любой линейно независимый список векторов может быть дополнен до базиса.

★ В частности, над полем любой ненулевой столбец может быть первым столбцом обратимой матрицы. Над конечным полем $\mathbb{F}_1$ имеется q^n-1 возможностей выбрать ненулевой столбец высоты n.

★ Аналогично, вторым столбцом обратимой матрицы над полем может быть любой столбец, линейно независимый от первого, т.е. любой столбец не лежащий на фиксированной прямой. Таким образом, *независимо от выбора первого столбца* над $\mathbb{F}_q$ имеется q^n-q возможностей выбрать второй столбец.

★ Точно так же, третьим столбцом обратимой матрицы над полем может быть любой столбец, линейно независимый от первого и второго, т.е. любой столбец не лежащий на фиксированной плоскости. Таким образом, *независимо от выбора первого и второго столбцов* над $\mathbb{F}_q$ имеется q^n-q^2 возможностей выбрать третий столбец.

Продолжая действовать таким образом, мы в конце концов убедимся, что *независимо от выбора первых* $n-1$ *столбцов* над $\mathbb{F}_q$ имеется q^n-q^{n-1} возможностей выбрать последний столбец обратимой матрицы. Это и дает требуемую формулу.

Часто эту формулу удобнее записывать в виде

$$|\operatorname{GL}(n,q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\dots(q-1).$$

Дело в том, что если $q=p^m$ есть степень простого числа p, то $q^{n(n-1)/2}$ является в этом случае степенью p, делящей $|\operatorname{GL}(n,q)|$, в то время как остальные множители взаимно просты с p.

Следствие 1. *Порядок полной линейной группы* $\operatorname{SL}(n,q)$ *степени* n *над полем* $\mathbb{F}_q$ *равен*

$$|\operatorname{SL}(n,q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\dots(q^2-1).$$

Следствие 2. *Порядок проективной линейной группы* $\operatorname{PGL}(n,q)$ *степени* n *над полем* $\mathbb{F}_q$ *равен*

$$|\operatorname{PGL}(n,q)| = q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\dots(q^2-1).$$

Следствие 3. *Порядок проективной специальной линейной группы* $\operatorname{PSL}(n,q)$ *степени* n *над полем* $\mathbb{F}_q$ *равен*

$$|\operatorname{PSL}(n,q)| = \frac{q^{n(n-1)/2}(q^n-1)(q^{n-1}-1)\dots(q^2-1)}{\gcd(n,q-1)}.$$

Задача.

§ 2. Исключительные изоморфизмы

Перечислим открытые Жорданом и Диксоном исключительные изоморфизмы меджу группами $\mathrm{PSL}(n,q)$, S_m и A_m.

• $\mathrm{PSL}(2,2) \cong S_3$ – неабелева группа порядка 6 (напомним, что $\mathrm{PSL}(n,2) = \mathrm{SL}(n,2) = \mathrm{GL}(n,2)$);

• $\mathrm{PSL}(2,3) \cong A_4$ – неабелева группа порядка 12;

• $\mathrm{PSL}(2,4) \cong \mathrm{PSL}(2,5) \cong A_5$ простая группа порядка 60;

• $\mathrm{PSL}(2,7) = \mathrm{PSL}(3,2)$ – простая группа порядка 168 (**группа Валентинера**);

• $\mathrm{PSL}(2,9) \cong A_6$ – простая группа порядка 360;

• $\mathrm{PSL}(4,2) \cong A_8$ – простая группа порядка 20160.

Описанные здесь исключительные группы $\mathrm{PSL}(2,2)$, $\mathrm{PSL}(2,3)$, $\mathrm{PSL}(2,3)$, $\mathrm{PSL}(2,5)$, $\mathrm{PSL}(2,7)$, $\mathrm{PSL}(2,7)$, $\mathrm{PSL}(3,2)$ $\mathrm{PSL}(4,2)$, Естественно возникает вопрос, существуют ли другие исключительные изоморфизмы?

Теорема. *Никаких других изоморфзмов между группами* $\mathrm{PSL}(n,q)$*, или этими группами и группами* S_m*,* A_m *нет.*

§ 3. Некоторые важнейшие подгруппы

Опишем некоторые важнейшие подгруппы, которые задаются особенно простыми уравнениями на коэффициенты входящих в них матриц.

• **Группа диагональных матриц.** Пусть $D = D(n,R)$ группа **диагональных матриц**, состоящая из всех матриц $x = (x_{ij}) \in G$ таких, что $x_{ij} = 0$ для всех $i \neq j$.

• **Группа верхних треугольных матриц.** Обозначим через $B = B(n,R)$ группу **верхних треугольных матриц**, состоящую из всех матриц $x = (x_{ij}) \in G$ таких, что $x_{ij} = 0 = x'_{ij}$ для всех $i > j$.

• **Группа нижних треугольных матриц.** Совершенно аналогично $B^- = B^-(n,R)$ обозначает группу **верхних треугольных матриц**, состоящую из всех матриц $x = (x_{ij}) \in G$ таких, что $x_{ij} = 0 = x'_{ij}$ для всех $i < j$.

Предостережение. Во многих книгах $B(n,R)$ определяются как группа обратимых матриц таких, что $x_{ij} = 0$, для всех $i > j$. Это *грубейшая* ошибка! Дело в том, что над некоммутативными кольцами существуют обратимые верхние треугольные матрицы, обратные к которым не являются верхними треугольными. Более того, над кольцами без свойства IBN, которые мы обсуждаем в книге IV, существуют даже такие обратимые верхние треугольные матрицы, обратные к которым являются нижними треугольными!

• **Группа верхних унитреугольных матриц.** Пусть $U = U(n,R)$ обозначает группу **верхних унитреугольных матриц** т.е. подгруппу в B, состоящую из **унипотентных** матриц. Иными словами, U состоит из всех матриц $x = (x_{ij})$ таких, что $x_{ij} = 0$ для всех $i > j$ и $x_{ii} = 1$ для всех i.

• **Группа нижних унитреугольных матриц.** Совершенно аналогично определяется и группа $U^- = U^-(n,R)$ **нижних унитреугольных матриц**, т.е. подгруппа а B^-, состоящая из всех матриц $x = (x_{ij})$ таких, что $x_{ij} = 0$ для всех $i < j$ и $x_{ii} = 1$ для всех i.

• **Мономиальная подгруппа.** Пусть $N = N(n, R)$ **мономиальная подгруппа**, состоящая из всех **мономиальных матриц**, т.е. матриц $x = (x_{ij}) \in G$ в каждой строке и каждом столбце которых ровно один ненулевой элемент (который в этом случае обязан быть обратимым). Иными словами, для любого i существует единственное j такое, что $x_{ij} \neq 0$ и наоборот.

Стандартные обозначения подгрупп. Мнемонически 'B' обозначает `Borel subgroup`, 'D' обозначает `Diagonal`, 'N' обозначает `torus Normalizer` и 'W' обозначает `Weyl group`. С точки зрения теории алгебраических групп D представляет собой *расщепимый максимальный тор* в G.

Пусть временно R обоазначает любое ассоциативное кольцо с 1 и $G = \mathrm{GL}(n, R)$ – полная линейая группа степени n над R. Ясно, что D нормальна в N и фактор-группа $W = N/D$ изоморфна $\S_n$, симметрической группе на n символах.

Группа B является полупрямым произведением нормальной подгруппы U и дополнительной подгруппы D.

соответствующие подгруппы в $\mathrm{SL}(n, R)$.

§ 4. Блочные подгруппы

1. Разбиение. Пусть $\nu = (n_1, \dots, n_t)$ **разбиение** n, т.е. $n = n_1 + \ldots + n_t$. Это разбитие определяет отношение эквивалентности $i \sim_\pi j$ (или просто $i \sim j$) на множестве индексов $I = \{1, \dots, n\}$, а именно, $i \sim_\pi j$ если и только если

$$n_1 + \ldots + n_{h-1} + 1 \leq i, j \leq n_1 + \ldots + n_h$$

для некоторого h, $1 \leq h \leq t$. Пусть $I_1, \dots, I_t$ – классы эквивалентности $\sim$, мощностей $n_1, \dots, n_t$, соответственно. Тогда $I = I_1 \sqcup \ldots \sqcup I_t$.

С ν можно связать несколько подгрупп в полной линейной группе $\mathrm{GL}(n, R)$ над произвольным кольцом R.

• **Группа элементарных блочно-диагональных матриц.** Едва ли не самая важная группа, связанная с разбиением ν, это группа $E(\nu, R)$ **элементарных блочно-диагональных матриц** типа ν. Она порождена всеми элементарными трансвекциями $t_{ij}(\xi)$ для $i \sim j$:

$$E(\nu, R) = \langle t_{ij}(\xi), 1 \leq i \neq j \leq n, i \sim j, \xi \in R \rangle .$$

Ясно, что

$$E(\nu, R) = E(n_1, R) \oplus \ldots \oplus E(n_t, R).$$

• **Группа блочно-диагональных матриц.** Далее, $D(\nu, R)$ обоазначает **группу блочно-диагональных матриц** типа ν. Она состоит из всех матриц $x = (x_{ij})$ таких, что $x_{ij} = 0$ если i не эквивалентно j:

$$D(\nu, R) = \{x = (x_{ij}) \in \mathrm{GL}(n, R) \mid x_{ij} = 0 \ \text{ for } \ i \not\sim j\} .$$

Ясно, что

$$D(\nu, R) = \mathrm{GL}(n_1, R) \oplus \ldots \oplus \mathrm{GL}(n_t, R).$$

• **Группа верхних блочно-треугольных матриц.** Можно рассмотреть также группу $B(\nu, R)$ **верхних клеточно-треугольных матриц** типа ν, которая состоит из всех матриц $x = (x_{ij})$ таких, что элементы x_{ij} и x'_{ij} равны 0 для всех $i > j$ таких, что i не эквивалентно j:

$$B(\nu, R) = \{x = (x_{ij}) \in \mathrm{GL}(n, R) \mid x_{ij} = 0 = x'_{ij} \quad \text{для} \quad i > j, i \sim j\}.$$

• **Группа нижних блочно-треугольных матриц.** Совершенно аналогично определяется также группа $B^-(\nu, R)$ **нижних клеточно-треугольных матриц** типа ν, которая состоит из всех матриц $x = (x_{ij})$ таких, элементы x_{ij} и x'_{ij} равны 0 для всех $i < j$ таких, что i не эквивалентно j:

$$B^-(\nu, R) = \{x = (x_{ij}) \in \mathrm{GL}(n, R) \mid x_{ij} = 0 = x'_{ij} \quad \text{для} \quad i < j, i \sim j\}.$$

Предостережение. Как и в случае группы верхних треугольных матриц условие на элементы обратной матрицы здесь совершенно необходимо. В общем случае легко построить матрицы, для которых $x_{ij} = 0$, но $x'_{ij} \neq 0$.

• **Группа блочно-мономиальных матриц.** Можно определить группу $N(\nu, R)$ of **клеточно-мономиальных матриц** ν. Эта группа особенно важна для случая, когда $\nu = (m, \dots, m)$ является разбиением на равные слагаемые. В этом случае $N(\nu, R)$ изоморфна сплетению группы $\mathrm{GL}(m, R)$ и симметрической группы $\mathrm{S}_{n/m}$.

Рассмотренные нами в предыдущем параграфе группы $B(n, R)$, $D(n, R)$ и $N(n, R)$ являются частным случаем групп $B(\nu, R)$, $D(\nu, R)$ и $N(\nu, R)$, который получается для разбиения $\nu = (1, \dots, 1)$.

Почему здесь необходимы условия на x'_{ij}!!!

§ 5. Элементарные трансвекции

1. Элементарные трансвекции. Сейчас мы опишем наиболее важный класс элементов в $\mathrm{GL}(n, R)$. **Элементарная трансвекция** называется матрица $t_{ij}(\xi)$ вида $t_{ij}(\xi) = e + \xi e_{ij}$, $\xi \in R$, $1 \leq i \neq j \leq n$. Умножение матрицы x на $t_{ij}(\xi)$ слева имеет следующий эффект: при этом j-я строка x умножается на ξ слева и прибавляется к i-й строке x. В свою очередь, умножение матрицы x на $t_{ij}(\xi)$ справа прибавляет к i-му столбец матрицы x, умноженный на ξ справа к j-му столбцу матрицы x. Это показывает, что элементарные трансвекции это в точности 'элементарные преобразования первого типа', которые появляются в книге, посвященной линейной алгебре.

2. Элементарная группа. Сейчас мы определим важнейшую подгруппу в $\mathrm{GL}(n, R)$. С одной стороны, эта группа явно задана в терминах самых простых мыслимых образующих. С другой стороны, как мы в дальнейшем убедимся, она, как правило, весьма близка к $\mathrm{GL}(n, R)$. Подгруппа полной линейной группы $G = \mathrm{GL}(n, R)$, порожденная всеми элементарными трансвекциями $t_{ij}(\xi)$, называется **элементарной подгруппой** и обозначается $E = E(n, R)$. Таким образом, по определению

$$E(n, R) = \langle t_{ij}(\xi),\ \xi \in R,\ 1 \leq i \neq j \leq n \rangle.$$

Пусть кольцо R коммутативно. Тогда определитель всех трансвекций равен 1. Поэтому, в общем случае нельзя ожидать, что $E(n, R) = GL(n, R)$.

Теорема. *Пусть $R = K$ – поле, $E(n, K) = \mathrm{SL}(n, K)$.*

§ 6. Псевдоотражения

1. Элементарные псевдоотражения. Для обратимого $\varepsilon \in R^*$ можно определить **элементарное псевдоотражение** $d_i(\varepsilon) = e + (\varepsilon - 1)e_{ii}$, $1 \le i \le n$ (здесь d является сокращением от `diagonal` – или `dilation`, точно так же, как в предыдущем параграфе t было сокращением от `transvection`). Умножение матрицы x на $d_i(\varepsilon)$ слева умножает i-ю строку матрицы x на ε слева, в то время как умножение на $d_i(\varepsilon)$ справа умножает i-й столбец матрицы x на ε справа. Это значит, что элементарные псевдоотражения – это в точности 'элементарные преобразования второго типа', которые появляются в книге, посвященной линейной алгебре.

2. Полная элементарная группа. Сейчас мы подправим определение элементарной группы, с тем, чтобы получить группу, которая еще ближе к $\mathrm{GL}(n, R)$. Что мешало $E(n, R)$ совпадать с $\mathrm{GL}(n, R)$? Дело в том, что все элементарные трансвекции имели определитель 1, так что мы заведомо получали подгруппу, содержащуюся в $\mathrm{SL}(n, R)$. Таким образом, нам нужно добавить еще матрицы со всевозможными определителями.

Рассмотрим группу $\mathrm{GE}(n, R)$ порожденную всеми элементарными трансвекциями u элементарными псевдоотражениями

$$\mathrm{GE}(n, R) = \langle t_{ij}(\xi),\ d_i(\varepsilon),\ \xi \in R,\ \varepsilon \in R^*,\ 1 \le i \ne j \le n \rangle.$$

Получающаяся таким образом группа $\mathrm{GE}(n, R)$ называется **полной элементарной группой**. Ее смысл состоит в том, что, с одной стороны, она задана очень простыми образующими, вычислять в которых очень легко, а, с другой стороны, она, как правило, она очень близка к $\mathrm{GL}(n, R)$. В качестве подтверждения этой мысли приведем следующий результат.

Теорема. *Если $R = K$ поле, то* $\mathrm{GE}(n, K) = \mathrm{GL}(n, K)$.

§ 7. Матрицы перестановки

Традиционно рассматриваются также '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 $1 \le i \ne j \le n$. Конечно, эти матрицы легко выражаются в терминах элементарных трансвекций и **элементарных отражений** $d_i(-1)$, $1 \le i \le n$.

Подгруппа в G, порожденная всеми w_{ij} обозначается через $W = W_n$ и называется группой **матриц перестановки**. 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 $\pi \in \mathrm{S}_n$ обозначим через (π) матрицу перестановки, элемент которой в позиции (i, j) равен $\delta_{i,\pi(j)}$.

Задача. Докажите, что отображение $\mathrm{S}_n \longrightarrow W_n$, $\pi \mapsto (\pi)$ является изоморфизмом. Выведите отсюда, что для матрицы перестановки обратная совпадает с транспонированной.

§ 8. Одномерные преобразования

Элементарные преобразования зависят от выбора базиса в свободном правом R-модуле R^n. Более геометрически настроенные индивидуумы обычно предпочитают работать с инвариантными понятиями, не зависящими от выбора базиса. Здесь мы вводим более широкий класс преобразований, который уже не зависит от выбора базиса и действительно играет центральную роль в *геометрическом* изучении линейных групп – точно такую же, как элементарные преобразования для алгоритмических аспектов этой теории.

1. Одномерные преобразования. Самые простые – и, *тем самым*, самые важные – элементы полной линейной группы $\mathrm{GL}(n, R)$ это, конечно, *одномерные* элементы. Самая общая форма одномерных преобразований такова: это $x_{ca}(\xi) = e + c\xi a$, где $c = (c_1, \dots, c_n)^t$ – столбец высоты n, $\xi \in R$, а $a = (a_1, \dots, a_n)$ – строка длины n.

Комментарий. Многие авторы предпочитают использовать бескоординатную нотацию. В этом случае они называют c вектором, а a – линейным функционалом. Используемые нами символы c и a являются реликтом традиционной геометрической терминологии. А именно, одномерное подпространство, в R^n порожденное c, называется **центром** (`centre`) преобразования $x_{ca}(\xi)$, в то время как гиперплоскость в R^n, ортогональная к a, называется (**осью**) `axis` преобразования $x_{ca}(\xi)$.

Положим $ac = a_1c_1 + \dots + a_nc_n = \delta$. Если $\delta = 0$, то преобразование $x_{ca}(\xi)$, $\xi \in R$, называется **трансвекцией**. Если $\delta \neq 0$, то, быть может после замены ξ, мы всегда можем считать, что $ac = \delta = 1$. В этом случае, чтобы гарантировать обратимость $x_{ca}(\xi)$, достаточно требовать $\xi \in 1 + R^*$. В этом случае преобразования $x_{ca}(\xi)$, $\xi \in 1 + R^*$, называются **дилациями** или **псевдоотражениями**.

Сейчас мы поймем, в чем состоит *решающее* техническое преимущество работы с одномерными преобразованиями, а не с элементарными преобразованиями. Дело в том, что он состоит целиком из классов сопряженных элементов этой группы.

Задача. Убедитесь, что

$$gx_{uv}(\xi)g^{-1} = x_{gu,vg^{-1}}(\xi), \quad g \in \mathrm{GL}(n, R),$$

Это равенство как раз и показывает, что класс одномерных преобразований замкнут относительно сопряжений при помощи произвольного элемента g группы $\mathrm{GL}(n, R)$.

Трансвекции аддитивны по отношению ко всем своим аргументам, в тех случаях, когда они определены.

Задача. Пусть строки $a = (a_1, \dots, a_n), d = (d_1, \dots, d_n) \in {}^nR$ и столбцы $b = (b_1, \dots, b_n)^T, c = (c_1, \dots, c_n)^T \in R^n$ подчинены условию $ab = ac = bd = 0$. Тогда

$$x_{b+c,a}(\xi) = x_{ba}(\xi)x_{ca}(\xi), \qquad x_{b,a+d}(\xi) = x_{ba}(\xi)x_{bd}(\xi).$$

Решение. Проверим первое из этих равенств. В самом деле, так как $ac = 0$, то

$$x_{b+c,a}(\xi) = e + (b + c)\xi a = (e + b\xi a)(e + c\xi a) = x_{ba}(\xi)x_{ca}(\xi).$$

Аналогичное равенство с заменой строк на столбцы проверяется совершенно аналогично.

2. Элементарные трансвекции versus трансвекций. Как связаны трансвекции и элементарные трансвекции? В обозначениях настоящего параграфа элементарную трансвекцию $t_{ij}(\xi)$ новых обозначениях переписать в виде $x_{e_i,f_j}(\xi)$. Таким образом, элементарная трансвекция – и, значит, все сопряженные с ней матрицы – являются трансвекцией в смысле нашего нового определения.

Естественно возникает вопрос, верно ли обратное, т.е. всякая ли трансвекция сопряжена с элементарной трансвекцией?

Задача. Докажите, что если $R = T$ является телом, то каждая трансвекция $x = x_{ca}(\xi)$ сопряжена с элементарной трансвекцией.

Решение. Если $a = 0$ или $c = 0$, то доказывать нечего, пусть поэтому $a \neq 0$ и $c \neq 0$, тогда ядро a, рассматриваемого как линейный функционал на T^n равно $L = \{b \in T^n \mid ab = 0\}$, причем $c \in L$. Выберем c в качестве первого вектора u_1 базиса пространства L, пусть $u_2, \dots, u_{n-1}$ – дополнение u_1 до базиса L, а $u_n \in T^n$ – любой вектор такой, что $au_n = 1$. Тогда x сопряжена с $t_{1n}(\xi)$.

Однако следующее очевидное соображение показывает, что в общем случае это совершенно не так! А именно, из последней задачи предыдущего пункта сразу следует, что для любых трех попарно различных индексов i, j, k матрица $x = t_{ij}(\xi)t_{ik}(\zeta)$ является трансвекцией. Однако эта матрица крайне редко сопряжена с элементарной трансвекцией. В самом деле, для того, чтобы x была сопряжена с $t_{12}(\theta)$, $\theta \in R$, по крайней мере *необходимо*, чтобы ξ и ζ порождали главный правый идеал (так как θ должен порождать тот же самый идеал, который порождают ξ и ζ). Обозначим через $T(n, R)$ подгруппу в $\mathrm{GL}(n, R)$, порожденную всеми трансвекциями $x_{uv}(\xi)$, $u \in R^n$, $v \in {}^nR$, $\xi \in R$, $vu = 0$. Группа $T(n, R)$ называется **группой трансвекций** в $\mathrm{GL}(n, R)$. В действительности в некоторых случаях группа $T(n, R)$ может быть *строго больше*, чем $E(n, R)$.

§ 9. Соотношения между элементарными трансвекциями

Как упомянуто в §§ 3 и 4, для случая поля группа $\mathrm{SL}(n, K)$ порождена всеми элементарными трансвекциями, в то время как группа $\mathrm{GL}(n, K)$ порождена элементарными трансвекциями и псевдоотражениями. Эти факты известны более двух тысяч лет и лежат в основе китайского метода решения систем линейных уравнений над полем, известного в Европе как **метод Гаусса**. Однако нам кажется, что даже в случае поля *соотношения* между этими образующими не были поняты до 1962 года!

1. Соотношения Стейнберга. Рассмотрим группу $\mathrm{GL}(n, R)$. Каковы очевидные соотношения между элементарными трансвекциями $t_{ij}(\xi)$, $\xi \in R$, $1 \leq i \neq j \leq n$? Прежде всего, он аддитивны по отношению к ξ, т.е.

$$t_{ij}(\xi)t_{ij}(\zeta) = t_{ij}(\xi + \zeta) \tag{R1}$$

для всех $\xi, \zeta \in R$.

2. Коммутационная формула Шевалле. Самое замечательное соотноше-

ние между трансвекциями – это следующее коммутационное соотношение

$$[t_{ij}(\xi), t_{hl}(\zeta)] = \begin{cases} e, & \text{if } j \neq h,\ i \neq l; \\ t_{il}(\xi\zeta), & \text{if } j = h,\ i \neq l; \\ t_{hj}(-\zeta\xi), & \text{if } j \neq h,\ i = l; \end{cases} \tag{R2}$$

являющееся специальным случаем **коммутационной формулы Шевалле** для корневых унипотентов в группе Шевалле (см. [Ca], [Sb2]). Обратите внимание, что случай $j = h$, $i = l$ здесь исключен. Дело в том, что никакого более простого выражения для коммутатора $[t_{ij}(\xi), t_{ji}(\zeta)]$ в терминах элементарных трансвекций нет!

§ 10. Корневые полупростые элементы

?. Элементы $w_{ij}(\varepsilon)$ и $d_{ij}(\varepsilon)$. Чтобы фактически задать группу $\mathrm{SL}(n, K)$ образующими и соотношениями, необходимы некоторые дополнительные соотношения, которые естественнее всего выражаются в терминах элементов $w_{ij}(\varepsilon)$ и $d_{ij}(\varepsilon)$, где $\varepsilon \in R^*$ и $1 \leq i \neq j \leq$n. А именно, положим

$$w_{ij}(\varepsilon) = t_{ij}(\varepsilon)t_{ji}(-\varepsilon^{-1})t_{ij}(\varepsilon) \tag{R3}$$

и

$$d_{ij}(\varepsilon) = w_{ij}(\varepsilon)w_{ij}(-1). \tag{R4}$$

Например, в случае $n = 2$ имеем

$$w_{12}(\varepsilon) = \begin{pmatrix} 0 & \varepsilon \\ -\varepsilon^{-1} & 0 \end{pmatrix}, \qquad d_{12}(\varepsilon) = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}.$$

Обратите внимание, что $d_{ij}(\varepsilon) = d_i(\varepsilon)d_j(\varepsilon^{-1})$ и что $w_{ij}(1)$ отличается от элемента w_{ij}, определенного в §1 знаком одного коэффициента! Это сделано для того, чтобы определитель $w_{ij}(1)$ равнялся 1, т.е., чтобы этот лемент попал в $\mathrm{SL}(n, R)$.

?. Соотношение в GL_2. В случае $n = 2$ коммутационная формула Шевалле не накладывает никаких соотношений на элементарные трансвекции. Однако в этом случае легко проверить выполнение следующего соотношения

$$w_{ij}(\varepsilon)t_{ij}(\xi)w_{ij}(-\varepsilon) = t_{ji}(-\varepsilon^{-1}\xi\varepsilon^{-1}) \tag{R5}$$

которое имеет смысл также и для $n = 2$

Перечисленные выше соотношения между $t_{ij}(\xi)$ называются **элементарными соотношениями** или **соотношениями Стейнберга**. Вообще говоря, они не образуют определяющей системы соотношений для группы $E(n, R)$, однако они дают весьма удачное приближение к такой системе соотношений. В действительности, чтобы задать группу $E(n, K) = \mathrm{SL}(n, K)$ в случае поля, к этой системе соотношений достаточно добавить единственный дополнительный тип соотношений – мультипликативность $d_{ij}(\varepsilon)$ in ε:

$$d_{ij}(\varepsilon)d_{ij}(\eta) = d_{ij}(\varepsilon\eta). \tag{R6}$$

§ 11. Гомоморфизм редукции, конгруэнц-подгруппы

В этом параграфе мы связываем с каждым идеалом R нормальные подгруппы в полной линейной группе $\mathrm{GL}(n,R)$.

1. Главная конгруэнц-подгруппа. Пусть I – идеал кольца R. Рассмотрим каноническую проекцию $\rho_I : R \longrightarrow R/I$, посылающую элемент $\lambda \in R$ в элемент $\overline{\lambda} = \lambda \pmod I = \lambda + I$. Эта проекция определяет **гомоморфизм редукции**

$$\rho_I : \mathrm{GL}(n,R) \longrightarrow \mathrm{GL}(n,R/I),$$

(**редукция по модулю** I) такой, что образ матрицы $x = (x_{ij})$ равен $\overline{x} = (\overline{x}_{ij})$. Стоит упомянуть, что ρ_I не обязательно сюръективен (скажем, $\rho_I : R^* \longrightarrow (R/I)^*$ вообще говоря, *не* сюръективен). Ядро гомоморфизма редукции ρ_I называется **главной конгруэнц-подгруппой** в $\mathrm{GL}(n,R)$ уровня I и обозначается $\mathrm{GL}(n,R,I)$. По определению

$$1 \longrightarrow \mathrm{GL}(n,R,I) \longrightarrow \mathrm{GL}(n,R) \longrightarrow \mathrm{GL}(n,R/I).$$

Две матрицы $x = (x_{ij})$ и $y = (y_{ij})$ называются **сравнимыми по модулю** I, если $x_{ij} \equiv y_{ij} \pmod I$ для всех $1 \leq i,j \leq n$. Как и для скаляров, сравнимость по модулю I обозначается через $x \equiv y \pmod I$. Главная конгруэнц-подгруппа $\mathrm{GL}(n,R,I)$ состоит из всех матриц $x \in GL(n,R)$ сравнимых с e по модулю I:

$$\mathrm{GL}(n,R,I) = \{x \in \mathrm{GL}(n,R) \mid x \equiv e \pmod I\}.$$

Так как ядро *любого* гомоморфизма является нормальной подгруппой, это показывает, что в группе $\mathrm{GL}(n,R)$ может быть довольно много нормальных подгрупп, по крайней мере, если в кольце R много идеалов.

2. Полная конгруэнц-подгруппа. С каждым идеалом связана еще одна естественная нормальная подгруппа в $\mathrm{GL}(n,R)$. А именно, рассмотрим центр $C(n,R/I)$ группы $\mathrm{GL}(n,R/I)$. Тогда полный прообраз группы $C(n,R/I)$ относительно гомоморфизма редукции ρ_I обозначается через $C(n,R,I)$ и называется **полной конгруэнц-подгруппой** уровня I:

$$C(n,R,I) = \rho_I^{-1}(C(n,R/I)).$$

Так как $C(n,R)$ является ядром канонической проекции $\pi_R : \mathrm{GL}(n,R) \longrightarrow \mathrm{PGL}(n,R)$, это значит, что $C(n,R,I)$ является ядром $\pi_{R/I} \circ \rho_I$:

$$1 \longrightarrow C(n,R,I) \longrightarrow \mathrm{GL}(n,R) \longrightarrow \mathrm{PGL}(n,R/I).$$

Тем самым, $C(n,R,I)$ тоже является нормальной подгруппой в $\mathrm{GL}(n,R)$.

Комментарий. Обратите внимание, что в одном важном аспекте использование обозначения $C(n,R,I)$ отличается от $\mathrm{GL}(n,R,I)$! А именно, группа $C(n,R)$ совпадает с $C(n,R,0)$, а не с $C(n,R,R)$, как можно было бы ожидать, зная, что $\mathrm{GL}(n,R,R)$ совпадает с $\mathrm{GL}(n,R)$. Мы надеемся, что это не вызовет никаких серьезных недоразумений. Хайман Басс обозначал группу $C(n,R,I)$ через $\mathrm{GL}'(n,R,I)$, в то время как в книге Хана и О'Миры используется обозначение $\mathrm{GL}\tilde{}(n,R,I)$. Однако обозначение $C(n,R,I)$ является общепринятым в русской литературе и кажется нам более суггестивным.

По определению

$$C(n,R,I)=\{x\in \mathrm{GL}(n,R)\mid x\equiv \lambda e \pmod I, \overline{\lambda}\in \mathrm{Cent}(R/I)\},$$

так что

$$[\mathrm{GL}(n,R),C(n,R,I)]\leq \mathrm{GL}(n,R,I).$$

3. Конгруэнц-подгруппы в специальных линейных группах. Если кольцо R коммутативно, то можно ввести аналоги главной и полной конгруэнц-подгрупп в специальной линейной группе $\mathrm{SL}(n,R)$. А именно, **главная конгруэнц-подгруппа** $\mathrm{SL}(n,R,I)$ это ядро гомоморфизма резукции

$$\rho_I:\mathrm{SL}(n,R)\longrightarrow \mathrm{SL}(n,R/I).$$

Полная конгруэнц-подгруппа $\mathrm{SC}(n,R,I)$ это прообраз центра $\mathrm{SC}(n,R/I)$ группы $\mathrm{SL}(n,R/I)$ по отношению к ρ_I. Таким образом,

$$1\longrightarrow \mathrm{SL}(n,R,I)\longrightarrow \mathrm{SL}(n,R)\longrightarrow \mathrm{SL}(n,R/I),$$

$$1\longrightarrow \mathrm{SC}(n,R,I)\longrightarrow \mathrm{SL}(n,R)\longrightarrow \mathrm{PSL}(n,R/I).$$

Замечание. Стоит заметить, что главные конгруэнц-подгруппы не зависят от выбора ассоциативного (коммутативного в случае специальной линейной группы) кольца с 1, содержащего I в качестве идеала. Таким образом, в принципе, мы могли бы использовать обозначения $\mathrm{GL}(n,I)$ и $\mathrm{SL}(n,I)$ вместо $\mathrm{GL}(n,R,I)$ и $\mathrm{SL}(n,R,I)$, и рассматривать эти группы как полную и специальную линейные группы над кольцом I *без* 1, соответственно. В то же время полные конгруэнц-подгруппы, $C(n,R,I)$ и $\mathrm{SC}(n,R,I)$, вообще говоря, зависят от выбора кольца R!

§ 2. Относительные элементарные группы

Сейчас мы хотим построить аналоги элементарной группы, зависязие от идеала.

1. Подгруппа, порожденная элементарными трансвекциями уровня I. Пусть I – идеал кольца R и $x=t_{ij}(\xi)$ – элементарная трансвекция. Говорят, что это трансвекция **уровня** I если $\xi\in I$ (классически в этом случае говорили, что уровень x *содержится в* I).

Рассмотрим подгруппу $F(n,R,I)$, порожденую всеми элементарными трансвекциями уровня I:

$$F(n,R,I)=\langle t_{ij}(\xi),\xi\in I,1\leq i\neq j\leq n\rangle.$$

Снова эта группа не зависит от выбора объемлющего кольца R с 1, а лишь от самого I, рассматриваемого как кольцо без 1, и часто обозначается просто $E(n,I)$. Однако с точки зрения группы $\mathrm{GL}(n,R)$ группа $E(n,I)$ не может быть правильным аналогом элементарной группы $E(n,R)$. Дело в том, что, вообще говоря, группа $E(n,I)$ не может быть нормальной в $\mathrm{GL}(n,R)$. Почему? Возьмем матрицу $x=(x_{ij})\in E(n,I)$. Тогда $x_{ij}\equiv 0 \pmod I$ для $i\neq j$, но $x_{ii}\equiv 1 \pmod{I^2}$). Таким образом, матрицы

$$z_{12}(\xi,\zeta)=t_{21}(\zeta)t_{12}(\xi)t_{21}(-\zeta)=\begin{pmatrix}1-\xi\zeta & \xi\\ -\zeta\xi\zeta & 1+\zeta\xi\end{pmatrix},$$

где $\xi \in I$, $\zeta \in R$, не могут принадлежать $E(n, I)$

2. Относительные элементарные группы. Чтобы подгруппа H была нормальной в $\mathrm{GL}(n, R)$, *по крайней мере* необходимо, чтобы H нормализовалась элементарной группой $E(n, R)$. Поэтому мы примем следующее определение введенное Хайманом Бассом. Нормальная подгруппа в элементарной группе $E(n, R)$, порожденная всеми элементарными трансвекциями уровня I, называется **элементарной подгруппой** уровня I и обозначается через $E(n, R, I)$. Иными словами, $E(n, R, I)$ это нормальное замыкание $F(n, R, I)$ в $E(n, R)$:

$$E(n, R, I) = \langle t_{ij}(\xi), \xi \in I, 1 \leq i \neq j \leq n \rangle^{E(n,R)}.$$

Если $I \neq R$, то группа $E(n, R, I)$ называется **относительной** элементарной подгруппой, в противоположность **абсолютной** элементарной группе $E(n, R)$. У этой группы уже больше шансов быть нормальной в $\mathrm{GL}(n, R)$. В действительности вскоре мы покажем, что при $n \geq 3$ эта группа действительно нормальна в $\mathrm{GL}(n, R)$, по крайней мере для случая, когда кольцо R клммутативно.

§ 2. Порождение относительных элементарных групп

Относительная элементарная группа $E(n, R, I)$ определялась нами как *нормальная* подгруппа в $E(n, R)$. Да, но чем она порождается как подгруппа? Настоящий параграф не только дает нам возможность прочувствовать разницу между $\langle X \rangle^G$ и $\langle X \rangle$, но и иллюстрирует, как именно используются тождества с коммутаторами. Предполагается, что читатель *активно* обалдел основным текстом главы 8 – в противном случае он не сможет следить за проводимыми ниже вычислениями с листа!!

1. Образующие относительных элементарных групп. Вообще говоря, совершенно неверно, что группа $E(n, R, I)$ порождается *элементарными* трансвекциями, но следующий результат показывает, что приведенный в предыдущем параграфе пример является по существу единственным. Этот результат доказан в статье Л.Н.Васерштейна и А.А.Суслина, и, в более общем контексте, в статьях Титса [Ti] и Абе [Abe] и Бака–Вавилова.

Теорема. *Для $n \geq 3$ относительная элементарная группа $E(n, R, I)$ порождена матрицами*

$$z_{ij}(\xi, \zeta) = t_{ji}(\zeta) t_{ij}(\xi) t_{ji}(-\zeta),$$

где $\xi \in I$, $\zeta \in R$, $1 \leq i \neq j \leq n$.

Доказательство. Так как $z_{ij}(\xi, 0) = t_{ij}(\xi)$ является обычной элементарной трансвекцией, то подггруппа, порожденная всеми $z_{ij}(\xi, \zeta)$, содержит $F(n, R, I)$. По определению $E(n, R, I)$ порождена матрицами вида ${}^x t_{ij}(\xi) = x t_{ij}(\xi) x^{-1}$, где $x \in E(n, R)$, $\xi \in I$ и $1 \leq i \neq j \leq n$. Мы хотим показать, что любая такая матрица принадлежит подгруппе, порожденной элементами $z_{ij}(\xi, \zeta)$. Будем рассуждать индукцией по длине t самого уороткого выражения x как произведения элементарных трансвекций. Если $t \leq 1$ доказывать нечего. Для $t \geq 2$ запишем x в виде $t_{hk}(\zeta) y$, где $y \in E(n, R)$, $\zeta \in R$ и $1 \leq h \neq k \leq n$. Применяя формулу ${}^{ab}c = {}^a[b, c]\, {}^a c$ которая, как мы знаем, выполняется для любых трех элементов $a, b, c \in G$, мы получаем

$${}^{t_{hk}(\zeta) y} t_{ij}(\xi) = {}^{t_{hk}(\zeta)}[y, t_{ij}(\xi)]\, {}^{t_{hk}(\zeta)} t_{ij}(\xi).$$

Если $(h, k) \neq (j, i)$, мы можем применить (R2), чтобы заключить, что $z = {}^{t_{hk}(\zeta)} t_{ij}(\xi)$ принадлежит $F(n, R, I)$, а если $(h, k) = (j, i)$, то $z = z_{ij}(\xi, \zeta)$. С другой стороны, так как y короче, чем x, то коммутатор $[y, t_{ij}(\xi)]$ уже представим как произведение множителей вида $z_{lm}(\omega, \vartheta)$, $\omega \in I$, $\vartheta \in R$, $1 \leq l \neq m \leq n$. Теперь для $w = {}^{t_{hk}(\zeta)} z_{lm}(\omega, \vartheta)$ мы имеем одну из следующих трех возможностей:

Либо $(h, k) \neq (l, m), (m, l)$, и тогда $w \in z_{lm}(\omega, \vartheta) F(n, R, I)$ by (R2).

Либо $(h, k) = (m, l)$, и тогда $w = w_{1m}(\omega, \vartheta + \zeta)$.

Либо, наконец, $(h,k)=(l,m)$ и тогда, взяв индекс $p\neq h,k$ и выражая $t_{lm}(\omega)$ как $t_{lm}(\omega)=[t_{lp}(1),t_{pm}(\omega)]$, мы получаем

$$\begin{aligned}{}^{t_{lm}(\zeta)}z_{lm}(\omega,\tau) &= {}^{t_{lm}(\zeta)t_{ml}(\tau)}t_{lm}(\omega)=\\ &= {}^{t_{lm}(\zeta)t_{ml}(\tau)}[t_{lp}(1),t_{mp}(\omega)]=\\ &= [{}^{t_{lm}(\zeta)t_{ml}(\tau)}t_{lp}(1),{}^{t_{lm}(\zeta)t_{ml}(\tau)}t_{pm}(\omega)]=\\ &= [t_{mp}(\tau)t_{lp}(1+\zeta\tau),t_{pl}(-\omega\tau)t_{pm}(\omega(1+\tau\zeta))]\end{aligned}$$

В этом месте Леонид Васерштейн и Андрей Суслин заканчивают доказательство следующей сакраментальной фразой: "**очевидно** что этот последний коммутатор является произведением множителей требуемого вида". Анатоль Франс комментирует: "Ce que l'un voit, l'autre ne le voit pas". Для пешеходов востановим, что скрывается за словом 'очевидно', выделив эту очевидную часть в отдельную лемму, которая будет использоваться и по другим поводам.

Лемма. *Пусть $\tau,\zeta\in R$, $\xi,\omega\in I$ и l,m,p три попарно различных индекса. Тогда коммутатор $[t_{mp}(\tau)t_{lp}(\zeta),t_{pl}(\xi)t_{pm}(\omega)]$ можно выразить как произведение трансвекций из $F(n,R,I)$ и множителей вида $z_{pl}(\sigma,\tau)$ и $z_{pm}(\sigma,\tau)$ для подходящих $\sigma\in I$ и $\tau\in R$.*

Доказательство. Действительно, пусть $a,b,c,d\in G$ – любые четыре элемента группы G. Тогда

$$[ab,cd]={}^a[b,c]\cdot{}^{ac}[b,d]\cdot[a,c]\cdot{}^c[a,d]={}^a[b,c]\cdot[a,c]\cdot{}^{ca}[b,d]\cdot{}^c[a,d].$$

Применяя первую из этих формул к рассматриваемому коммутатору, мы выразим его как произведение следующих четырех множителей:

$${}^{t_{mp}(\tau)}[t_{lp}(\zeta),t_{pl}(\xi)]={}^{t_{mp}(\tau)}z_{pl}(\xi,\zeta)^{t_{mp}(\tau)}t_{pl}(\omega\tau),$$

$${}^{t_{mp}(\tau)t_{pl}(\xi)}t_{lm}(\zeta\omega)={}^{t_{mp}(\tau)}\big(t_{lm}(\zeta\omega)t_{pm}(\xi\zeta\omega)\big)={}^{t_{mp}(\tau)}t_{lm}(\zeta\omega)z_{pm}(\xi\zeta\omega,\omega)$$

$$[t_{mp}(\tau),t_{pl}(\xi)]=t_{ml}(-\tau\xi),$$

$${}^{t_{pl}(\xi)}[t_{mp}(\tau),t_{pm}(\omega)]={}^{t_{pl}(\xi)}z_{pm}(\omega,\tau)t_{pm}(-\omega).$$

Так как ξ и ω принадлежат I, то все эти выражения являются произведениями трансвекций их $F(n,R,I)$ и множителей требуемого вида.

Замечание. Разумеется, можно было бы сформулировать двойственное утверждение для случая, когда $\tau,\zeta\in I$, а $\xi,\omega\in R$. В этом случае коммутатор в формулировке леммы выразился бы как произведение траснвекций из $F(n,R,I)$ и множителей вида $z_{lp}(\sigma,\tau)$ и $z_{mp}(\sigma,\tau)$.

Следствие. *Пусть $n\geq 3$. Тогда для любого идеала I в R имеет место включение*

$$F(n,R,I)\geq E(n,R,I^2).$$

Доказательство. Так как $z_{ij}(\xi,\zeta)$ аддитивно по отношению к ξ, то группа $E(n,R,I^2)$ порождена матрицами вида $z_{ij}(\xi_1\xi_2,\zeta)$, где $\xi_1,\xi_2\in I$, $\zeta\in R$, $1\leq i\neq j\leq n$. Возьмем индекс $h\neq i,j$. Тогда

$$z_{ij}(\xi_1\xi_2,\zeta)={}^{t_{ji}(\zeta)}[t_{ih}(\xi_1),t_{hj}(\xi_2)]=[t_{ih}(\xi_1)t_{jh}(\zeta\xi_1),t_{hj}(\xi_2)t_{hi}(\xi_2\zeta)]$$

и последняя матрица принадлежит $F(n,R,I)$ по определению.

§ 2. Леммы типа Уайтхеда

В этом параграфе мы увидим, что умножение матриц и образование прямой суммы *совпадают по модулю элементарных матриц*. Это удивительное наблюдение, которое обычно называется **леммой Уайтхеда**, было одной из отправных точек алгебраической K-теории. В действительности, мы обсудим

чуть более общие факты, связанные с редукцией к меньшему рангу, которые обычно цитируются как **леммы типа Уайтхеда**.

1. Лемма Уайтхеда-Васерштейна. Пусть $x, y \in R$ таковы, что $1+xy \in R^*$. В книге III нам представится случай заинтересоваться вопросом, следует ли отсюда, что $1 + yx \in R^*$? Следующий результат означает, в частности, что это действительно так, причем в гораздо более общем контексте.

Лемма Уайтхеда. *Пусть матрицы $x \in M(r, s, I)$ и $y \in M(s, r, R)$ таковы, что $e + xy \in \mathrm{GL}(r, R)$. Тогда $e + yx \in \mathrm{GL}(s, R)$ и*

$$\begin{pmatrix} e+xy & 0 \\ 0 & (e+yx)^{-1} \end{pmatrix} \in E(r+s, R, I).$$

Доказательство. Первое утверждение следует из равенства

$$\begin{pmatrix} e & 0 \\ 0 & e+yx \end{pmatrix} = \begin{pmatrix} e & 0 \\ -y & e \end{pmatrix} \begin{pmatrix} e & -x \\ 0 & e \end{pmatrix} \begin{pmatrix} e+xy & 0 \\ 0 & e \end{pmatrix} \begin{pmatrix} e & 0 \\ y & e \end{pmatrix} \begin{pmatrix} e & x \\ 0 & e \end{pmatrix},$$

все множители в правой части которого обратимы. Умножая это равенство справа на $(e + xy)^{-1} \oplus e$, мы получим

$$\begin{pmatrix} (e+xy)^{-1} & 0 \\ 0 & e+yx \end{pmatrix} = \begin{pmatrix} e & 0 \\ -y & e \end{pmatrix} \begin{pmatrix} e & -x \\ 0 & e \end{pmatrix} \begin{pmatrix} e & 0 \\ y & e \end{pmatrix} \begin{pmatrix} e & 0 \\ y(e+xy)^{-1} - y & e \end{pmatrix} \begin{pmatrix} e & (e+xy)x \\ 0 & e \end{pmatrix}.$$

Произведение первых трех множителей и последний множитель принадлежат $E(r+s, R, I)$ по самому определению этой группы. Но так как $(e+xy)^{-1} = e+z$, где $z \in M(r, I)$, то и четвертый множитель тоже принадлежит $E(r + s, R, I)$.

2. Лемма Уайтхеда. Из предыдущей леммы сразу вытекает такой факт.

Лемма. *Пусть $a \in \mathrm{GL}(n, R, I)$ и $b \in \mathrm{GL}(n, R)$. Тогда*

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \quad \begin{pmatrix} ba^{-1}b^{-1} & 0 \\ 0 & a \end{pmatrix}, \quad \begin{pmatrix} aba^{-1}b^{-1} & 0 \\ 0 & e \end{pmatrix} \in E(2n, R, I)$$

Доказательство. Применяя предшествующую лемму вначале к $x = a-e, y = e$ а потом к $x = (a^{-1} - 1)b^{-1}, y = b$ мы видим, что первые две матрицы принадлежат $\mathrm{GL}(2n, R, I)$. Третья матрица является их произведением.

Теперь как следствие мы получаем первоначальную форму леммы Уайтхеда.

Лемма Уайтхеда. *Пусть $a \in \mathrm{GL}(n, R, I)$ и $b \in \mathrm{GL}(n, R)$. Тогда левые (и правые) смежные классы матриц*

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, \quad \begin{pmatrix} ab & 0 \\ 0 & e \end{pmatrix}, \quad \begin{pmatrix} ba & 0 \\ 0 & e \end{pmatrix}$$

относительно подгруппы $E(2n, R, I)$ совпадают.

Сформулируем еще одну форму леммы Уайтхеда.

Лемма. *Пусть матрицы $x \in M(n, I)$ и $y \in M(n, R)$ таковы, что $e + xy \in \mathrm{GL}(n, R)$. Тогда*

$$\begin{pmatrix} (e+xy)(e+yx)^{-1} & 0 \\ 0 & e \end{pmatrix} \in E(2n, R, I).$$

Доказательство. В самом деле, в этом случае

$$\begin{pmatrix} e+xy & 0 \\ 0 & (e+yx)^{-1} \end{pmatrix}, \quad \begin{pmatrix} (e+yx)^{-1} & 0 \\ 0 & e+yx \end{pmatrix} \in E(2n, R, I).$$

§ 3. Трансвекции стабильно элементарны

1. Трансвекции с нулевым коэффициентом. Из леммы Уайтхеда-Васерштейна сразу вытекает следующий важный факт (см., например, [VS], [Su?]). Этот факт можно рассматривать как первый шаг в направлении доказательства нормальности элементарной подгруппы.

Лемма. *Рассмотрим трансвекцию $x = t_{uv}(\xi)$, $u \in R^n$, $v \in {}^nR$, $\xi \in I$, $vu = 0$. если одна из компонент строки v (или столбца u) равна 0, то $x \in E(n, R, I)$.*

Первое доказательство. Пусть одна из компонент v равна нулю. Так как все компоненты социологически равны, мы можем не теряя общности считать, что $u_n = 0$. Выразим u и v как $u = (\widehat{u}, u_n)^T$ и $v = (\widehat{v}, 0)$, где $\widehat{u} \in R^{n-1}$ является столбцом высоты $n-1$, а $\widehat{v} \in {}^{n-1}R$ – строкой длины $n-1$. Тогда $\widehat{v}\widehat{u} = 0$ и

$$x = \begin{pmatrix} e + \widehat{u}\xi\widehat{v} & 0 \\ u_n\xi\widehat{v} & 1 \end{pmatrix} = \begin{pmatrix} e + \widehat{u}\xi\widehat{v} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} e & 0 \\ u_n\xi\widehat{v} & 1 \end{pmatrix}.$$

Оба множителя в правой части являются трансвекциями из $E(n, R, I)$: что касается второго множителя, это очевидно, а для первого следует из леммы Уайтхеда-Васерштейна с $x = \widehat{u}$ и $y = \xi\widehat{v}$.

В действительности, эта лемма сразу вытекает из коммутационной формулы Шевалле – в нашем случае из соотношения (R2). Сейчас мы дадим такое ее доказательство, которое не использует лемму Уайтхеда-Васерштейна. Идея этого доказательства взята из [BMS] (см. также [V?]). Возьмем $\xi \in R$ и посмотрим на трансвекцию $x = gt_{ij}(\xi)g^{-1}$, где $1 \le i, j \le n-1$, и $g \in \mathrm{GL}(n-1, R)$. Почему она должна принадлежать элементарной группе $E(n, R, I)$ при обычном вложении

$$g \mapsto \begin{pmatrix} g & 0 \\ 0 & 1 \end{pmatrix}?$$

Так как все трансвекции социологически эквивалентны, возьмем $(i, j) = (1, 2)$. Выражая $t_{12}(\xi)$ в форме $t_{12}(\xi) = [t_{1n}(1), t_{n2}(\xi)]$, мы получаем

$$gt_{12}(\xi)g^{-1} = [gt_{1n}(1)g^{-1}, gt_{n2}(\xi)g^{-1}].$$

При этом

$$gt_{1n}(1)g^{-1} = \begin{pmatrix} e & ge_1 \\ 0 & 1 \end{pmatrix}, \qquad gt_{n2}(\xi)g^{-1} = \begin{pmatrix} e & 0 \\ \xi f_2 g^{-1} & 1 \end{pmatrix},$$

где $ge_1 = g_{*1}$ является первым столбцом матрицы g в то время как $\xi f_2 g^{-1} = \xi g_{2*}$ является второй строкой матрицы g^{-1}, умноженным на ξ.

Второе доказательство. Только что проведенные рассуждения показывают, что для любых $u \in R^{n-1}$ и $v \in {}^{n-1}R$ таких, что $vu = 0$ естественно ждать, что

$$\begin{pmatrix} e + u\xi v & 0 \\ 0 & 1 \end{pmatrix} = \left[\begin{pmatrix} e & 0 \\ -v & 1 \end{pmatrix}, \begin{pmatrix} e & \xi u \\ 0 & 1 \end{pmatrix} \right].$$

Разумеется, после того, как такая формула написана, она сразу проверяется непосредственным вычислением.

Эта лемму можно истолковать в том смысле, что **все** трансвекции стабильно элементарны. Рассмотрим трансвекцию $e + u\xi v$, где $u \in R^n$, $v \in {}^nR$, $\xi \in I$, $vu = 0$. Рассматриваемая как элемент группы $\mathrm{GL}(n+1, R)$ посредством вложения φ_n^{n+1} эта трансвекция имеет вид $e + \widetilde{u}\xi\widetilde{v}$, где $\widetilde{u}$ и $\widetilde{v}$ получаются из u и v, соответственно, добавлением нулей. Таким образом, *рассматриваемая как элемент* $\mathrm{GL}(n+1, R)$ эта трансвекция удовлетворяет условиям предыдущей леммы.

Следствие. *Для любого ассоциативного кольца R имеет место включение $T(n, R, I) \subset E(n+1, R, I)$.*

§ 10. Разложение Брюа

Разложение Брюа вне всякого сомнения самый важный факт о линейных группах над телами, который объясняет большую часть специфики этих групп, по сравнению с группами над кольцами.

Пусть $R = T$ – тело. Очень хорошо известно, что в этом случае подгруппы $B = B(n, T)$ и $N = N(n, T)$ образуют BN-пару в $G = \mathrm{GL}(n, T)$ [Bu], [Hm]. В частности, это значит, что в группе $\mathrm{GL}(n, T)$ выполняется **лемма Брюа**. Однако мы дадим прямое доказательство, не зависящее от теории BN-пар. НУЖНО ЛИ ЭТО!! W УЖЕ ЕСТЬ!! Для каждого $w \in W$ выберем представитель $n_w \in N$. В формулировку и доказательство следующиего результата обозначим двойной смежный класс Bn_wB просто через BwB. Так как B содержит D, никакой двусмысленности здесь нет. В действительности, класс Bn_wB не зависит от специального выбора n_w, а только от самого элемента w.

Лемма Брюа. *Для любого тела T полная линейная группа $G = \mathrm{GL}(n, T)$ допускает следующее разложение*

$$G = BNB = BWB,$$

причем W образует в точности множество представителей двойных смежных классов G по модулю B, т.е. если $Bw_1B = Bw_2B$ для некоторых $w_1, w_2 \in W$, то $w_1 = w_2$.

Элементарное доказательство. **Существование.** Прежде всего мы докажем, что любую матрицу $g \in \mathrm{GL}(n, T)$ можно выразить в форме $g = b_1?b_2$ для некоторого $b_1, b_2 \in B$ и $? \in N$. Действуем индукцией по n. В качестве базы индукции можно взять случай $n = 1$, когда наше утверждение очевидно. Так

как матрица g обратима, то $g_{*1} \neq 0$. Пусть $h = i_1$ максимальный индекс такой, что $g_{h,1} \neq 0$. Рассмотрим следующие верхние унитреугольные матрицы

$$u = t_{1h}(-a_{11}a_{h1}^{-1}) \dots t_{h-1,h}(-a_{h-1,1}a_{h1}^{-1}),$$
$$v = t_{12}(-a_{h1}^{-1}a_{h2}) \dots t_{1n}(-a_{h1}^{-1}a_{hn}).$$

Теперь x_{h1} является единственным ненулевым элементом в 1-м столбце x_{*1} и h-й строке x_{h*} матрицы $x = ugv$. Вычеркивая из x этот столбец и эту строку, мы получаем матрицу $y \in \mathrm{GL}(n-1,T)$. Применяя к y индукционное предположение, мы получаем, что $y \in B(n-1,T)N(n-1,T)B(n-1,T)$.

Единственность. Пусть теперь $Bw_1B = Bw_2B$ для некоторых $w_1, w_2 \in W$. Это значит, что $w_2 \in Bw_1B$, или, другими словами, что $w_2 = b_1w_1b_2^{-1}$ для некоторых $b_1, b_2 \in B$. Это равенство можно переписать в виде $w_2b_2 = b_1w_1$. Первый столбец матрицы w_2b_2 отличается от первого столбца матрицы w_2 самое большее на ненулевой множитель из T. Рассмотрим первый столбец матрицы b_1w_1. If w_1???

2. Каноническая форма. В действительности разложение Брюа можно уточнить так, чтобы получить каноническую форму элементов G, называемой **приведенным разложением Брюа**. Для элемента $w \in W$ положим $U_w^- = \{u \in U \mid wuw^{-1} \in V\}$. Ясно, что U_w^- является подгруппой в U. Тогда приведенное разложение Брюа состоит в том, что любой элемент $g \in G$ модно *единственным образом* выразить в виде $g = duwv$, где $d \in D$, $u \in U$, $w \in W$, $v \in U_w^-$.

§ 11. Параболические подгруппы

1. Параболические подгруппы. Напомним, что **стандартной параболической подгруппой** в G называется подгруппа, соджержащая B. Знаменитая теорема Жака Титса утверждает, что из того, что B и N образуют BN-пару вытекает **стандартное описание** стандартных параболических подгрупп. Для нашего случая стандартное описание утверждает в точности, что каждая подгруппа, содержащая $B(n,T)$, совпадает с одной из групп $B(\nu,T)$ для какого-то разбиения ν степени n.

Еще одна знаменитая теорема Титса утверждает, что B абнормальна в G, или, другими словами, что все группы $B(\nu,T)$ совпадают со своими нормализаторами и что никакие две различные подгруппы $B(\mu,T)$ и $B(\nu,T)$ не сопряжены в G.

§ 12. Неприводимость

Для тел имеется очень мощный инструмент, который во многих случаях позволяет сводить вопросы о всех группах из данного класса к изучению *примитивных неприводимых* подгрупп.

Пусть теперь $R = T$ – тело. Подгруппа G полной линейной группы $\mathrm{GL}(n,T)$ называется **неприводимой**, если она на содержится *с точностью до сопряженности* ни в одной собственной подгруппе верхних блочно-треугольных матриц $B(\nu,T)$. Иными словами, это означает, что ни одна сопряженная xGx^{-1}, $x \in \mathrm{GL}(n,T)$, группы G не содержится в группе $B(\nu,T)$ для разбиения ν степени n с более, чем одним слагаемым.

Конечно, это определение эквивалентно обычному. Чтобы убедиться в этом, рассмотрим линейную гшруппу $G \leq \mathrm{GL}(n,T)$. Напомним, что подпространство U *правого* векторного пространства $V = T^n$ называется **G-инвариантным**, если $gU \subseteq U$ для всех $g \in G$. Для каждой подгруппы $G \leq \mathrm{GL}(n,T)$ имеется два *очевидных* инвариантных подпространства, а именно, V и 0. Подгруппа G называется **неприводимой**, если других G-инвариантных подпространств в V нет.

Действительно, пусть у G есть неочевидное инвариантное подпространство U. Тогда G содержится в стабилизаторе этого подпространства. Если $\dim U = m$, то его стабилизатор сопряжен с группой верхних блочно-треугольных матриц типа $(m, n-m)$.

§ 13. Примитивность

Пусть $V = U_1 \oplus \ldots \oplus U_t$ – разложение пространства V в прямую сумму подпространств размерностей $n_1, \ldots, n_t$, соответственно. Тогда *поэлементный стабилизатор* $C(\mathcal{U})$ разложения $\mathcal{U} = \{U_1, \ldots, U_t\}$ состоит из всех $g \in \mathrm{GL}(n,T)$ таких, что $g(U_i) \subseteq U_i$ для всех i. Ясно, что поэлементный стабилизатор $\{U_1, \ldots, U_t\}$ сопряжен с $D(\nu,T)$, где $\nu = (n_1, \ldots, n_t)$.

Напомним, что **флаг** $\mathcal{F} = \{V_1, \ldots, V_s\}$ это последовательность $V_1 \subset \ldots \subset V_s$ вложенных (nested) подпространств в V. Стабилизатор флага (flag stabilizer) $C(\mathcal{F})$ состоит из всех $g \in \mathrm{GL}(n,T)$ таких, что $g(V_i) \subseteq V_i$ для всех i. Разложение $\mathcal{U} = \{U_1, \ldots, U_t\}, V = U_1 \oplus \ldots \oplus U_t$ определяет флаг $\mathcal{F} = \mathcal{F}(\mathcal{U})$:

$$U_1 \subset U_1 \oplus U_2 \subset \ldots \subset U_1 \oplus \ldots \oplus U_{t-1}$$

Группа $B(\nu,T)$ сопряжена со стабилизатором флага $C(\mathcal{F})$.

В свою очередь блочно-мономиальная подгруппа $N(\nu,T)$ сопряжена со стабилизатором разложения $\mathcal{U} = \{U_1, \ldots, U_t\}$ в целом. Она состоит их всех матриц $g \in \mathrm{GL}(n,T)$ таких, что для любого i существует такое j, что $g(U_i) \subseteq U_j$. Подгруппа $G \leq \mathrm{GL}(n,T)$ называется **примитивной**, если она не содержится *с точностью до сопряженности* ни в одной из собственных подгрупп вида $N(\nu,T)$. Как мы только что отметили, это определение эквивалентно обычному определению, что не существует *нетривиального* разложения в прямую сумму $\mathcal{U} = \{U_1, \ldots, U_t\}$ такого, что для любого $g \in G$ и любого i существует j такое, что $g(U_i) \subseteq U_j$. Группа, которая не является примитивной, называется *импримитивной*, Любое нетривиальное разложение $\mathcal{U} = \{U_1, \ldots, U_t\}$ с этим свойством называется *системой импримитивности* для подгруппы G, а члены такой системы $U_1, \ldots, U_t$ называются **блоками импримитивности**.

Самый интересный случай – это случай *неприводимых* подгрупп. Если группа $N(\nu,T)$ неприводима, то $\nu = (m, \ldots, m)$ является разбиением на равные слагаемые.

§ 21. Теорема Клиффорда

§ 22. Теорема Маклафлина

Глава X. ГРУППЫ, revisited

> Теорию групп ныне преподают в средней школе; поэтому лица, окончившие школу недавно, могут пропустить этот параграф. Однако более пожилым физикам его необходимо проработать, чтобы иметь возможность беседовать со своими детьми и учить студентов.
>
> Я.Б.Зельдович, И.М.Яглом, Высшая математика для начинающих физиков и техников

В этой главе мы начинаем знакомство с настоящей теорией групп. Большая часть из того, о чем шла речь в Главе 1, относится к общей алгебре. То, что мы обсуждаем здесь, специфично именно для групп.

Тема 1. Коммутаторы и коммутант

Одним из самых полезных и часто используемых инструментов теории групп являются вычисления с коммутаторами.

§ 1. Коммутаторы, коммутант, абелианизация

1. Коммутаторы, коммутант. Напомним, что в Главе II мы уже имели дело с коммутаторами элементов в группе. Обычно мы понимаем под **коммутатором** элементов $x, y \in G$ их **левонормированный коммутатор** $[x, y] = [x, y]_l = xyx^{-1}y^{-1}$. Заметим, впрочем, что во многих книгах по комбинаторной теории групп коммутатором называется **правонормированный коммутатор** $[x, y]_r = x^{-1}y^{-1}xy$. Ясно, что $[x, y]_r = [x^{-1}, y^{-1}]_l$. Таким образом, любая формула в правонормированных коммутаторах легко переводится на язык левонормированных коммутаторов и наоборот.

Напомним (ibid.), что **коммутантом** группы называется подгруппа, *порожденная* множеством всех коммутаторов:

$$[G, G] = \langle [x, y] \mid x, y \in G \rangle.$$

Так как $[x, y]^{-1} = [y, x]$, то любой элемент коммутанта представляется в виде произведения конечного числа коммутаторов. Классики XIX века, в частности, Софус Ли, обычно называли $[G, G]$ **производной группой** группы G (abgeleitete Gruppe, erste abgeleitete Gruppe, erste Ableitung, откуда derived group, sous-groupe dérivé).

Предостережение. Типичная ошибка начинающих состоит в том, что они считают, что коммутант *состоит* из коммутаторов. Это не так, еще раз подчеркнем, что коммутант *порождается* коммутаторами и, тем самым, состоит из всевозможных *конечных произведений* коммутаторов. В §§ 3 и 4 мы приведем примеры, показывающие, что, вообще говоря, **не каждый** элемент коммутанта является коммутатором. Первый такой пример был построен У.Файтом (W.Fite) в 1902 году, его группа имела порядок 2^8. Наименьший порядок группы, в которой коммутант не совпадает с множеством коммутаторов, равен 96. С помощью любой системы компьютерной алгебры/символьных вычислений несложно проверить, что существует ровно 2 неизоморфных группы порядка 96, в каждой из которых не каждый элемент коммутанта является коммутатором. А именно, в каждой из этих двух групп порядок коммутанта равен 32, в то время как имеется лишь 29 коммутаторов (см. [Ro], стр.34).

2. Основные свойства коммутанта. Коммутант, как и центр, измеряет отклонение группы от абелевости. Чем *больше* центр и чем *меньше* коммутант, тем ближе группа к абелевой. Сейчас мы придадим этому утверждению точный технический смысл. В Главе I мы уже убедились в том, что $[G,G] \trianglelefteq G$. Сейчас мы усилим этот результат и покажем, что коммутант – это *наименьшая* нормальная подгруппа в G, фактор-группа по которой абелева.

Напомним, что подгруппа $H \leq G$ нормальна, если $\varphi(H) \leq H$ для любого *внутреннего автоморфизма* $\varphi \in \mathrm{Inn}(G)$. Подгруппа H называется **характеристической**, если $\varphi(H) \leq H$ для любого *автоморфизма* $\varphi \in \mathrm{Aut}(G)$. Подгруппа H называется **вполне характеристической**, если $\varphi(H) \leq H$ для любого *эндоморфизма* $\varphi \in \mathrm{End}(G)$. Так как $\mathrm{Inn}(G) \leq \mathrm{Aut}(G) \leq \mathrm{End}(G)$, то имеет место следующая цепочка импликаций: H вполне характеристическая $\Longrightarrow H$ характеристическая $\Longrightarrow H$ нормальная.

Теорема. *1) Коммутант $[G,G]$ является вполне характеристической и, в частности, нормальной подгруппой в G;*

2) Фактор по коммутанту $G/[G,G]$ – абелева группа;

3) Если $H \trianglelefteq G$ такая нормальная подгруппа, что фактор G/H абелев, то $H \leq [G,G]$.

В частности, ядро $\mathrm{Ker}(\psi)$ любого гомоморфизма $\psi : G \longrightarrow A$ в абелеву группу A, содержит $[G,G]$.

Доказательство. 1) Пусть $\varphi \in \mathrm{End}(G)$. Тогда для произвольного коммутатора $[x,y]$, $x,y \in G$, имеем $\varphi([x,y]) = [\varphi(x),\varphi(y)] \in [G,G]$. Так как $[G,G]$ порождается коммутаторами, то $\varphi([G,G] \leq [G,G]$.

2) Пусть $\overline{h} = h[G,G]$ и $\overline{g} = g[G,G]$ – два смежных класса по коммутанту. Так как $[G,G]$ – нормальная подгруппа, то $[\overline{h},\overline{g}] = [h,g][G,G] = [G,G]$. Но это и значит, что $G/[G,G]$ абелева.

3) Обозначим через π каноническую проекцию $G \longrightarrow G/H$. Тогда так как группа G/H абелева, то для любого коммутатора $[x,y]$ имеем $\pi([x,y]) = [\pi(x),\pi(y)] = 1$. Но это и значит, что $[x,y] \in \mathrm{Ker}(\pi) = H$. Так как $[G,G]$ порождается коммутаторами, то $[G,G] \leq H$.

3. Абелианизация. Только что доказанная нами теорема утверждает, что фактор-группа $G/[G,G]$ является *наибольшей* абелевой фактор-группой. Обычно она обозначается G^{ab} и называется **абелианизацией группы** G. Заметим, впрочем, что некоторые авторы называют абелианизацией каноническую проекцию $\pi^{\mathrm{ab}} = \pi^{\mathrm{ab}}_G : G \longrightarrow G^{\mathrm{ab}}$.

Абелианизации важна и полезна *потому*, что она **функториальна**, т.е. каждый гомоморфизм групп $\varphi : H \longrightarrow G$ индуцирует гомоморфизм абелианизаций $\varphi^{\mathrm{ab}} : H^{\mathrm{ab}} \longrightarrow G^{\mathrm{ab}}$. Так как $\pi^{\mathrm{ab}}_G\varphi : H \longrightarrow G \longrightarrow G^{\mathrm{ab}}$ есть гомоморфизм группы H на абелеву группу G^{ab}, то по только что доказанной теореме $\mathrm{Ker}(\pi^{\mathrm{ab}}\varphi)[H,H]$ и, следовательно, по теореме о гомоморфизме, он пропускается через $\pi^{\mathrm{ab}}_H : H \longrightarrow H^{\mathrm{ab}}$. Иными словами, существует единственный гомоморфизм $\varphi^{\mathrm{ab}} : H^{\mathrm{ab}} \longrightarrow G^{\mathrm{ab}}$ такой, что $\pi^{\mathrm{ab}}_G\varphi = \varphi^{\mathrm{ab}}\pi^{\mathrm{ab}}_H$, называемый **абелианизацией гомоморфизма** φ.

Задача. Докажите, что для если φ,ψ – два гомоморфизма, то $(\varphi\psi)^{\mathrm{ab}} = \varphi^{\mathrm{ab}}\psi^{\mathrm{ab}}$.

Таким образом, сопоставление каждой группе и гомоморфизму их абелианизаций действительно определяет функтор из катеории групп в категорию абелевых групп.

§ 2. Коммутант S_n и $\mathrm{GL}(n,K)$

В этом параграфе мы вычислим коммутант двух важнейших групп.

1. Коммутант S_n. В этом случае вычислить коммутант совсем просто.

Теорема. *1) Для любого n имеет место равенство $[S_n, S_n] = A_n$;*

2) Для любого $n \geq 5$, кроме того, $[A_n, A_n] = A_n$;

3) $[A_4, A_4] = V$.

Доказательство. Без потери общности можно предполагать $n \geq 3$. Ясно, что коммутатор $[\pi, \rho]$ двух любых перестановок $\pi, \rho \in S_n$ является четной перестановкой, поэтому $[A_n, A_n] \leq [S_n, S_n] \leq A_n$. С другой стороны, так как A_n порождается 3-циклами (Глава II, § ?), то для завершения доказательства первого утверждения достаточно заметить, что для любых трех различных индексов i, j, h имеем $(ijh) = [(ij), (ih)]$, а для завершения доказательства второго – что для любых пяти различных индексов i, j, h, k, l имеем $(ijh) = [(ijk), (ihl)]$. Для доказательства третьего утверждения заметим, что из Глава II, § ? нам известно, что V – нормальный делитель в A_4 фактор- группа по которому имеет порядок 3 и, поэтому, абелев. Тем самым, $[A_4, A_4] \leq V$. Наконец, если i, j, h, k четыре различных индекса, то $(ij)(hk) = [(ijh), (ijk)]$, так что $V \leq [A_4, A_4]$.

2. Совершенные группы. Группа G называется **совершенной**, если она совпадает со своим коммутантом, т.е. $[G, G] = G$. Термин *совершенная группа* (perfekte Gruppe) ввел Софус Ли. Вторая часть теоремы предыдущего пункта утверждает в точности, что знакопеременная группа A_n, $n \geq 5$, совершенна. Ясно, что если G – простая группа, то ее коммутант $[G, G]$ обязан совпадать либо с 1, либо с G. таким образом, если G – неабелева простая группа, то $[G, G] = G$. Таким образом, вторая часть вытекает также из теоремы Галуа о простоте знакопеременной группы, доказанной нами в § ?. В самом деле, группа A_n, $n \geq 5$, проста и поэтому обязана быть совершенной. Однако ссылаться на теорему простоты для доказательства гораздо более простого факта, прямое доказательство которого занимает несколько строчек, было бы нелепо. С другой стороны, группа A_3 абелева и поэтому не может совпадать со своим коммутантом.

Легко видеть, что существует много совершенных групп, не являющихся простыми.

Упражнение. Убедитесь, что если $G = G_1 \times \ldots \times G_n$, то $[G, G] = [G_1, G_1] \times \ldots \times [G_n, G_n]$. В частности, прямое произведение неабелевых простых групп совершенно.

В действительности, в следующем пункте мы построим широкий класс совершенных групп, которые весьма далеки от простых.

Предостережение. Во многих старых книгах, включая [Hall], [KaMe], группа называлась *совершенной* (vollkommene Gruppe, complete group), если ее центр тривиален, а все автоморфизмы внутренние. Однако это понятие представляет интерес только как курьез и в настоящее время употребление термина 'совершенная группа' в смысле vollkommene Gruppe *полностью* вышло из употребления. Последние 20-30 лет специалисты употребляют термин 'совершенная группа' в смысле perfekte Gruppe (perfect group). Отметим, кроме того, что многие авторы называют группы, совпадающие со своим коммутантом, **связными** (connected).

3. Коммутант $\mathrm{GL}(n, K)$**.** Начнем с рассмотрения более общей ситуации. Пусть вначале R – произвольное ассоциативное кольцо и $G = E(n, R)$ – элементарная группа степени n над R, порожденная всеми элементарными трансвек-

циями $t_{ij}(\xi) = e + \xi e_{ij}$, $\xi \in R$, $1 \leq i \neq j \leq n$. Следующее ключевое соображение доказывается непосредственным вычислением.

Лемма. *Для любых $\xi, \zeta \in R$ и любых четырех индексов i, j, h, k таких, что $i \neq j$, $h \neq k$, имеет место равенство*

$$[t_{ij}(\xi), t_{hk}(\zeta)] = \begin{cases} e & \text{если } j \neq h,\ i \neq k, \\ t_{ik}(\xi\zeta) & \text{если } j = h,\ i \neq k, \\ t_{hj}(-\zeta\xi) & \text{если } j \neq h,\ i = k. \end{cases}$$

Приведенная в этой лемме формула является частным случаем коммутационной формулы Шевалле. Заметим, что про ситуацию, когда $j = h$, $i = k$ здесь ничего не говорится, так как столь же простой формулы в этом случае нет. Ясно, что из этой леммы сразу вытекает что группа $E(n, R)$ совершенна.

Следствие. *Для любого ассоциативного кольца R и любого $n \geq 3$ имеет место равенство*

$$[E(n, R), E(n, R)] = E(n, R).$$

С другой стороны, если $R = K$ поле, то для любого $n \geq 2$ имеем $E(n, K) = \mathrm{SL}(n, K)$ (см. Главу IV, § ?). Комбинируя два эти результата мы сразу получаем полный ответ в случае, когда $R = K$ – поле, а $n \geq 3$. В случае $n = 2$ понадобятся дополнительные вычисления.

Теорема. *Предположим, что K – поле и либо $n \geq 3$, либо $n = 2$ и $|K| \geq 4$. Тогда*

$$[\mathrm{GL}(n, K), \mathrm{GL}(n, K)] = [\mathrm{SL}(n, K), \mathrm{SL}(n, K)] = \mathrm{SL}(n, K).$$

Доказательство. 1) Ясно, что определитель коммутатора $[x, y]$ любых двух матриц $x, y \in \mathrm{GL}(n, K)$ равен 1. Поэтому

$$[\mathrm{SL}(n, K), \mathrm{SL}(n, K)] \leq [\mathrm{GL}(n, K), \mathrm{GL}(n, K)] \leq \mathrm{SL}(n, K).$$

2) В случае $n \geq 3$ достаточно сослаться на предыдущее следствие.

3) Если $n = 2$ и $|K| \geq 4$, то найдется $\epsilon \in K^*$ такое, что $\epsilon^2 \neq 1$. Тогда

$$\left[\begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon^{-1} \end{pmatrix}, \begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & \xi(\epsilon^2 - 1) \\ 0 & 1 \end{pmatrix}.$$

Таким образом, $t_{12}(\xi) \in [\mathrm{SL}(2, K), \mathrm{SL}(2, K)]$, для $t_{21}(\xi)$ проверка аналогична.

Исключенные в этой теореме группы $\mathrm{GL}(2, 2)$ и $\mathrm{GL}(2, 3)$ являются истинными исключениями. В самом деле, $\mathrm{GL}(2, 2) = \mathrm{SL}(2, 2) = S_3$, так что коммутант H этих групп имеет, как мы знаем из пункта 1, порядок 3 и, таким образом, не совпадает с $\mathrm{SL}(2, 2)$. В матрицах H можно представить как

$$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}.$$

С другой стороны, точно так же, как в шаге 3) легко убедиться, что

$$[\mathrm{GL}(2, 3), \mathrm{GL}(2, 3)] = \mathrm{SL}(2, 3)$$

(проверьте это!). Однако в отличие от групп $\mathrm{SL}(2,q)$, $q \geq 4$, группа $\mathrm{SL}(2,3)$ не является совершенной. Чтобы убедиться в этом, рассмотрим следующую подгруппу $H \leq \mathrm{SL}(2,3)$:

$$H = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}.$$

Задача. Докажите, что $[\mathrm{SL}(2,3), \mathrm{SL}(2,3)] = H$.

Решение. Несложно проверить, что $H \trianglelefteq \mathrm{SL}(2,3)$, для этого достаточно убедиться в том, что H нормализуется элементарными матрицами. Но тогда фактор-группа $\mathrm{SL}(2,3)/H$ имеет порядок 3 и, следовательно абелева. Это значит, что коммутант $\mathrm{SL}(2,3)$ содержится в H. Для доказательства обратного включения достаточно вычислить коммутатор $[t_{12}(\xi), t_{21}(\zeta)]$.

Теорема. *Предположим, что K, $|K| \geq 2$, – поле. Тогда*

$$[B(n,K), B(n,K)] = U(n,K).$$

§ 3. Теорема Оре, проблема Оре

В предыдущем параграфе мы доказали, что группа A_n, $n \geq 5$, совершенна, иными словами, что каждый элемент A_n является произведением коммутаторов. Однако в действительности имеет место гораздо более точное утверждение.

Теорема Оре. *При $n \geq 5$ каждый элемент группы A_n является коммутатором.*

Доказательство.

Проблема Оре. *Верно ли, что каждый элемент неабелевой конечной простой группы является коммутатором.*

Почти для всех конечных простых групп известно, что ответ на этот вопрос положителен.

§ 4. Не каждый элемент коммутанта является коммутатором
1st instalment

Здесь мы воспроизводим *замечательный* пример Филлис Кассиди[204], показывающий, что, вообще говоря, коммутант не только не совпадает с множеством коммутаторов, но и не имеет относительно этого множества **конечной ширины**. Иными словами, существует группа G такая, что *для любого* $n \in \mathbb{N}$ найдется элемент $x \in [G,G]$, который никакими силами нельзя записать как произведение менее, чем n коммутаторов.

1. Пример Кассиди. Пусть K – произвольное поле, x и y независимые переменные над K. Рассмотрим следующую подгруппу G в $\mathrm{GL}(3, K[x,y])$:

$$\begin{pmatrix} 1 & K[x] & K[x,y] \\ 0 & 1 & K[y] \\ 0 & 0 & 1 \end{pmatrix}.$$

Следующее утверждение почти очевидно.

[204] P.J.Cassidy, Products of commutators are not always commutators: an example. – Amer. Math. Monthly, 1979, vol.86, p.772.

Лемма 1. *Коммутант группы G совпадает с*

$$\begin{pmatrix} 1 & 0 & K[x,y] \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Доказательство. Ясно, что $[G,G]$ содержится в этой группе. С другой стороны, из коммутационной формулы Шевалле следует, что $[t_{12}(ax^i), t_{23}(y^j)] = t_{13}(ax^iy^j)$ а, так как $t_{13}(y)t_{13}(z) = t_{13}(y+z)$, то любая матрица $t_{13}(h)$, $h \in K[x,y]$, лежит в $[G,G]$.

Обозначим теперь для краткости

$$m(f,g,h) = \begin{pmatrix} 1 & f & h \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$$

Следующее утверждение проверяется непосредственным вычислением.

Лемма 2. *Коммутаторы в группе G имеют вид*

$$[m(f_1,g_1,*), m(f_2,g_2,*)] = m(0,0,f_1g_2 - f_2g_1)$$

для некоторых $f_1, f_2 \in K[x]$, $g_1, g_2 \in K[y]$.

Теорема. *Не каждый элемент $[G,G]$ является коммутатором.*

Доказательство. Покажем, что $z = m(0,0,1+xy+x^2y^2) \in [G,G]$ не может быть коммутатором. В самом деле, если z коммутатор, то найдутся такие многочлены $f_1, f_2 \in K[x]$, $g_1, g_2 \in K[y]$, что $f_1g_2 - f_2g_1 = 1 + xy + x^2y^2$. Пусть $f_1 = a_0 + a_1x + a_2x^2 + \ldots$, $f_2 = b_0 + b_1x + b_2x^2 + \ldots$, где $a_i, b_i \in K$. Сравнивая в равенстве $f_1g_2 - f_2g_1 = 1 + xy + x^2y^2$ коэффициенты при $1, x, x^2$, мы видим, что

$$a_0g_2 - b_0g_1 = 1, \qquad a_1g_2 - b_1g_1 = y, \qquad a_2g_2 - b_2g_1 = y^2,$$

и теперь из теоремы Штейница вытекает, что $1, y, y^2$ линейно зависимы. Противоречие.

Следствие из доказательства. *Ширина $[G,G]$ по отношению к коммутаторам неограничена.*

Доказательство. Тем же методом, что и выше, можно показать, что трансвекцию $t_{13}(1 + xy + \ldots + x^ny^n)$ нельзя представить как произведение меньше, чем $\lfloor \frac{n+1}{2} \rfloor$ коммутаторов.

2. Вариация Ротмана. Пример Кассиди можно модифицировать следующим образом. Возьмем этом примере $K = \mathbb{F}_p$ и заменим $K[x,y]$ на $K[x,y]/I$, где $I = (x^3, x^2y, xy^2, y^3)$ – идеал, порожденный третьими степенями. Это приводит к примеру группы порядка p^{12}, для которой коммутант не совпадает с множеством коммутаторов. В самом деле, в матрицах из этого примера в позиции $(1,2)$ стоят линейные комбинации $1, x, x^2$, в позиции $(2,3)$ – линейные комбинации $1, y, y^2$, и, наконец, в позиции $(1,3)$ – линейные комбинации $1, x, y, x^2, xy, y^2$. Убедитесь в том, что этого хватает, чтобы провести рассуждение из доказательства теоремы Кассиди.

3. Длинные коммутаторы. Однако, возникающая у многих начинающих иллюзия, что каждый элемент коммутанта есть коммутатор, имеет под собой материальный субстрат.

Задача. Показать, что коммутант $[G,G]$ совпадает с множеством

$$\{g_1\dots g_n g_1^{-1}\dots g_n^{-1} \mid n\in\mathbb{N}, g_i\in G\}$$

длинных коммутаторов.

Решение. Прежде всего, проверим, что все длинные коммутаторы действительно лежат в коммутанте, т.е. представимы в виде произведения обычных коммутаторов. Это делается при помощи стандартного **трюка накопления** alias **трюка Абеля**:

$$g_1g_2\dots g_ng_1^{-1}g_2^{-1}\dots g_n^{-1}=[g_1,g_2\dots g_n][g_2,g_3\dots g_n]\dots[g_{n-1},g_n].$$

Конечно, в курсе анализа при суммировании рядов вы видели этот трюк с накоплением слева направо, а не справа налево, как у нас, но это потому, что наше умножение некоммутативно! В следующем параграфе мы напомним, в чем состоит обычный коммутативный трюк Абеля и приведем еще одно важное приложение.

Проверка того, что любой элемент коммутанта является длинным коммутатором, по сути еще проще. Для этого запишем обычный коммутатор как длинный коммутатор:

$$[h,g^{-1}]=h(g^{-1}h^{-1})g=h(g^{-1}h^{-1})gh^{-1}(g^{-1}h^{-1})^{-1}g^{-1}.$$

Обратите внимание, что **фанфрелюшка** (pendant – варианты перевода на выбор: побрякушка, подвеска, висюлька) $h^{-1}(g^{-1}h^{-1})^{-1}g^{-1}$, которую мы дописали, чтобы придать коммутатору нужную форму, просто равна 1 сама по себе. Теперь уже совершенно ясно, как поступать в общем случае: по определению любой элемент коммутанта имеет вид

$$[h_1,g_1^{-1}]\dots[h_n,g_n^{-1}]=h_1(g_1^{-1}h_1^{-1})g_1\dots h_n(g_n^{-1}h_n^{-1})g_n$$

для некоторого $n\in\mathbb{N}$ и некоторых $h_i,g_i\in G$. Осталось просто дописать после g_n фанфрелюшки ко всем входящим сюда коммутаторам. Все фанфрелюшки равны 1, но их дописывание придаст нашему выражению вид длинного коммутатора.

§ 5. Не каждый элемент коммутанта является коммутатором
2nd instalment

Сейчас мы построим целый класс примеров *конечных* групп, для которых коммутант не совпадает с множеством коммутаторов[205,206].

1. Низкий старт. Следующая лемма почти очевидна.

Лемма. *Если G – группа такая, что $|G:C(G)|^2<|[G,G]|$, то в $[G,G]$ есть элементы, которые не являются коммутаторами.*

Доказательство. Положим $n=[G:C(G)]$. Ясно, что если $h,g\in G$, $a,b\in C(G)$, то $[xa,yb]=[x,y]$. Поэтому любой коммутатор равен одному из n^2 коммутаторов вида $[x,y]$, где x,y пробегают систему представителей X смежных классов G по $C(G)$.

Таким образом, нам нужно построить группу с очень большим центром и достаточно большим коммутантом. Оказывается, такие группы существуют уже среди p-групп класса 2. Группа G называется **группой класса 2**, если $[G,G]\le C(G)$ (см. § ?).

Лемма. *Для групп класса 2 коммутатор билинеен, иными словами,*

$$[xy,z]=[x,z][y,z],\qquad [x,yz]=[x,y][x,z],$$

для любых $x,y,z\in G$.

[205]I.M.Isaacs, Commutators and the commutator subgroup. – Amer. Math. Monthly, 1977, vol.84, p.720–722.

[206]I.D.Macdonald, Commutators and their products. – Amer. Math. Monthly, 1986, June–July, p.440–444.

Доказательство. Проверим, например, первую из этих формул, доказательство второй совершенно аналогично. В самом деле, так как $[y,z]\in C(G)$, то

$$[xy,z]=(xy)z(xy)^{-1}z^{-1}=x(yzy^{-1}z^{-1})zx^{-z}z^{-1}=[x,z][y,z].$$

Задача. Докажите, что в группе класса 2

$$(xy)^n=x^ny^n[x,y]^{n(n-1)/2}.$$

2. Плодотворная дебютная идея. Предположим, что G группа класса 2 с n образующими $x_1,\dots,x_n$. Тогда любые элементы y,z этой группы имеют вид

$$y=x_1^{h_1}\dots x_n^{h_n}a,\qquad z=x_1^{k_1}\dots x_n^{k_n}b,$$

где $h_i,k_i\in\mathbb{N}_0$, $a,b\in C(G)$, так что по лемме 2 их коммутатор равен

$$[y,z]=\prod_{i<j}[x_i,x_j]^{h_ik_j-h_jk_i}.$$

Иными словами, коммутатор $[G,G]$ порождается $n(n-1)/2$ элементами $[x_i,x_j]$, $i<j$. Вообще говоря, эти коммутаторы не обязаны быть независимыми, однако сейчас мы построим пример n-порожденной матричной группы, в которой $[G,G]$ не порождается менее, чем $n(n-1)/2$ элементом. В этой группе все коммутаторы $[x_i,x_j]$, $i<j$, обязаны быть независимыми. Если дополнительно предполагать, что порядок всех образующих $x_1,\dots,x_n$ равен p, то индекс $C(G)$ не превосходит p^n, в то время как порядок коммутанта равен $p^{n(n-1)/2}$. Так как при $n\geq 6$ выполняется неравенство $2n<n(n-1)/2$, то мы оказываемся в ситуации описанной в лемме 1 и можем утверждать, что в $[G,G]$ найдутся элементы, не являющиеся коммутаторами.

Итак, нам остается построить p-группу класса 2, порожденную n элементами $x_1,\dots,x_n$ порядка p, в которой все коммутаторы $[x_i,x_j]$, $i<j$, независимы. В следующем пункте мы дадим конструкцию такой группы G в подходящей полной линейной группе $\mathrm{GL}(m,p)$ над полем $\mathbb{F}_p$ из p элементов. В действительности, G будет уже подгруппой группы $U(m,p)$ верхних унитреугольных матриц.

3. Матричная конструкция. Сейчас мы завершим построение конечной группы, в которой коммутант не совпадает с коммутатором. Наш наименьший пример имеет порядок 2^{21} – это связано исключительно с нашим методом доказательства, в действительности, как мы уже упоминали, пример Файта имел порядок 2^8 и это и будет в точности подгруппа, получающаяся из нашей конструкции при $n=4$.

Теорема. *Для любого n существует подгруппа $G=G_n$ в $U(m,p)$ класса 2, порожденная n матрицами порядка p, такая что $[G,G]$ является элементарной абелевой группой порядка $p^{n(n-1)/2}$. В частности, при любом $n\geq 6$ не каждый элемент $[G,G]$ является коммутатором.*

Доказательство. Мы приведем конструкцию группы $G=G_6$ как подгруппы в $\mathrm{GL}(28,p)$ оставляя читателю обобщение этой конструкции на произвольное n в качестве несложного упражнения. Положим

$$\begin{aligned}
x_1&=t_{12}(1),\\
x_2&=t_{23}(1)t_{89}(1),\\
x_3&=t_{24}(1)t_{9,10}(1)t_{15,16}(1),\\
x_4&=t_{25}(1)t_{9,11}(1)t_{16,17}(1)t_{20,21}(1),\\
x_5&=t_{26}(1)t_{9,12}(1)t_{16,18}(1)t_{21,22}(1)t_{24,25}(1),\\
x_6&=t_{27}(1)t_{9,14}(1)t_{16,19}(1)t_{21,23}(1)t_{25,26}(1)t_{27,28}(1),
\end{aligned}$$

Сслыка на коммутационную формулу Шевалле из § 2 (или непосредственное вычисление!) показывает, что $[x_1,x_i]=t_{1,i+1}(1)$ для $i=2,3,4,5,6$; $[x_2,x_i]=t_{8,i+7}(1)$ для $i=3,4,5,6$; $[x_3,x_i]=t_{16,i+13}(1)$ для $i=4,5,6$; $[x_4,x_i]=t_{21,i+17}(1)$ для $i=5,6$ и, наконец, $[x_5,x_6]=t_{24,26}(1)$. Еще одна ссылка на коммутационную формулу Шевалле показывает, что каждая из 15 получающихся трансвекций коммутируют со всеми x_i, так что G действительно имеет класс 2 и, значит, центр в ней имеет индекс p^6. Так как 15 матричных единиц

$$e_{13},e_{14},e_{15},e_{16},e_{17},e_{8,10},e_{8,11},e_{8,12},e_{8,13},e_{15,17},e_{15,18},e_{15,18},e_{20,22},e_{20,23},e_{24,26}$$

попарно коммутируют и линейно независимы, то порядок коммутанта $[G,G]$ равен p^{15}. Поскольку $p^{12}<p^{15}$, нам остается сослаться на лемму 1.

§ 6. Трюк Абеля, метод Шрайера

Сейчас мы напомним, в чем состоит обычный коммутативный **трюк Абеля**, часто называемый также **трюком накопления** (summing up).

1. Лемма Абеля. Вот коммутативная версия трюка накопления. Пусть R ассоциативное кольцо. Следующее утверждение очевидно.

Лемма Абеля. *Пусть* $a_1, \dots, a_n, b_1, \dots, b_n \in R$. *Тогда*

$$\begin{aligned} a_1b_1 + \dots + a_nb_n =& a_1(b_1 - b_2) + (a_1 + a_2)(b_2 - b_n) + \dots \\ &+ (a_1 + \dots + a_{n-1})(b_{n-1} - b_n) + (a_1 + \dots + a_n)b_n. \end{aligned}$$

Этот прием оказывается особенно полезным когда $a_1 + \dots + a_n = 0$, потому что при этом вдруг выясняется, что $a_1b_1 + \dots + a_nb_n$ лежит в левом идеале, порожденном разностями $b_i - b_j$

2. Метод Шрайера. А вот чуть менее очевидный вопрос: пусть группа G конечно порождена и $H \leq G$ – подгруппа конечного индекса. Будет ли H конечно порождена. Ответ на этот вопрос легко дать при помощи **метода Шрайера**, основанного на некоммутативной версии того же трюка.

Пусть $X \subseteq G$ – порождающее множество группы G, а Y – система представителей левых смежных классов G по H, т.е. $G = HY$, причем если $Hy_1 = Hy_2$ для $y_1, y_2 \in Y$, то $y_1 = y_2$. Будем считать, что $H \cap Y = \{1\}$. Рассмотрим проекцию $G \longrightarrow Y$, $g \mapsto \overline{g}$, которая каждому $g \in G$ сопоставляет тот единственный $\overline{g} \in Y$, для которого $H\overline{g} = Hg$. По нашему соглашению относительно представителя H для любого $h \in H$ имеем $\overline{h} = 1$.

Теорема Шрайера. *Группа* H *порождается множеством*

$$Z = \{(yx)(\overline{yx})^{-1} \mid y \in Y, x \in X\}.$$

Доказательство. Так как $Hyx = H\overline{yx}$, все эти элементы действительно лежат в H. Для доказательства того, что они порождают H заметим, прежде всего, что, так как $H\overline{g}_1g_2 = Hg_1g_2$, то $\overline{\overline{g}_1g_2} = \overline{g_1g_2}$ для любых $g_1, g_2 \in G$. Кроме того, так как $\overline{\overline{xy^{-1}}y} = \overline{xy^{-1}y} = \overline{x} = x$, то $yx^{-1}(\overline{yx^{-1}})^{-1} = (\overline{xy^{-1}}y)\left(\overline{\overline{xy^{-1}}y}\right)^{-1}$, то элемент вида $(yx^{-1})(\overline{yx^{-1}})^{-1}$, где $y \in Y$, $x \in X$, можно переписать в виде $(y'x)(\overline{y'x})^{-1}$, для подходящего $y' \in Y$, так что без потери общности можно считать, что $X = X^{-1}$, множество Z при этом не изменится. Теперь взяв какое-то выражение $h = x_1 \dots x_l$ элемента $h \in H$ через образующие $x_1, \dots, x_l \in X$, и вспоминая, что $\overline{x_1 \dots x_l} = \overline{h} = 1$, мы можем воспользоваться трюком накопления и переписать это выражение для h в виде

$$\begin{aligned} h = \left(1x_1(\overline{1x_1})^{-1}\right)\left(\overline{x_1}x_2(\overline{x_1x_2})^{-1}\right)\left(\overline{x_1x_2}x_3(\overline{x_1x_2x_3})^{-1}\right)\dots \\ \left(\overline{x_1\dots x_{l-1}}x_l(\overline{x_1\dots x_l})^{-1}\right), \end{aligned}$$

где все сомножители в правой части принадлежат Z.

Пусть $\mathrm{gen}(G)$ обозначает **минимальное число образующих** группы G. Например, $\mathrm{gen}(G) = 1$ означает, что группа G циклическая, $\mathrm{gen}(G) = 2$ означает, что группа может быть порождена двумя элементами, но при этом не является циклической и т.д. Выше мы уже пользовались тем, что $\mathrm{gen}(E_{p^n}) = n$.

Следствие. *Пусть* $H \leq G$. *Тогда* $\mathrm{gen}(H) \leq |G : H| \mathrm{gen}(G)$. *В частности, подгруппа конечного индекса в конечно порожденной группе сама является конечно порожденной.*

§ 7. Тождества с коммутаторами

В этом параграфе мы рассматриваем $(x, y) \mapsto [x, y]$ как новую бинарную операцию на группе G. В действительности, в здесь мы изучаем группу как множество с **двумя** бинарными операциями, умножения и коммутирования (или

умножения и сопряжения) и интересуемся **тождествами**, связывающими эти операции.

1. Кратные коммутаторы. Как мы знаем, непосредственно из определения вытекает, что операция коммутирования **антикоммутативна** в том смысле, что $[x,y]^{-1}=[y,x]$. Однако за крайне редкими исключениями (такими как, скажем, абелевы группы) операция коммутирования *неассоциативна*, так что, вообще говоря, $[[x,y],z]\neq[x,[y,z]]$.

Выражения, которые можно составить из элементов $x_1,\dots,x_n\in G$ применением коммутирования, называются **сложными коммутаторами** или **высшими коммутаторами** (higher commutators). Например, как мы знаем из Главы 1, из четырех элементов $x,y,z,w\in G$ можно составить 5 сложных коммутаторов $[[[x,y],z],w]$, $[[x,[y,z]],w]$, $[[x,y],[z,w]]$, $[x,[[y,z],w]]$, $[x,[y,[z,w]]]$. Обычно мы будем пользоваться **левонормированными сложными коммутаторами**, который будет называться **кратными коммутаторами** и обозначаться одной парой скобок, так что **тройной коммутатор** $[x,y,z]$ следует понимать как $[[x,y],z]$. Точно так же, $[x,y,z,w]=[[[x,y],z],w]$, и вообще,

$$[x_1,\dots,x_{n-1},x_n]=[[x_1,\dots,x_{n-1}],x_n].$$

2. Аналогия групп с алгебрами Ли. Читатель, наверное обратил внимание, что коммутатор в группах и в алгебрах Ли обозначается одинаково. Однако в математике **не бывает** совпадений. Математика – это царство необходимости. Даже самое поверхностное и случайное на вид совпадение **всегда** выражает более глубокую аналогию и математик это тот, кто может превратить аналогию в точное утверждение.

Группа с операциями умножения и коммутирования аналогична кольцу Ли с операциями сложения и коммутирования, только умножение в группе некоммутативно. Являясь значительно более простым объектом, чем группы (сложение коммутативно!), алгебры Ли служат одним из основных инструментов при изучении групп, причем как групп с дополнительной структурой (группы Ли, алгебраические группы, и т.д.), так и абстрактных групп. Применение алгебр Ли к абстрактным группам было начато в конце 30-х годов Эрнстом Виттом, Филиппом Холлом, Гансом Цассенхаузом и Вильгельмом Магнусом. Огромный вклад в развитие этого направления внесли русские математики, в особенности, Алексей Иванович Кострикин и Ефим Исаакович Зельманов.

Задача. Пусть G группа с абелевым коммутантом $[G,G]$. Докажите, что тогда в G выполняется тождество Якоби

$$[[x,y],z]\,[[y,z],x]\,[[z,x],y]=1.$$

Если, кроме того, $[x,z]=1$, то $[[x,y],z]=[x,[y,z]]$.

3. Аналоги тождеств дистрибутивности. Руководствуясь этим мы будем искать тождества для коммутирования в группе, аналогичные тождествам для коммутирования в алгебрах Ли. Разумеется, теперь порядок сомножителей имеет значение, так что в некоторых тождествах придется заменить элементы на их сопряженные. Вот два важнейших тождества. являющихся аналогами тождеств дистрибутивности.

Предложение. *Для любых трех элементов $x, y, z \in G$ имеют место равенства*

$$[xy, z] = {}^x[y, z] \cdot [x, z] \qquad [x, yz] = [x, y] \cdot {}^y[x, z]$$

Доказательство. Проверка этих тождеств, как и всех последующих, может быть произведена расписыванием всех входящих в них коммутаторов непосредственно по определению с последующим сокращением подвыражений вида xx^{-1} и $x^{-1}x$.

Часто бывает удобно переписать эти тождества используя тройные коммутаторы:

$$[xy, z] = [y, z][z, y, x][x, z],$$

$$[x, yz] = [x, y][x, z][z, x, y].$$

Мы видим, что **по модулю тройных коммутаторов** коммутирование уже в обычном смысле дистрибутивно относительно умножения.

Задача. Напишите выражение для $[xy, zw]$ через коммутаторы $[x, z]$, $[x, w]$, $[y, z]$, $[y, w]$.

Отметим еще два следствия антикоммутативности:

$$[x^{-1}, y] = [y, x]^x, \qquad [x, y^{-1}] = [y, x]^y$$

Задача. Проверьте, что $[x, {}^y z] = [x, y]^y [x, z]^{yz} [x, y^{-1}]$. Напишите аналогичную формулу для $[{}^x y, z]$.

4. Тождества Холла-Витта. Теперь мы хотим найти аналог тождества Якоби. Расписывая все тройные коммутаторы, входящие в тождество Якоби, получаем

$$[x, y, z][z, x, y][y, z, x] = [x, y]^z [y, x][z, x]^y [x, z][y, z]^x [z, y].$$

что, вообще говоря, отлично от 1. Витт переписал это тождество как

$$[x, y, z][z, x, y][y, z, x] = [x, y][z, y]^y [z, x][y, x]^x [y, z]^y [x, z][y, z]^x [z, y].$$

А вскоре Холл заметил, что тождеству Витта можно придать следующую более симметричную форму. Следующий некоммутативный аналог тождества Якоби – это знаменитое **тождество Холла**, один из наиболее полезных фактов всей элементарной теории групп:

$$[x, y, {}^y z][y, z, {}^z x][z, x, {}^x y] = 1.$$

Иногда это тождество также называют **тождеством Витта**[207]. В действительности, обычно удобнее пользоваться этим тождеством в такой форме, когда сопряжение вынесено за знак коммутатора, и мы будем называть получающееся тождество **тождеством Холла-Витта**

Лемма Холла–Витта. *Для любых $x, y, z \in G$ имеет место равенство*

$$[x, y^{-1}, z^{-1}]^x [z, x^{-1}, y^{-1}]^z [y, z^{-1}, x^{-1}]^y = 1.$$

Доказательство. Мы оставляем читателю в качестве упражнения расписать тройные коммутаторы в левой части и убедиться, что все сокращается.

[207] Х.Нейман, Многообразия групп, М., Мир, 1969, 264с.

§ 8. Взаимный коммутант, лемма о трех подгруппах

Для дальнейших приложений нам нужно обобщить понятие коммутанта.

1. Взаимный коммутант Пусть $F, H \leq G$ – подгруппы в H. Тогда их **взаимным коммутантом** называется подгруппа, порожденная всевозможными коммутаторами $[f, h]$, где $f \in F$, $h \in H$:

$$[F, H] = \langle [f, h], f \in F, h \in H \rangle.$$

Ясно, что $[F, H] = [H, F]$, так что взаимный коммутант не зависит от порядка подгрупп. Взаимный коммутант двух подгрупп может оказаться значительно больше, чем каждая из них.

Задача. Докажите, что для любого ассоциативного кольца с 1 и любого $n \geq 3$ имеем

$$[U(n, R), U^-(n, R)] = E(n, R).$$

Легко видеть, что подгруппа $H \leq G$ в том и только том случае нормальна в G, когда $[H, G] \leq H$.

Лемма. *Для любых подгрупп $F, H \leq G$ имеем*

$$[F, H], F[F, H], H[F, H] \trianglelefteq \langle F, H \rangle.$$

Доказательство. Пусть $f \in F$, $h \in H$. Мы хотим показать, что для любого $g \in \langle F, H \rangle$ элемент $g[f, h]g^{-1}$ снова можно представить в виде произведения коммутаторов из $[F, H]$. Очевидно, достаточно проверять это для какой-то системы образующих группы $\langle F, H \rangle$. Для этого в случае $g \in F$ достаточно воспользоваться формулой $g[f, h]g^{-1} = [gf, h][h, g]$, а в случае $g \in H$ – формулой $g[f, h]g^{-1} = [g, f][f, gh]$. Это показывает нормальность $[F, H]$, нормальность двух других подгрупп сразу отсюда следует.

Следствие. *Для любой подгруппы $H \leq G$ имеем $[H, G] \trianglelefteq G$.*

Задача. Пусть $F \leq H \leq G$, $F \trianglelefteq G$. Тогда $[H, G] \leq F$ в том и только том случае, когда $H/F \leq C(G/F)$.

Задача. Докажите, что если $F, H \trianglelefteq G$, то $[F, H] \trianglelefteq G$. Если F и H – (вполне) характеристические, то и $[F, H]$ – (вполне) характеристическая.

Задача. Докажите, что если $F, H, K \trianglelefteq G$, то

$$[FH, K] = [F, K][H, K], \qquad [F, HK] = [F, H][F, K].$$

Задача. Предположим, что $G = FH$, причем $H \trianglelefteq G$. Докажите, что тогда $[G, G] = [F, F][G, H]$.

Задача. Предположим, что $G = FH$, причем $F, H \trianglelefteq G$. Докажите, что тогда $[G, G] = [F, F][F, H][H, H]$.

2. Лемма о трех подгруппах. Пусть теперь $A, B, C \leq G$. Как и выше, мы положим $[A, B, C] = [[A, B], C]$. Следующий простой результат является одним из самых полезных инструментов всей элементарной теории групп.

Лемма о трех подгруппах. *Пусть $A, B, C \in G$, а $H \trianglelefteq G$. Тогда если две из трех подгрупп $[A, B, C]$, $[B, C, A]$, $[C, A, B]$ содержатся в H, то третья тоже содержится в H.*

Доказательство. Сразу вытекает из тождества Холла-Витта.

Приведем пример использования этой леммы. Пусть R – ассоциативное кольцо с 1, $C(n, R)$ – центр полной линейной группы $\mathrm{GL}(n, R)$, состоящий из всех скалярных матриц ϵe, где $\epsilon \in C(R)$.

Предложение. *Предположим, что $n \geq 3$. Если $g \in \mathrm{GL}(n, R)$ выполнено включение $[E(n, R), g] \leq C(n, R)$, то $g \in C(n, R)$.*

Доказательство. Заметим, прежде всего, что матрица g коммутирующая с $E(n, R)$ центральна, для этого достаточно рассмотреть коммутаторы $[t_{ij}(\xi), g]$ для $1 \leq i \neq j \leq n$, $\xi \in R$. По предположению

$$[g, E(n, R), E(n, R)] = [E(n, R), g, E(n, R)] = 1.$$

Из того, что группа $E(n, R)$ совершенна (§ 2) и леммы о трех подгруппах, вытекает, что

$$[E(n, R), g] = [E(n, R), E(n, R), g] = 1,$$

но это, как мы только что заметили, и значит, что матрица g центральна.

§ 7. Теорема Шура

Мы уже упоминали общий принцип, что чем больше центр группы, тем меньше ее коммутант и наоборот. Сейчас мы докажем одну из замечательных классических теорем, придающих точный количественный смысл этому утверждению.

Теорема Шура. *Если $|G : C(G)| < \infty$, то $|[G, G]| < \infty$.*

Доказательство Орнштейна. ([Ro], стр.114) Пусть $g_1, \ldots, g_n$ – представители смежных классов G по $C(G)$. Представим элементы $x, y \in G$, в виде $x = g_i a$, $y = g_j b$, где $a, b \in C(G)$. Тогда $[x, y] = [g_i a, g_j b] = [g_i, g_j]$. Тем самым, всего имеется не более n^2 коммутаторов.

Ясно, что каждый элемент $g \in [G, G]$ можно записать в виде $h_1, \ldots h_m$, где h_i коммутатор. Среди всех записей g в таком виде выберем такую, для которой m наименьшее возможное. Сейчас мы покажем, что $m < n^3$. Прежде всего, индукцией по r убедимся в том, что для любых $x, y \in G$ имеем $[x, y]^r = (xy)^r (x^{-1}y^{-1})^r u$, где u – произведение $r - 1$ коммутатора. Для $r = 1$ это очевидно. Для индукционного шага заметим, что $xy = yx[x^{-1}, y^{-1}]$. Таким образом, для $r > 1$ имеем

$$[x, y]^{r+1} = xyx^{-1}y^{-1}[x, y]^r = xy(x^{-1}y^{-1})(xy)^r(x^{-1}y^{-1})^r u = xy(xy)^r(x^{-1}y^{-1})^r(x^{-1}y^{-1})hu = (xy)^{r+1}(x^{-1}y^{-1})^{r+1}hu$$

для некоторого коммутатора h, что и утверждалось.

Вспомним, что из $|G : C(G)| = n$ следует, что $z^n \in C(G)$ для любого $z \in G$. Тем самым, из $yx = x^{-1}(xy)x$, вытекает, что $(yx)^n = x^{-1}(xy)^n x = (xy)^n$. Но это значит, что $(x^{-1}y^{-1})^n = ((yx)^{-1})^n = ((yx)^n)^{-1} = ((xy)^n)^{-1}$. В силу доказанного в предыдущем абзаце, $[x, y]^n$ является произведением $n - 1$ коммутаторов.

С другой стороны, $xyx = (xyx^{-1})x^2$, так что два вхождения x можно собрать вместе, заменив y на его сопряженный. Выразим $g \in [G, G]$ как произведение $g = h_1 \ldots h_m$ коммутаторов. Если $m \geq n^3$, то какой-то из коммутаторов появляется $> n$ раз. По последнему замечанию все такие множители можно собрать вместе (при этом остальные клммутаторы заменяются на сопряженные к ним, по прежнему являющиеся коммутаторами), что не меняет количества коммутаторов. Но тогда m можно понизить, противоречие. Это значит, что $m < n^3$.

Задача. Докажите, что если $\mathrm{Aut}(G)$ конечна, то $[G, G]$ конечен.

Тема ?: Нильпотентность и разрешимость: синопсис[208]

Во введении я уже высказывал уюеждение, что теория групп есть теория *простых* групп. Однако в 30-е, 40-е и 50-е годы теория групп в результате утраты веры в светлое будущее теория групп превратилась в теорию *разрешимых* групп. Это касается как теории конечных групп, так и в особенности теории бесконечных групп, где изучение разрешимых групп оказалось *чудовищно* гипертрофированым. Трудность этой теории (как и любой подобной теории!) для начинающего и неспециалиста, состоит в обилии близких понятий и отсутствии ярких контрастов. Поэтому мы ограничимся лишь несколькими наиболее важными классами. в настоящем параграфе мы сопоставим несколько важнейших классов

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[209] принято называть **рядом подгрупп**, при этом n называется **длиной** этого ряда. Если все включения $G_{i-1} < G_i$ являются строгими, то такой ряд называется **рядом без повторений**.

Предостережение. 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.

Ряд подгрупп состоящий из нормальных подгрупп называется **нормальным**. Таким образом, для нормального ряда $G_i \trianglelefteq G$ для всех i. Ряд подгрупп называется **субнормальным**, если $G_{i-1} \trianglelefteq G_i$ для всех i. В частности, субнормальный ряд состоит из субнормальных подгрупп, хотя, конечно, не любой ряд, состоящий из субнормальных подгрупп, субнормален. Ряд подгрупп, состоящий из (вполне) характеристических подгрупп называется **(вполне) характеристическим**.

Предостережение. В некоторых старых книгах **нормальным рядом** называется то, что мы называем субнормальным рядом, то, что мы называем нормальным рядом, называется в этом случае **инвариантным рядом**. Однако эта терминология представляется мне *крайне* неудачной, так как в этом случае членами *нормального* ряда оказываются *субнормальные* подгруппы!

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**

[208] **Синопсис** — общая точка зрения, позволяющая увидеть весь предмет в целом; общий обзор, сводка результатов, конспект; **синоптический** — дающий общий взгляд или общую точку зрения; излагающий общепринятую версию или версию, согласующуюся с другими источниками ('Евангелия от Матфея, Марка и Луки являются синоптическими'); сводный, конспективный, обзорный

[209] В других алгебраических теориях для обозначения аналогичных понятий используются другие термины, например, в теории Галуа принято говорить о **башнях полей**, а в линейной алгебре, теории представлений, дифференциальной, алгебраической и комбинаторной геометрии говорят о **флагах подпространств**.

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.

Разрешимые группы – это группы, которые можно собрать последовательными расширениями или, *что то же самое*, расщепляющимися расширениями из конечного числа *абелевых* кусков. Нильпотентные группы – это группы, которые можно собрать последовательными *центральными* расширениями из конечного числа абелевых кусков. Реже используются варианты разрешимости такие, как полицикличность или сверхразрешимость. А именно, полициклические/сверхразрешимые группы – это группы, которые можно собрать последовательными расширениями/*расщепляющимися* расширениями из конечного числа *циклических* кусков.

Разрешимая группа – группа, обладающая *нормальным* рядом подгрупп с *абелевыми* факторами. Легко проверить, что это условие эквивалентно более слабому условию существования *субнормального* ряда подгрупп с *абелевыми* факторами.

Полициклическая группа – группа, обладающая *субнормальным* рядом подгрупп с *циклическими* факторами.

Сверхразрешимая группа – группа, обладающая *нормальным* рядом подгрупп с *циклическими* факторами.

Нильпотентная группа – группа, обладающая *центральным* рядом подгрупп.

Таким образом, мы получаем следующие пять условий убывающей силы:

$$\text{абелевость} \Longrightarrow \text{нильпотентность} \Longrightarrow \text{сверхразрешимость} \Longrightarrow$$
$$\Longrightarrow \text{полицикличность} \Longrightarrow \text{разрешимость},$$

которые приводят к включениям соответствующих классов групп. Все эти включения являются строгими, и все, *кроме последнего*, продолжают оставаться строгими даже для *конечных* групп:

- Группа Q нильпотентна, но не абелева;
- Группа S_3 сверхразрешима, но не нильпотентна;
- Группа S_4 разрешима, но не сверхразрешима.

Полициклические группы = разрешимые группы с условием максимальности для подгрупп. В частности, для *конечных* групп полицикличность = разрешимость.

Подгруппы и фактор-группы полициклической группы полициклические.

Расширение полициклической группы при помощи полициклической группы полициклично.

Подгруппы и фактор-группы сверхразрешимой группы сверхразрешимы.

Расщепляющееся расширение сверхразрешимой группы при помощи сверхразрешимой группы сверхразрешимо??

§ ?. Нильпотентные группы

Определим **нижний центральный ряд** группы G по индукции следующим образом. Положим $C_0(G) = G$ и $C_n(G) = [C_{n-1}(G), G]$ для $n \geq 1$. Таким образом,

$$C_1(G) = [G, G],$$
$$C_2(G) = [[G, G], G],$$
$$C_3(G) = [[[G, G], G], G],$$

и т.д. Из определения сразу вытекает, что

$$G = C_0(G) \geq C_1(G) \geq C_2(G) \geq \ldots \geq C_n(G) \geq \ldots,$$

Задача. Убедитесь, что этот ряд действительно является **центральным рядом** в обычном смысле, т.е. фактор-группа $C_{n-1}(G)/C_n(G)$ лежит в центре группы $G/C_n(G)$ или, что то же самое, $[G, C_{n-1}(G)] \leq C_n(G)$.

Нижний центральный ряд (`lower central ceries`) известен также под алиасом **убывающий центральный ряд** (`descending central ceries`). Очень часто эпитет **`нижний/убывающий`** здесь опускается и говорят просто о **центральном ряде** *par excellence*. При этом совсем оголтелые групповики-фетишисты[210] советского периода настолько обстоятельно знали по-английски, что истолковывали `central ceries` как **ряд централов**. Вскоре мы определим *верхний* центральный ряд $C^n(G)$ (возрастающий центральный ряд, ряд гиперцентров) и тогда станет ясно, почему построенный выше ряд *естественно* называть *нижним*[211].

Задача. Докажите, что члены нижнего центрального ряда являются вполне характеристическими подгруппами.

Задача. Докажите, что

$$[C_m(G), C_n(G)] \leq C_{m+n}(G).$$

Указание. Воспользуйтесь леммой о трех подгруппах.

Группа G называется **нильпотентной**, если ее нижний центральный ряд за конечное число шагов доходит до единичной подгруппы, иными словами, если найдется такое n, что $\mathrm{C}_n(G) = 1$. Это означает в точности, что группа G удовлетворяет тождеству $[\ldots[x_1, x_2], \ldots, x_n] = 1$ выполнение которого означает, что все левонормированные коммутаторы длины n тривиальны. При этом *наименьшее* n такое, что $\mathrm{C}_n(G) = 1$ называется **классом нильпотентности** группы G. В частности, абелева группа — это в точности нильпотентная группа класса 1, нильпотентная группа класса 2 — это группа, удовлетворяющая тождеству $[[x, y], z] = 1$, и т.д.

Группа $U_m(n, R)$ — множество унитреугольных матриц с m нулевыми наддиагоналями. Иными словами,

$$U_m(n, R) = \{u = (u_{ij}) \in U(n, R) \mid u_{ij} = 0, j - i = 1, \ldots, m\}.$$

[210] 'group theorists simply do it'.

[211] Кроме, конечно, очевидной типографической причины, состоящей в том, что в его обозначении индекс n пишется снизу: чем отличается Гантмахер от Хермандера?

Например,

$$U_2(6,R)=\begin{pmatrix}1&0&0&*&*&*\\0&1&0&0&*&*\\0&0&1&0&0&*\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{pmatrix}$$

Задача. Докажите, что $C_m(U(n,R))=U_m(n,R)$.

Определим **верхний центральный ряд** группы G по индукции следующим образом. Положим $C^0(G)=1$, а для $n\geq 1$ обозначим через $C^n(G)$ полный прообраз центра фактор-группы $G/C^{n-1}(G)$ по предыдущему члену ряда, относительно канонической проекции. Иными словами, $C^n(G)$ это такая подгруппа $C^{n-1}(G)\leq C^n(G)\leq G$, что ее фактор-группа по $C^{n-1}(G)$ совпадает с центром фактор-группы $G/C^{n-1}(G)$:

$$C^n(G)/C^{n-1}(G)=C(G/C^{n-1}(G)).$$

Таким образом, $C^1(G)=C(G)$ – центр группы G, $C^2(G)$ — **гиперцентр**, т.е. такая подгруппа в G, что $C^2(\mathrm{C})/C(G)=C(G/C(G))$ и так далее. Верхний центральный ряд (`upper central ceries`) часто называется также **возрастающий центральным рядом** (`ascending central ceries`), а его член $C^n(G)$ обычно называется также **n-м гиперцентром** группы G.

§ ?. Конечные нильпотентные группы

Нормализаторное условие. *Конечная группа G в том и только том случае нильпотентна, когда $H<N_G(H)$ для любой собственной подгруппы $H<G$.*

Автоморфизм $\varphi\in\mathrm{Aut}(G)$ конечной группы G называется **регулярным**, если у него нет никаких неподвижных элементов, кроме 1: из $\varphi(g)=g$, где $g\in G$, следует, что $g=1$.

Теорема. *Конечная группа, у которой есть регулярный автоморфизм простого нечетного порядка, нильпотентна.*

§ ?. Подгруппа Фиттинга

Следующий результат доказан Фиттингом в 1938 году[212]

Теорема Фиттинга. *Произведение $FH\leq G$ двух нильпотентных нормальных подгрупп $F,H\trianglelefteq G$ является нильпотентной нормальной подгруппой, класс которой не превосходит сумму класса F и класса H.*

Доказательство. Пусть класс F равен r, а класс H равен s. Из § ? мы знаем, что $[FH,FH]=[F,F][F,H][H,H]$. Продолжая действовать по индукции, мы видим, что

$$C_n(FH)=[FH,\dots,FH]=\prod[K_1,\dots,K_{n+1}],$$

[212]H.Fitting, Beiträge zur Theorie der Gruppen endlicher Ordnung. – Jahresberichte Deutsch. Math. Vereinigung, 1938, Bd.48, S.77–141.

где каждая из подгрупп K_i равна F или H. Так как подгруппа $C_m(F)$ является характеристической подгруппой в F, она нормальна в G. В частности, $[C_m(F), H] \leq C_m(F)$. Это значит, что если среди подгрупп K_i по крайней мере $m+1$ штука равны F, то $[K_1, \dots, K_{n+1}]$ содержится в $C_m(F)$. По той же причине, если среди подгрупп K_i по крайней мере $m+1$ штука равны H, то $[K_1, \dots, K_{n+1}]$ содержится в $C_m(H)$. Но ведь каждый длинный коммутатор $[K_1, \dots, K_{n+1}]$, входящий в $C_{r+s}(FH)$, содержит либо по крайней мере $r+1$ подгруппу F, либо о крайней мере $s+1$ подгруппу H. В первом случае такой коммутатор содержится в $C_r(F) = 1$, а во втором случае — в $C_s(H) = 1$. Но это и значит, что $C_{r+s}(FH) = 1$, как и утверждалось.

Определение. *Подгруппа $F(G)$ порожденная всеми нильпотентными нормальными подгруппами, называется* **подгруппой Фиттинга**.

Для конечной группы G подгруппу $F(G)$ можно охарактеризовать как единственную максимальную нильпотентную нормальную подгруппу группы G.

Задача?? Насколько это сложно?? Пусть G конечная группа. Докажите, что $[F(G), F(G) \leq \Phi(G) \leq F(G)$, $F(G)/\Phi(G) = F(G/\Phi(G))$.

§ ?. Разрешимые группы

Определим **производный ряд** группы G по индукции следующим образом. Положим $D_0(G) = G$ и $D_n(G) = [D_{n-1}(G), D_{n-1}(G)]$ для $n \geq 1$. Таким образом,

$$\begin{aligned} D_1(G) &= [G, G], \\ D_2(G) &= [[G, G], [G, G]], \\ D_3(G) &= [[[G, G], [G, G]], [[G, G], [G, G]]], \end{aligned}$$

и т.д. Из определения сразу вытекает, что

$$G = D_0(G) \geq D_1(G) \geq D_2(G) \geq \ldots \geq D_n(G) \geq \ldots,$$

причем все фактор-группы $D_n(G)/D_{n-1}(G)$ абелевы. Обозначение мотивировано тем, что по-английски этот ряд называется `derived series`, впрочем, часто его называют попросту **ряд коммутантов**. Традиционно члены ряда коммутантов обозначались $G \geq G' \geq G'' \geq \ldots \geq G^{(n)} \geq \ldots$

Конфронтация. Весьма поучительно сличить это определение с определением нижнего центрального ряда, которое дано в § ?. Первые два члена обоих рядов совпадают: $D_0(G) = C_0(G) = G$ есть сама группа G, а $D_1(G) = C_1(G) = [G, G]$ — ее коммутант. Однако каждый следующий член производного ряда является коммутантом предыдущего, в то время как член нижнего центрального ряда представляет собой *взаимный* коммутант предыдущего члена с самой группой G. Это значит, что начиная со второго члена эти ряды, вообще говоря, начинают расходиться, причем

$$D_2(G) = [[G, G], [G, G]] \leq [[G, G], G] = C_2(G),$$

и далее по индукции

$$D_n(G) = [D_{n-1}(G), D_{n-1}(G)] \leq [C_{n-1}(G), G] = C_n(G)$$

при всех n.

Задача. Докажите, что члены нижнего центрального ряда являются вполне характеристическими подгруппами.

Группа G называется **разрешимой**, если ее производный ряд за конечное число шагов доходит до единичной подгруппы, иными словами, если найдется такое n, что $D_n(G) = 1$. Это означает в точности, что группа G удовлетворяет тождеству

$$d_n(x_1, x_2, \dots, x_{2^n}) = 1$$

от 2^n переменных. Здесь $d_0(x) = x$, и

$$d_n(x_1, x_2, \dots, x_{2^n}) = [d_{n-1}(x_1, \dots, x_{2^{n-1}}), d_{n-1}(x_{2^{n-1}+1}, \dots, x_{2^n})]$$

для $n \geq 1$. При этом *наименьшее* n такое, что $D_n(G) = 1$ называется **ступенью разрешимости** группы G. В частности, абелева группа — это в точности разрешимая группа ступени 1, разрешимая группа ступени 2 — это группа, удовлетворяющая тождеству $[[x, y], [z, w]] = 1$, и т.д. разрешимые группы ступени 2 называются **метабелевыми**.

Задача. Докажите, что группа G в том и только том случае разрешима, когда выполняется одно из двух следующих эквивалентных условий:

• Группа G обладает *субнормальным* рядом подгрупп с абелевыми факторами. Иными словами, существуют такие подгруппы $G_i \leq G$, что

$$1 = G_n \trianglelefteq G_{n-1} \trianglelefteq \dots \trianglelefteq G_1 \trianglelefteq G_0 = G,$$

а все фактор-группы G_{i-1}/G_i абелевы.

• Группа G обладает *нормальным* рядом подгрупп с абелевыми факторами. Иными словами, существуют такой же ряд подгрупп, что и выше, в котором все G_i являются не просто подгруппами в G, а нормальными делителями.

Задача. Докажите, что класс разрешимых групп замкнут относительно перехода к подгруппам, фактор-группам и расширениям. Иными словами, имеют место следующие три утверждения:

• подгруппа разрешимой группы разрешима: если $H \leq G$ и G разрешима, то H разрешима.

• фактор-группа разрешимой группы разрешима: если $H \trianglelefteq G$ и G разрешима, то G/H разрешима.

• Расширение разрешимой группы при помощи разрешимой группы разрешимо: если $H \trianglelefteq G$, причем как H, так и G/H разрешимы, то G разрешима.

В частности, из последнего из этих утверждений вытекает, что прямое произведение разрешимых групп разрешимо. В действительности, имеет место гораздо более точный факт.

Задача. Докажите, что если $F, H \trianglelefteq G$, причем F, H разрешимы, то группа $FH \leq G$ тоже разрешима.

Решение. В самом деле, по теореме Нетер $FH/F \cong H/(F \cap H)$, причем нормальный делитель $F \trianglelefteq FH$ разрешим по условию, а фактор-группа $H/(F \cap H)$ разрешимой группы H тоже разрешима.

Задача. Докажите, что в конечной группе G, существует наибольший разрешимый нормальный делитель $R(G)$. Фактор-группа $G/R(G)$ полупроста в том смысле, что $R(G/R(G)) = 1$

Решение. В самом деле, из результата предыдущей задачи вытекает, что произведение $R(G)$ всех разрешимых нормальных делителей группы G снова является разрешимым нормальным делителем. Ясно, что любой разрешимый нормальный делитель содержится в $R(G)$. С другой стороны, если бы $G/R(G)$ существовал разрешимый нормальный делитель $H \neq 1$, то его полный прообраз $\pi^{-1}(H)$ относительно канонической проекции $\pi : G \longrightarrow G/R(G)$ был бы разрешимой подгруппой, строго содержащей $R(G)$, что противоречит максимальности $R(G)$.

Предостережение. В теории групп Ли и алгебраических групп радикалом $R(G)$ группы G принято называть наибольший **связный** замкнутый разрешимый нормальный делитель в G. Тем самым, с точки зрения этих теорий радикал любой конечной группы равен 1. Поэтому наибольшая разрешимая нормальная подгруппа в G обозначается через $\mathrm{Sol}(G)$.

Примеры разрешимых групп. Сейчас мы приведем несколько очевидных примеров разрешимых групп.

Следующий пример является самым важным и самым типичным. Интуитивно читатель должен представлять себе разрешимую группу именно как группу верхних треугольных матриц.

Группа верхних треугольных матриц $B(n, R)$ над коммутативным кольцом R разрешима.

Конечные разрешимые группы.

pq-теорема Бернсайда. *Если $|G| = p^m q^n$, где $p, q \in \mathbb{P}$, то группа G разрешима.*

Теорема Томпсона-Фейта. *Конечная группа G нечетного порядка разрешима.*

§ ?. Теорема Колчина–Мальцева

Теорема Колчина–Мальцева. *Пусть K — алгебраически замкнутое поле. Тогда любая разрешимая подгруппа G в $\mathrm{GL}(n, K)$ виртуально триангулируема.*

Иными словами, утверждается, что G содержит триангулируемую подгруппу конечного индекса,

§ ?. Сверхразрешимые группы

Ясно, что каждая подгруппа простого индекса максимальна. Легко построить примеры, показывающие, что обратное, вообще говоря, неверно. Следующий результат отвечает на вопрос о том, в каких группах индекс всех максимальных подгрупп является простым.

Теорема Хупперта. *Конечная группа в том и только том случае сверхразрешима, когда все ее максимальные подгруппы имеют простые индексы.*

Доказательство этой теоремы приведено в [Hu], а на русском языке его можно найти, например, в [KM], гл. VII, § 2.

Коммутант сверхразрешимой группы нильпотентен.

§ ?. Локально нильпотентные группы

Теорема Хирша–Плоткина. *Произведение $FH \leq G$ двух локально нильпотентных нормальных подгрупп $F, H \trianglelefteq G$ является локально нильпотентной нормальной подгруппой.*

§ ?. Локально разрешимые группы

§ ?. Теорема Жордана-Гельдера

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}.

Неуплотняемый нормальный ряд с различными членами называется **главным**. Факторы главного ряда называются **главными факторами** группы G.

Неуплотняемый субнормальный ряд с различными членами называется **композиционным** рядом группы G. Факторы композиционного ряда называются **композиционными факторами** группы G.

Задача. Композиционные факторы являются *простыми* группами.

Задача. Докажите, что каждая конечная группа имеет композиционный ряд.

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.

Задача. Приведите пример бесконечной группы, имеющей композиционный ряд.

Композиционный ряд имеет максимальную возможную длину среди всех рядов с различными членами.

Жордан в 1869 году доказал совпадение порядков факторов композиционного ряда[213], а Гельдер в 1889 году — изоморфизм самих факторов[214].

Теорема Жордана–Гельдера. *Набор композиционных факторов конечной группы не зависит от выбора композиционного ряда.*

Иными словами, утверждается, что любые два композиционных ряда конечной группы имеют одинаковую длину и, после подходящей перестановки, соответствующие факторы изоморфны.

Доказательство.

[213] C.Jordan, Commentaire sur Galois. – Math. Ann., 1869, Bd.1, S.141–160.

[214] O.Hölder, Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen. – Math. Ann., 1889, Bd.34, S.26–56.

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 не обязательно различные простые числа. 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.

Следующий важный результат был доказан Гансом Цассенхаузом в 1934 году[215]. Он известен как **лемма Цассенхауза**, **лемма о бабочке** или, полностью, **лемма Цассенхауза о бабочке**. Почему? Для этого нужно посмотреть на

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

$$F(F^* \cap H^*)/F(F^* \cap H) \cong (F^* \cap H^*)/(F \cap H^*)(F^* \cap H).$$

Сравнение двух этих изоморфизмов и доказывает лемму.

Следующий результат был доказан Отто Шрайером в 1928 году[216]

Теорема Шрайера об уплотнении. *Любые два субнормальных ряда подгрупп обладают эквивалентными уплотнениями.*

---

[215] H.Zassenhaus, Zum Satz von Jordan–Hölder–Schreier. – Abh. Math. Sem. Hamburg, 1934, Bd.11, S.106–108.

[216] O.Schreier, Über den Jordan–Hölderschen Satz. – Abh. Math. Sem. Hamburg, 1928, Bd.6, S.300–302.

Тема ?: СВОБОДНЫЕ ГРУППЫ

§ 1. Определение свободных групп

Ни возможность описать, ни возможность изобразить объект не гарантируют еще его существование.

Рене Магритт

Понятие свободной группы аналогично понятию свободного моноида, свободной абелевой группы, свободного модуля (векторного пространства), кольца многочленов и десяткам других аналогичных конструкций.

Универсальное свойство. Сейчас мы введем одно из основных понятий всей теории групп. Пусть X подмножество группы F.

Определение. *Говорят, что* F **свободно порождается** *множеством* X*, если для любой группы* G *и любого отображения* $\varphi : X \longrightarrow G$ *существует единственный гомоморфизм* $\psi : F(X) \longrightarrow G$*, ограничение которого на* X *совпадает с* φ*. В этом случае группа* F *называется* **свободной группой** *и обозначается* F_X *или* $F(X)$*, а само* X *называется* **свободной системой образующих** *или (реже!)* **базисом** *или* **базой** F*.*

В соответствии с общей философией (commonplace philosophy) свободная группа, порожденная X, если она существует, единственна с точностью до (единственного!) изоморфизма.

Задача. Докажите, что если $F(X)$ и $F(Y)$ свободные группы, свободно порожденные множествами X и Y, а $\varphi : X \longrightarrow Y$ — биекция X на Y, то существует *единственный* изоморфизм $F(X) \longrightarrow F(Y)$, ограничение которого на X совпадает с φ.

В частности, *с точностью до изоморфизма* группа $F(X)$ зависит не от самого множества X, а только от его мощности. Мощность множества X называется **рангом** свободной группы $F(X)$. Часто вместо F_X пишут просто[217] $F_\beth$, где $\beth = |X|$ и говорят об этой группе как о свободной группе ранга $\beth$. В частности для любого $n \in \mathbb{N}_0$ через F_n обозначается свободная группа ранга n, о которой принято говорить также как о **свободной группе с** n **образующими**. Свободная группа со счетным числом образующих обычно обозначается через F_∞. Ясно, что $F_0 = 1$, $F_1 \cong \mathbb{Z}$, существование дальнейших свободных групп уже не столь очевидно. В действительности без дополнительного анализа приведенное определение мало что говорит о свойствах группы $F(X)$ и *ничего* не говорит нам о ее существовании.

Задача. Докажите, что свободная система образующих X действительно порождает группу F_X.

Решение. В самом деле, пусть $H = \langle X \rangle$ — подгруппа, порожденная X. Если предположить, что $H \neq F$, то отображение $X \longrightarrow G = F/H$, переводящее все элементы X в 1, продолжается до гомоморфизма $F \longrightarrow G$ по крайней мере двумя различными образами: до тривиального гомоморфизма 1 и до канонической проекции — *А ведь милиционер и бабочка — это совсем не одно и то же.*

[217] Напомним, что $\beth$ — это вторая буква еврейского алфавита, используемого в иврите, идиш и арамейском. Эта буква называется `бет`, а ее TEX'ническое название `\beth`.

§ 2. Конструкция свободного моноида

1. Свободный моноид. Пусть вначале X — произвольное множество, которое мы будем называть **алфавитом**. Элементы X называются **буквами**. В книге I мы уже построили свободный моноид, порожденный X. Напомним, что свободный моноид — это не моноид, это просто набор слов. Напомним, что **словом** в алфавите X называется любая конечная последовательность букв. При этом не исключается и случай пустой последовательности, называемой также **пустым словом** и обозначаемой Λ (это не греческая буква Λ, а перевернутая буква V, от английского void[218]). Элемент $w \in X^n = X \times \ldots \times X$ рассматривается как **слово** длины $l(w) = n$. При этом когда тупель $w = (x_1, \ldots, x_n)$ рассматривается как слово, то его принято записывать в виде $w = x_1 \ldots x_n$. При такой записи длина слова w это просто количество входящих в него букв. Например, если X — обычный латинский алфавит, то $l(bububu) = 6$. Обозначим через $W(X)$ множество *всех* слов в алфавите X:

$$W(X) = X^0 \sqcup X^1 \sqcup X^2 \sqcup \ldots$$

Здесь $X^0 = \{\Lambda\}$, $X^1 = X$. В дальнейшем, в тем случаях, когда нам нужно будет отличать элементы множества $W(X)$ от более общих *групповых* слов в алфавите X, мы будем называть элементы $W(X)$ **полугрупповыми словами** в алфавите X.

Замечание. Обратите внимание, что во всех обычных ситуациях элементы алфавита X мыслятся как **праэлементы**, которые не имеют никакой дальнейшей структуры. В этом случае множества X^n, $n \in \mathbb{N}_0$, *автоматически* не пересекаются, так что мы могли бы использовать здесь обычное объединение $\cup$, а не дизъюнктное объединение $\sqcup$. Пусть, однако $X = \{x, y, (x, y)\}$. Тогда

$$X^2 = \{(x,x), (x,y), (x,(x,y)), (y,x), (y,y), (y,(x,y)), ((x,y),x), ((x,y),y), ((x,y),(x,y))\}$$

пересекается с X по (x, y). Таким образом, в общем случае только использование $\sqcup$ вместо $\cup$ в определении $W(X)$ гарантирует, что длина слова определена однозначно.

Определим теперь операцию над словами, известную как **конкатенация** (alias **приписывание**) слов. Если w_1 и w_2 два слова, то их **конкатенацией** называется слово $w_1 * w_2$, получающееся приписыванием слова w_2 справа к слову w_1. При этом $l(w_1 * w_2) = l(w_1) + l(w_2)$. Например, если X — обычный русский алфавит, то

кон∗катенация=конка∗тенация=конкате∗нация=конкатенация.

Обычно мы будем записывать конкатенацию как умножение и писать uv вместо $u * v$. Очевидно, что так определенная операция ассоциативна и имеет Λ в качестве нейтрального элемента (приписывание пустого слова к произвольному слову как справа, так и слева не меняет это слово). Таким образом, $W(X)$ превращается в моноид, называемый **свободным моноидом** в алфавите X. Говорят также, что $W(X)$ **свободно порождается** множеством X.

Все элементы этого моноида регулярны, но *ни один из них*, кроме пустого слова, не является обратимым. К этому моноиду применимы все данные выше определения. Например, можно говорить о степенях слов. В частности, $bububu = (bu)^3$. При $|X| \geq 2$ умножение в этом моноиде настолько далеко от коммутативности, насколько это только возможно. Например, $ub \neq bu$ и $(bu)^3 \neq b^3u^3$.

[218] на самом деле, от итальянского vuoto.

§ 3. Конструкция свободной группы

Свободная группа с двумя образующими — это не группа, это просто набор слов.

Анатолий Моисеевич Вершик

1. Групповые слова. Как и в предыдущем параграфе начнем с алфавита X. Создадим свежую копию[219] этого алфавита, которую мы обозначим через X^{-1}. По определению *копия* находится в каноническом биективном соответствии с X, обозначим биекцию X на X^{-1} через $^{-1} : X \longrightarrow X^{-1}$, $x \mapsto x^{-1}$. Таким образом, $X^{-1} = \{x^{-1} \mid x \in X\}$, причем $x^{-1} = y^{-1}$ в том и только том случае, когда $x = y$. Обратная биекция также обозначается через $^{-1} : X^{-1} \longrightarrow X$, по определению, $(x^{-1})^{-1} = x$. *Свежесть* копии означает, что X и X^{-1} дизъюнктны, $X \cap X^{-1} = \varnothing$. Элемент $W(X \sqcup X^{-1})$ называется **групповым словом** в алфавите X. По определению любое групповое слово имеет вид $x_1^{\epsilon_1} \dots x_l^{\epsilon_l}$ для некоторых $x_1, \dots, x_l \in X$ и $\epsilon_i = \pm 1$.

По-прежнему ни один элемент $W(X \sqcup X^{-1})$ не является обратимым, и сейчас для исправления этой ситуации мы введем на множестве групповых слов отношение эквивалентности, которое в дальнейшем будет называться **равенством** групповых слов. При этом рассматривавшееся ранее равенство слов как элементов множества $W(X \sqcup X^{-1})$ будет называться **графическим равенством** и образначаться $w \equiv z$. А именно, пусть $x \in X$. Мы говорим, что слово z получается из слова z **вставкой** фрагмента вида xx^{-1} или $x^{-1}x$, если w можно представить в виде uv так, чтобы $z = uxx^{-1}v$ или $z = ux^{-1}xv$, соответственно. В этом случае говорят, что слово w получается из z **вычеркиванием** фрагмента вида xx^{-1} или $x^{-1}x$. Два слова w и z **элементарно эквивалентны**, если z получается из w вставкой или вычеркиванием фрагмента вида xx^{-1} или $x^{-1}x$ для какой-то буквы $x \in X$. Если слова w и z элементарно эквивалентны, мы пишем $w \approx z$. Отношение эквивалентности $\sim$ определяется как транзитивное замыкание отношения элементарной эквивалентности $\approx$. Иными словами, два слова w и z эквивалентны, если z получается из w конечной цепочкой вставок и вычеркиваний. Временно обозначим эту эквивалентность через $w \sim z$, но после завершения всех необходимых формальностей мы будем писать просто $w = z$. Обозначим класс слова w относительно этой эквивалентности через $[w]$.

Задача. Отношение $\sim$ является конгруэнцией на $W(X \sqcup X^{-1})$. Иными словами, если $u \sim v$ и $w \sim z$, то $uw \sim vz$.

2. Свободная группа. Обозначим через $F(X)$ множество классов эквивалентности $\sim$ на $W(X \sqcup X^{-1})$. Так как $\sim$ является конгруэнцией, то формула $[w][z] = [wz]$ корректно задает умножение классов.

3. Редуцированные слова. В действительности свободную группу несколько удобнее описывать чуть иначе. Слово w называется **редуцированным** (alias **приведенным** или **несократимым**), если оно не содержит фрагментов вида xx^{-1} и $x^{-1}x$.

Теорема. *Каждый класс содержит единственное редуцированное слово.*

[219] Я *без затей* перевожу `fresh copy` как `свежая копия`. Следует иметь в виду, что `fresh` может значить еще `дополнительный`, `только что появившийся`, `только что изготовленный`, `не использовавшийся` , `не бывший в употреблении`.

Доказательство. Существование такого слова очевидно, в самом деле, любое слово наименьшей длины в $[w]$ очевидно является редуцированным. Доказать единственность чуть сложнее. В самом деле, предположим, что w и z суть два эквивалентных редуцированных слова. Эквивалентность означает, что слова w и z можно соединить цепочкой элементарных эквивалентностей $w = w_0 \approx w_1 \approx w_2 \approx \ldots \approx w_l = z$. Если $z \neq w$, то (так как слова редуцированные!) длина l соединяющей их цепочки ≥ 2. Выберем *минимальную* среди всех таких цепочек. Минимальность означает, что, во-первых, эта цепочка имеет наименьшую возможную длину и, во-вторых, что среди всех цепочек наименьшей длины для нашей цепочки сумма длин $l(w_1) + \ldots + l(w_{l-1})$ ее внутренних членов наименьшая возможная. Так как $l(w) < l(w_1)$, $l(z) < l(w_{l-1})$, то найдется такой индекс $1 \leq i \leq l-1$, что $l(w_i) > l(w_{i-1}), l(w_{i+1})$. Это значит, что w_{i-1} получается из w_i вычеркиванием какого-то фрагмента вида xx^{-1} или $x^{-1}x$, а w_{i-1} — вычеркиванием какого-то фрагмента вида yy^{-1} или $y^{-1}y$. Имеет место следующая альтернатива: либо эти фрагменты пересекаются, либо нет. Если они пересекаются, то $w_{i-1} = w_{i+1}$ и мы можем соединить слова w и z более короткой цепочкой элементарных эквивалентностей. С другой стороны, если они не пересекаются, то мы могли бы сначала вычеркнуть фрагмент с y, и только потом врисовать фрагмент с x, получив таким образом соединяющую w и z цепочку с меньшей суммой длин внутренних членов.

Обозначим редуцированное слово в классе $[w]$ слова w через $\rho(w)$. Из предыдущей теоремы вытекает, что $\rho(w)$ есть в точности единственное слово наименьшей длины в классе $[w]$. Ясно, что $\rho(\rho(w)) = w$.

Задача. Докажите, что

$$\rho(wz) \equiv \rho(\rho(w)z) \equiv \rho(w\rho(z)) \equiv \rho(\rho(w)\rho(z)).$$

Предыдущая теорема означает, что мы можем определить $F(X)$ как множество *редуцированных* групповых слов в алфавите X. Следует, однако иметь в виду, что в произведение двух редуцированных слов не является редуцированным, так что умножение редуцированных слов надлежит определяться следующим образом: вначале образовать их обычное произведение как полугрупповых слов, а потом произвести все возможные сокращения, $u * v = \rho(uv)$. В дальнейшем мы объединим точку зрения настоящего пункта с точкой зрения предыдущего пункта. А именно, мы перестаем различать эквивалентные групповые слова и называем их просто **равными**. Тем самым, мы перестаем различать $[w]$ и w. Например, мы пишем $xyx^{-x}xy^{-1} = xyy^{-1} = x$ в том смысле, в котором мы до сих пор писали $[xyx^{-x}xy^{-1}] = [xyy^{-1}] = [x]$ или $xyx^{-x}xy^{-1} \sim xyy^{-1} \sim x$.

§ ?. Классы сопряженных элементов свободной группы

Определим преобразование слов

$$\texttt{RotateLeft[}x_1x_2x_3\ldots x_n\texttt{]} = x_2x_3\ldots x_nx_1.$$

Групповое слово w называется **циклически редуцированным**, если как w, так и `RotateLeft[`w`]` редуцированы. Иными словами, это значит, что слово w не только не содержит фрагментов вида xx^{-1} или $x^{-1}x$, но и не представимо

в форме xzx^{-1} или $x^{-1}zx$ для какого-либо слова z. Например, слово xyx^{-1} является редуцированным, но не циклически редуцированным.

Задача. Докажите, что два слова w и z свободной группы в том и только том случае сопряжены, когда z=`RotateLeft`^{m}`[`w`]` для подходящего m. В частности, в каждом классе сопряженности есть циклически редуцированное слово.

§ ?. Теорема Нильсена–Шрайера

Don't force it, get a larger hammer.

Американская пословица

Сейчас мы увидим нечто совершенно удивительное. А именно, окажется, что каждая подгруппа свободной группы F_n сама свободна, но при этом если $n \geq 2$ ее ранг может оказаться больше n.

Незадача. На странице 121 книги [BB] читателю предлагается доказать, что если $F = F_2$ – свободная группа ранга 2, со свободными образующими x и y, то элементы $x, xy, xy^2, \dots, xy^n$ порождают в F свободную подгруппу H ранга n. Так ли это?

Указание. Это вряд ли.

Brutta ora il mattino.[220]: $xy^2 = (xy)x^{-1}(xy)$. А все потому, что $\langle x, xy\rangle = \langle x, y\rangle = F$.

А вот два исправленных варианта этой задачи.

Задача. Докажите, что если $F = F_2$ – свободная группа ранга 2, со свободными образующими x и y, то $x, yxy, y^2xy^2, \dots, y^nxy^n$ порождают в F свободную подгруппу H ранга $n+1$.

Задача. Докажите, что если $F = F_2$ – свободная группа ранга 2, со свободными образующими x и y, то $x, yxy^{-1}, y^2xy^{-2}, \dots, y^nxy^{-n}$ порождают в F свободную подгруппу H ранга $n+1$.

Указание к обеим задачам. Возьмите приведенное слово в новых образующих и посмотрите на него как на слово в исходных образующих. Происходят ли в нем сокращения, и если да, то где и какие?

Следующий результат был доказан в 1921 году Якобом Нильсеном[221] для конечно порожденных групп и 5 лет спустя Отто Шрайером в общем случае. В работе[222] содержится очень живое изложение биографии Нильсена и его вклада в математику.

Теорема Нильсена-Шрайера. *Подгруппа свободной группы сама свободна.*

Топологическое доказательство. Пусть F – свободная группа со свободной системой образующих X. Пусть, далее, Y – букет окружностей, занумерованных элементами множества X. Тогда F можно истолковать как фундаментальную группу Y. Каждая подгруппа $H \leq F$ является фундаментальной

[220] "А поутру они проснулись."

[221] **Якоб Нильсен**, (15.10.1890, деревня Mjels на острове Альс в Северном Шлезвиге – 03.08.1959, Эльсинор) – крупнейший Датский математик, известный в первую очередь своими работами в области теории групп и топологии, в особенности топологии поверхностей. Кроме теоремы Нильсена-Шрайера центральную роль в комбинаторной теории групп играют преобразования Нильсена и теорема Нильсена об автоморфизмах свободной группы.

[222] V.L.Hansen, Jakob Nielsen (1890–1959). – Math. Intelligencer, 1993, vol.15, N.15, N.4, p.44–53.

группой какого-то накрытия пространства Y. Однако каждое накрытие Y само гомотопно букету окружностей. Но и значит, что H свободна.

Оказывается, ранг подгруппы конечного индекса в свободной группе F_n однозначно определяется ее индексом.

Формула Шрайера. *Если $H \leq F_n$ есть подгруппа конечного индекса, скажем $|F_n : H| = m$, то ранг H равен $1 + (n-1)m$.*

В частности, при $n \geq 2$ ранг любой собственной подгруппы конечного индекса в F_n строго больше ранга самой группы F_n.

Задача. Покажите, что в любой свободной группе множество всех слов четной длины образует подгруппу индекса 2. Что мешает таким же образом построить подгруппу индекса m, взяв в качестве ее элементов все слова длины m?

Задача. Пусть $F_2 = \langle x, y\rangle$ — группа ранга 2 свободно порожденная x и y. Докажите, что в этом случае подгруппа, состоящая из всех слов четной длины, свободно порождена x^2, xy, y^2.

Задача. Пусть $F_2 = \langle x, y\rangle$. Будет ли подгруппа $H = \langle x, y^2\rangle$ иметь конечный индекс в F_2? Напишите бесконечное число слов несравнимых слева по модулю H. Добавьте к подгруппе H еще один элемент g так, чтобы получившаяся подгруппа $G = \langle H, g\rangle$ продолжала оставаться собственной подгруппой, но при этом имела конечный индекс в F_2.

Решение. В самом деле, любые два различных слова, начинающиеся с y несравнимы по модулю H. Поэтому нам нужно добавить какое-то слово g, начинающееся с y (или заканчивающееся y!), скажем, слово yxy^{-1}. Легко видеть, что подгруппа $G = \langle x, y^2, yxy^{-1}\rangle$ имеет индекс 2 в F_2.

Задача. Перепишите формулу Шрайера в таком виде, чтобы она продолжала иметь смысл для случая групп бесконечного ранга и их подгрупп бесконечного индекса.

Свойство Хаусона. Говорят, что группа G обладает **свойством Хаусона**, если пересечение двух конечно порожденных подгрупп свободной группы конечно порождено. Следующий результат утверждает, что свободная группа обладает этим свойством и, в действительности, дает оценку на количество образующих пересечения двух конечно порожденных подгрупп.

Теорема. *Пусть $H \cong F_l$, $G \cong F_m$ — подгруппы конечного ранга свободной группы F. Тогда $H \cap G \cong F_r$, где*

$$r \leq 1 + 2(m-1)(n-1) - \min(m-1, n-1).$$

§ ?. Коммутант свободной группы

Теорема. *Коммутант свободной группы F_2 свободно порожден коммутаторами $[x^m, y^m]$, $x, y \in \mathbb{Z}^\bullet$.*

Доказательство. Легко видеть, что эти коммутаторы порождают $[F_2, F_2]$. В самом деле, рассмотрим произвольный элемент коммутанта. Он имеет вид $x_M \ldots$

§ ?. Теорема Нильсена об автоморфизмах свободной группы

Теорема Нильсена. *Любая система свободных образующих свободной группы F конечного ранга может быть получена из фиксированной системы свободных образующих $x_1, \dots, x_n$ многократным применением следующих трех типов преобразований:*

1) транспозиция двух элементов системы $x_1, \dots, x_n$;

2) замена одного из x_i на x_i^{-1};

3) замена одного из x_i на $x_i x_j$ для $j \neq i$.

§ ?. Свободное произведение групп

В различных частных случаях таких, как $\mathrm{PSL}(2, \mathbb{Z})$ свободные произведения возникали в конце XIX века в работах Фрике и Клейна. В явном виде конструкция свободного произведения была введена в 1927 году Шрайером.

$G^\sharp = G \setminus \{1\}$.

Теорема. *Пусть H, G — суть две группы. Сущесвтует группа $H * G$ содержащая изоморфные копии подгрупп H и G, обладающее следующими свойствами:*

$H \cap G = 1$

Каждый элемент $x \in H * G$ допускает единственное представление в виде $x = x_1 \dots x_n$, $n \in \mathbb{N}_0$, где каждое x_i принадлежит $H^\sharp \sqcup G^\sharp$, причем если $x_i \in H$, то $x_{i+1} \in G$ и, наоборот, если $x_i \in G$, то $x_{i+1} \in H$.

Доказательство Эйленберга[223]. Заменяя H и G на их изоморфные копии, мы можем с самого начала предполагать, что $H \cap G = 1$. Определим теперь $H * G$ как подмножество в $W(H^\sharp \sqcup G^\sharp)$, состоящее из таких слов $w = x_1 \dots x_n$, $n \in \mathbb{N}_0$, что никакие две соседних буквы не принадлежат H или G. В частности, слово $1 = \Lambda$ длины 0 обладает этим свойством. Определим произведение двух слов $w = x_1 \dots x_m$ и $z = y_1 \dots y_n$ по индукции следующим образом:

$$wz = \begin{cases} x_1 \dots x_m y_1 \dots y_n, & \text{если } x_m \in H, y_1 \in G \text{ или } x_m \in G, y_1 \in H, \\ x_1 \dots x_{m-1}(x_m y_1) y_2 \dots y_n, & \text{если } x_m, y_1 \in H \text{ или } x_m, y_1 \in G, \text{ причем } x_n x_1 \neq 1, \\ x_1 \dots x_{m-2}(x_{m-1} y_2) y_3 \dots y_n, & \text{если } x_m, y_1 \in H \text{ или } x_m, y_1 \in G, \text{ причем } x_n x_1 = 1. \end{cases}$$

Эту формулу следует понимать следующим образом: в первом случае это обычная конкатенация слов в $W(H^\sharp \sqcup G^\sharp)$, во втором случае x_m переносится из w в z и умножается на y_1 в группе H или G, после чего слова $x_1 \dots x_{m-1}$ и $(x_m y_1) y_2 \dots y_n$ конкатенируются. Наконец, в третьем случае последний множитель w и первый множитель z сокращаются, после чего получившиеся (более короткие!) слова снова умножаются по тому же правилу. При этом могут произойти дальнейшие сокращения, которые приведут нас к еще более коротким словам и т.д. В конце концов мы либо сможем применить второй случай, либо одно из слов сократится полностью и мы сможем применить первый случай (конкатенация с пустым словом).

Ясно, что пустое слово служит нейтральным элементом, и из третьего случая вытекает, что если $w = x_1 \dots x_m$, то $w^{-1} = x_m^{-1} \dots x_1^{-1}$, где x_i^{-1} есть обратный к x_i в H или G, действительно будет обратным к w в $H * G$. Таким образом, чтобы проверить, что $H * G$ действительно группа, нам осталось лишь доказать, что так определенное произведение на $H * G$ ассоциативно. Рассмотрим произведение $(uv)w$. Будем вести рассуждение индукцией по длине слова v. Шаг индукции очевиден. В самом деле, пусть длина l слова v по крайней мере 2 и $v = xz$, где $x \in H^\sharp \sqcup G^\sharp$, а z — более короткое слово. Тогда, так как для слов длины 1 и $l - 1$ наша теорема уже доказана,

$$(uv)w = (u(xz))w = ((ux)z)w = (ux)(zw) = u(x(zw)) = u((xz)w) = u(vw).$$

[223] См. Ленг, стр.53–54.

Таким образом, нам остается доказать базу индукции, а именно, ассоциативность для случая, когда v слово длины 0 или 1. Если v пустое слово, это очевидно — как $(uv)w$, так и $u(vw)$ равно uw, точно так же в дальнейшем мы можем считать и что слова u, w непустые. Итак, нам остается рассмотреть только случай, когда $v = z$, где $z \in H^\sharp \sqcup G^\sharp$. Пусть для определенности $z \in H^\sharp$, случай $z \in G^\sharp$ рассматривается совершенно аналогично. В этом случае как $(uz)w$, так и $u(zw)$, где $u = x_1 \dots x_m$, $w = y_1, \dots y_n$, равны одному из следующих слов, as is the case:

- $x_1 \dots x_n z y_1 \dots y_n$, если $x_n, y_1 \in G$;
- $x_1 \dots x_{n-1}(x_n z) y_1 \dots y_n$, если $x_n \in H$, $x_n z \neq 1$, $y_1 \in G$;
- $x_1 \dots x_n (z y_1) y_2 \dots y_n$, если $x_n \in G$, $y_1 \in H$, $z y_1 \neq 1$;
- $x_1 \dots x_{n-1} y_1 \dots y_n$, если $x_n = z^{-1} \in H$, $y_1 \in G$;
- $x_1 \dots x_n y_2 \dots y_n$, если $x_n \in G$, $y_1 = z^{-1} \in H$;
- $x_1 \dots x_{n-1}(x_n z y_1) y_2 \dots y_n$, если $x_n, y_1 \in H$, $x_n z y_1 \neq 1$;
- $x_1 \dots x_{n-1} y_2 \dots y_n$, если $x_n, y_1 \in H$, $x_n z y_1 = 1$.

Осталось заметить, что группы H и G очевидным образом вкладываются в $H * G$.

§ ?. Примеры свободных произведений

$D_\infty = C_2 * C_2$.

Лемма Титса. *Пусть K — поле, t — трансцендентен над K. Тогда*

$$\left\langle \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ tK & 1 \end{pmatrix} \right\rangle = \begin{pmatrix} 1 & K \\ 0 & 1 \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ tK & 1 \end{pmatrix}$$

§ ?. Геометрические модели свободных произведений

Чрезвычайно удачное описание относящихся сюда топологических понятий можно найти в книге

Ч.Косневский, Начальный курс алгебраической топологии. – ???

Котенок со шпулькой

Пинг-понг

Любое нетривиальное соотношение начинается и заканчивается разными буквами.

Теорема.

$$\langle x, w \rangle \cong \mathbb{Z} * C_2$$

$$x = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}, \qquad w = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

Доказательство. Рассмотрим соотношение между x и w. Не теряя общности можно считать, что это соотношение заканчивается нетривиальной степенью x, иными словами, $\dots w x^{m_1} = 1$. Обозначим через $\mathbb{B}$ внутренность единичного круга. Тогда $x^m : z \mapsto z + 2m$ так что $x^m \mathbb{B}$ является *собственным* подмножеством дополнения к $\overline{\mathbb{B}}$. С другой стороны, $w : z \mapsto -z^{-1}$ переводит дополнение к $\overline{\mathbb{B}}$ в $\mathbb{B}$ и, значит, $w x^{m_1} \mathbb{B}$ является *собственным* подмножеством $\mathbb{B}$. Повторяя это соображение, мы видим, что $w x^{m_r} \dots w x^{m_1} \mathbb{B} \subset \mathbb{B}$, так что $w x^{m_r} \dots w x^{m_1} \neq 1$.

Модулярная картинка

$$\mathrm{PSL}(2,\mathbb{Z}) \cong C_2 * C_3.$$

$$x = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \qquad y = \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix}$$

альтернатива Титса[224]

§ ?. Свободные подгруппы группы монотонных отображений

Рассмотрим группу $\mathrm{Aut}(\mathbb{R},\geq)$ возрастающих отображений поля $\mathbb{R}$ в себя, относительно обычного порядка. В 1949 году Бернард Нойман доказал следующую важную теорему[225].

Теорема Ноймана. *Группа* $\mathrm{Aut}(\mathbb{R},\geq)$ *содержит свободную подгруппу ранга* $2^{\aleph_0}$.

К сожалению, доказательство этого замечательного результата опирается на несколько довольно трудных теорем и совершенно неконструктивно. Наиболее простая пара независимых элементов в $\mathrm{Aut}(\mathbb{R},\geq)$ была указана Уайтом[226].

Теорема Уайта. *Для любого нечетного простого* p *группа, порожденная отображениями* $x \mapsto x+1$ *и* $x \mapsto x^p$, *свободна.*

Этот чрезвычайно естественный и красивый результат оказался на удивление глубоким и до сегодняшнего дня не известно никаких простых доказательств, которые не использовали бы трудные теоремы теории полей или алгебраической геометрии.

В 1997 году Беннет[227] дал очень простое доказательство вложимости F_n в $\mathrm{Aut}(\mathbb{R},\geq)$, хотя и относительно гораздо менее естественных образующих.

§ ?. Амальгамированное произведение

$$\mathrm{SL}(2,\mathbb{Z}) \cong C_4 *_{C_2} C_6.$$

$$x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$$

Подгруппа Гекке

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid c \equiv 0 \pmod{p} \right\}.$$

Теорема Ихара. *Пусть* K *– поле, тогда*

$$\mathrm{SL}(2,\mathbb{Z}[1/p]) = \mathrm{SL}(2,\mathbb{Z}) *_{\Gamma_0(p)} \mathrm{SL}(2,\mathbb{Z}).$$

Теорема Нагао. *Пусть* K *– поле, тогда*

$$\mathrm{GL}(2,K[t]) = \mathrm{GL}(2,K) *_{B(2,K)} B(2,K[t]).$$

---

[224] J.Tits, Free subgroups in linear grous. – J. Algebra, 1972, vol.20, p.250–270.

[225] B.H.Neumann, On ordered groups. – Amer. J. Math., 1949, vol.71, p.1–18.

[226] S.White, The group generated by $x \mapsto x+1$ and $x \mapsto x^p$ is free. – J.Algebra, 1988, vol.118, p.408–422.

[227] C.D.Bennett, Explicit free subgroups of $\mathrm{Aut}(\mathbb{R},\geq)$. – Proc. Amer. Math. Soc., 1997, vol.125, N.5, p.1305–1308.

§ ?. Проблема Бернсайда: синопсис

В 1902 году Уилльям Бернсайд поставил вопрос о том, конечна ли конечно порожденная группа, все элементы которой имеют конечный порядок[228]. В дальнейшем эта задача получила название **общей проблемы Бернсайда** (`general Burnside problem`[229]). В этом и нескольких следующих параграфах мы обсудим основные результаты относящиеся к этой проблеме, ее вариантам и обобщениям.

Магнус, Каррас и Солитер сравнили роль проблемы Бернсайда в комбинаторной теории групп с ролью проблемы Ферма в алгебраической теории чисел.

§ ?. Общая проблема Бернсайда

Общая проблема Бернсайда. *Является ли конечно порожденная периодическая группа конечной?*

Ответ — нет, первые примеры приведены Голодом[230,231] на основе общей конструкции Голода–Шафаревича[232]. С тех пор было построено много дальнейших примеров.

Теорема Голода. *Для любого простого $p \in \mathbb{P}$ и любого $n \in \mathbb{N}$ существует $(n+1)$-порожденная p-группа, в которой все n-порожденные подгруппы конечны.*

§ ?. Ограниченная проблема Бернсайда

Ограниченная проблема Бернсайда. *Является ли конечно порожденная группа конечной экспоненты конечной?*

Обозначим через $B(m,n) = F_m/F_m^n$ **группу Бернсайда** экспоненты n с m образующими. В этой группе соотношение $w^n = 1$ имеет место для *всех* слов, а не только для образующих.

Задача. Убедитесь, что $B(m,1) \cong 1$, $B(1,n) \cong C_n$ и $B(m,2) \cong C_2^m$.

Сам Бернсайд доказал, что группа $B(m,3)$ конечна, а Фридрих Леви и Бартельс ван дер Варден[233] оценили порядок группы $B(m,3)$:

$$|B(m,3)| = 3^{\binom{m}{1}+\binom{m}{2}+\binom{m}{3}}.$$

В 1902 году Бернсайд доказал, что группа $B(2,4)$ конечна и что ее порядок *делит* 2^{12}, а в 1960 году Тобин[234] доказал, что порядок этой группы действительно *равен* 2^{12}. Заметим, что в той же работе Бернсайд доказал, что для

---

[228] W.Burnside, On an unsettled problem in the theory of discontinuous groups. – Quart. J. Math., 1902, vol.33, p.230–238.

[229] проблема генерала Бернсайда.

[230] Е.С.Голод, О ниль-алгебрах и финитно-аппроксимируемых группах. – Изв. АН СССР, Сер. Мат., 1964, т.28, с.273–276.

[231] Е.С.Голод, О некоторых проблемах бернсайдовского типа. – В кн.: Труды Междунар. Конгр. Математиков, М., Мир, 1968, с.284–289.

[232] Е.С.Голод, И.Р.Шафаревич, О башне полей классов. – Изв. АН СССР, Сер. Мат., 1964, т.28, с.13–24.

[233] F.Levi, B.van der Waerden, Über eine besondere Klasse von Gruppen. – Hamburg Math. Abh., 1932, Bd.9, S.154–158.

[234] S.Tobin, Simple bounds for Burnside p-groups. – Proc. Amer. Math. Soc., 1960, vol. 11, p.704–706.

любого простого $p \in \mathbb{P}$ порядок группы $B(2,p)$ не меньше p^{2p-3}. В 1940 году Петербургский математик Санов[235] доказал, что группа $B(m,4)$ конечна (этот результат был одним из основных результатов диссертации Санова, которую он защитил в 1946 году), но не вычислил порядок этой группы.

Теорема Санова. *Группа $B(m,4)$ конечна.*

Доказательство.

Этот порядок вычислен в отдельных частных случаях, например,

$$|B(2,4)| = 2^{12}, \qquad |B(3,4)| = 2^{69}, \qquad |B(4,4)| = 2^{422}.$$

Маршал Холл доказал, что $B(m,6)$ конечна и

$$|B(m,6)| = 2^a 3^{\binom{b}{1}+\binom{b}{2}+\binom{b}{3}},$$

где коэффициенты

$$a = 1 + (m-1)3^{\binom{m}{1}+\binom{m}{2}+\binom{m}{3}}, \quad b = 1 + (m-1)2^m,$$

уже знакомы нам из порядков $B(m,2)$ и $B(m,3)$.

В 1947 году Санов[236] доказал, что для доказательства конечности групп Бернсайда при фиксированном n достаточно доказать конечность группы Бернсайда с двумя образующими.

Теорема Санова. *Если группа $B(2,n)$ конечна, то и все группы $B(m,n)$ конечны.*

Однако вопрос о конечности группы $B(2,n)$ оказался невероятно сложным. Следующий замечательный результат был анонсирован П.С.Новиковым[237] (в предположении $n \geq 72$) и окончательно установлен П.С.Новиковым и С.И.Адяном в 1968 году[238] (с другой оценкой на n, а именно, $n \geq 4381$). Детальное изложение доказательства (с приведенной ниже оценкой n) можно найти в книге С.И.Адяна[239]. В дальнейшем для А.Ю.Ольшанский[240] предложил гораздо более простое геометрическое доказательство в предположении, что $n > 10^{10}$.

Теорема Новикова-Адяна. *При любом нечетном $n \geq 665$ группа $B(2,n)$, бесконечна.*

В дальнейшем с помощью своего геометрического метода Ольшанский[241] доказал следующий совершенно удивительный результат.

---

[235]И.Н.Санов, Решение проблемы Бернсайда для показателя 4. – Учен. Зап. Ленингр. Ун-та, 1940, т.10, с.166–170.

[236]И.Н.Санов, О проблеме Бернсайда. – Докл. АН СССР, 1947, т.57, с.759–161.

[237]П.С.Новиков, О периодических группах – Докл. АН СССР, 1959, т.127, с.749–752.

[238]П.С.Новиков, С.И.Адян, Бесконечные периодические группы. I, II, III. – Изв. АН СССР, Сер. Мат., 1968, т.32, с.212–244, с.251–524, с.709–731.

[239]С.И.Адян, Проблема Бернсайда и тождества в группах. – М., 1975.

[240]А.Ю.Ольшанский, О теореме Новикова–Адяна. – Мат. сб., 1982, т.118, N.2, с.203–235.

[241]А.Ю.Ольшанский, Группы ограниченного периода с подгруппами простого порядка. – Алгебра и Логика, 1982, т.21, N.5, с.555–618.

Теорема Ольшанского. *Для любого достаточно большого простого $p \in \mathbb{P}$ существует бесконечная группа, все собственные подгруппы которой имеют порядок p.*

Как отмечает А.И.Кострикин[242]: 'это — наиболее сильная форма отрицательного ответа на вопрос Бернсайда, означающая существование безбрежного архипелага конечно порожденных периодических групп с тождеством $x^n = 1$, сколь угодно далеких по своим свойствам от конечных.'

§ ?. Ослабленная проблема Бернсайда

В 1930-е годы в связи с отсутствием прогресса по общей проблеме Бернсайда многие специалисты считали, что следует сконцентрировать внимание на *конечных* фактор-группах группы $B(m,n)$. К началу 1940-х годов у нескольких ведущих экспертов по комбинаторной теории групп, в том числе у Магнуса и Цассенхауза, возникло предположение, что возможна такая ситуация, когда группа $B(m,n)$ бесконечна, но у нее имеется лишь конечное число неизоморфных конечных факторов. Это предположение было явным образом сформулировано в 1940 году Отто Грюном[243], а в 1950 году Вильгельм Магнус[244], назвал его **ослабленной проблемой Бернсайда** (`restricted Burnside problem`).

Ослабленная проблема Бернсайда. *Ограничены ли в совокупности порядки конечных фактор-групп группы Бернсайда $B(m,n)$?*

Иными словами, это означает, что в группе $B(m,n)$ имеется лишь конечное число нормальных делителей конечного индекса. В этом случае по теореме Пуанкаре их пересечение $\overline{B}(m,n)$ тоже является нормальным делителем конечного индекса. Фактор-группа $B_0(m,n) = B(m,n)/\overline{B}(m,n)$ является максимальной *конечной* группой с m образующими и соотношением $x^n = 1$. Все остальные такие конечные группы являются ее фактор-группами. Ослабленная проблема Бернсайда утверждает в точности, что $B_0(m,n)$ *существует*.

Первым ключевым продвижением в этом направлении был следующий результат, полученный в ? Холлом и Хигменом.

Теорема Холла–Хигмена. *Предположим, что ослабленная проблема Бернсайда допускает положительное решение для всех примарных показателей. Тогда порядки конечных разрешимых n-порожденных групп периода m ограничены в совокупности.*

Этот результат концентрирует внимание на случае, когда $m = q = p^l$ примарно. Этот случай оказался необычайно трудным. Вначале Кострикин[245,246] и Г.Хигмен[247] положительно решили ослабленную проблему Бернсайда для

[242]А.И.Кострикин, Вокруг Бернсайда. – М., Наука, 1986, с.1–232; стр.8.

[243]O.Grün, Zusammenhang zwischen Potenzbildung und Kommutatorbildung. – J. reine angew. Math., 1940, Bd.182, S.158–177.

[244]W.Magnus, A connection between the Baker–Hausdorff formula and a problem of Burnside. – Ann. Math., 1950, vol.52, p.11–26; Errata – ibid., 1953, vol.57, p.606.

[245]А.И.Кострикин, Решение ослабленной проблемы Бернсайда для показателя 5. – Изв. АН СССР, Сер. Мат., 1955, т.19, N.3, с.233–244.

[246]А.И.Кострикин, Кольца Ли, удовлетворяющие условию Энгеля. – Изв. АН СССР, Сер. Мат., 1957, т.21, с.515–540.

[247]G.Higman, On finite groups of exponent five. – Proc. Cambridge Phil. Soc., 1956, vol.52, p.381–390.

показателя $p = 5$. Вскоре после этого Кострикин[248,249] положительно решил ослабленную проблему Бернсайда для случая простого показателя для произвольного простого показателя p.

Теорема Кострикина–Зельманова. *При любом примарном $q = p^l$, $p \in \mathbb{P}$, ослабленная проблема Бернсайда допускает положительное решение.*

Отсюда и из теоремы Холла-Хигмена и классификации конечных простых групп следует положительное решение ослабленной проблемы Бернсайда для всех показателей.

Тема ?: Задание групп образующими и соотношениями

§ ?. Задание групп образующими и соотношениями

Пусть $G = \langle g_1, \dots, g_n \rangle$ — подгруппа, порожденная элементами $g_1, \dots, g_n$. Рассмотрим свободную группу F, свободно порожденную $x_1, \dots, x_n$. По универсальному свойству свободной группы существует единственный гомоморфизм $\pi : F \longrightarrow G$, $x_i \mapsto g_i$. Обозначим ядро этого гомоморфизма через R. По теореме о гомоморфизме $G \cong F/R$. Таким образом, чтобы задать группу G нам нужно научиться описывать подгруппу R.

Наивная попытка задать систему образующих R *как подгруппы* не имеет большого смысла. Дело в том, что любая нетривиальная нормальная подгруппа бесконечного индекса в F_n имеет бесконечный ранг. Тем самым, при выписывании системы образующих R *как подгруппы*, для задания всех бесконечных групп, кроме свободных, требовалось бы бесконечное число соотношений.

Однако ядро любого гомоморфизма является нормальной подгруппой. Поэтому гораздо осмысленнее задавать образующие R как нормального делителя.

$C_n = \langle x | x^n \rangle$

$D_n = \langle x, y | x^2 = y^2 = (xy)^n \rangle$

Теорема фон Дика. *Если*

§ ?. Группы с одним соотношением

Фундаментальная группа $\pi_1(X)$ компактной поверхности X имеет задание

$$\langle x_1, \dots, x_n \mid w = 1 \rangle,$$

где w – слово в образующих $x_1, \dots, x_n$. Любая группа, допускающая такое задание, называется группой с одним соотношением (one-relator group).

А именно, если X – сфера с m ручками и n пленками, то ее фундаментальная группа допускает задание

$$\pi_1(X) = \langle x_1, y_1, \dots, x_m, y_m, z_1, \dots, z_n \mid z_1^2 \dots z_n^2 [x_1, y_1] \dots [x_m, y_m] = 1 \rangle.$$

[248]А.И.Кострикин, О проблеме Бернсайда. – Докл. АН СССР, Сер. Мат., 1958, т.119, N.6, с.1081–1084.

[249]А.И.Кострикин, О проблеме Бернсайда. – Изв. АН СССР, Сер. Мат., 1959, т.23, N.1, с.1–34.

Фундаментальная группа компактной ориентируемой поверхности рода $g \geq 2$ допускает следующее задание

$$\pi_1(X) = \langle x_1, y_1, \dots, x_g, y_g, \mid [x_1, y_1] \dots [x_g, y_g] = 1 \rangle.$$

Фундаментальная группа компактной неориентируемой поверхности рода $g \geq 2$ допускает следующее задание

$$\pi_1(X) = \langle z_1, \dots, z_g \mid z_1^2 \dots z_g^2 = 1 \rangle.$$

§ ?. Задание симметрической группы

Задание группы S_n в терминах фундаментальных транспозиций

$$s_1 = (12), s_2 = (23), \dots, s_n = (n-1, n),$$

обычно называется **Коксетеровским заданием** этой группы, так как оно является частным случаем полученного Коксетером задания групп, порожденных отражениями. Однако для этого частного случая оно было получено уже в 1897 году Муром[250].

Теорема. *Группа S_n допускает задание*

$$S_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, (s_i s_j)^2 = 1, |i-j| \geq 2; \\ (s_i s_{i+1})^3 = 1, i = 1, \dots, n-2 \rangle.$$

$$S_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, s_i s_j = s_j s_i, |i-j| \geq 2; \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, i = 1, \dots, n-2 \rangle.$$

§ ?. Задание октаэдральной группы

Ближайшим родственником симметрической группы является октаэдральная группа Oct_n, которую проще всего представлять себе как подгруппу в S_{2n}. А именно, рассмотрим множество $X = \{1, \dots, n, -n, \dots, -1\}$, состоящее из $2n$ символов. Тогда Oct_n является подгруппой в S_X, состоящей из тех перестановок π, для которых $\pi(-i) = -\pi(i)$. В следующей теореме мы задаем группу Oct_n относительно следующих образующих:

$$s_1 = (12)(-2, -1), s_2 = (23)(-3, -2), \dots, \\ s_{n-1} = (n-1, n)(-n, -(n-1)), s_n = (n, -n)$$

Первые $n-1$ из этих образующих порождают подгруппу в Oct_n, состоящую в изоморфную S_n, а последняя состоит в одной смене знака.

Теорема. *Группа Oct_n допускает задание*

$$\mathrm{Oct}_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, (s_i s_j)^2 = 1, |i-j| \geq 2; \\ (s_i s_{i+1})^3 = 1, i = 1, \dots, n-2; (s_{n-1} s_n)^4 = 1 \rangle.$$

$$\mathrm{Oct}_n = \langle s_1, \dots, s_{n-1} \mid s_i^2 = 1, s_i s_j = s_j s_i, |i-j| \geq 2; \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, i = 1, \dots, n-2; s_{n-1} s_n s_{n-1} s_n = s_n s_{n-1} s_n s_{n-1} \rangle.$$

[250] E.H.Moore, Concerning the abstract groups of order $k!$ and $\frac{1}{2}k!$ – Proc. London. Math. Society, 1897, vol.28, p.357–366.

§ ?. Группы Коксетера

§ ?. Группы кос

В настоящем параграфе мы рассмотрим совершенно замечательные группы, которые были введены Эмилем Артином[251,252,253]. Эти группы оказались теснейшим образом связаны со многими вопросами топологии, алгебры, физики и функционального анализа.

1. Заплетающее соотношение. Группа кос с двумя нитями B_2 изоморфна $\mathbb{Z}$. А вот группа кос с *тремя* нитями B_3 представляет собой уже довольно интересный объект, в котором проявляется вся специфика кос. Эта группа порождается *двумя* элементами:

$$B_3 = \langle x, y \mid xyx = yxy \rangle.$$

Возникающее здесь соотношение $xyx = yxy$ называется **заплетающим соотношением** (от английского `braid relation`[254].

Задача. Убедитесь, что элемент $xyxyxy \in B_3$ централен.

Задача. Покажите, что относительно образующих $u = xy$, $v = xyx$ группа B_3 задается следующими соотношениями:

$$B_3 = \langle u, v \mid u^3 = v^2 \rangle$$

В частности, по теореме фон Дика это значит, что группа $\mathrm{PSL}(2, \mathbb{Z})$ является фактор-группой B_3 по *центральной* подгруппе, порожденной u^3.

2. Группа кос. Перейдем теперь к общему случаю. **Группа кос** B_n с n нитями порождается $n-1$ элементом:

$$B_n = \langle s_1, \dots, s_{n-1} \mid s_i s_j = s_j s_i, |i-j| \geq 2; \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, i = 1, \dots, n-2 \rangle.$$

Эта группа действительно связана с геометрическими объектами, называемыми **косами** (`Zopf`, `braid`, `tresse`).

Задача. Докажите, что B_n порождается s_1 и $w = s_1 s_2 \dots s_{n-1}$.

Решение. В самом деле, $s_i = w^{i-1} s_1 w^{-(i-1)}$.

Артин доказал, что относительно этих образующих группа B_n допускает следующее задание

$$B_n = \langle s_1, w \mid w^n = (ws_1)^{n-1}, [s_1, w^{-i} s_1 w^i] = 1, 2 \leq i \leq n/2 \rangle.$$

Задача (Чжоу[255]). Докажите, что центр группы кос B_n совпадает с бесконечной циклической группой, порожденной w^n.

---

[251] E.Artin, Theorie der Zöpfe. – Abh. Math. Sem. Univ. Hamburg, 1926, Bd.4, S.47–72.

[252] E.Artin, Theory of braids. – Ann. Math. 1947, vol.48, p.101–126.

[253] E.Artin, Braids and permutations. – Ann. Math. 1947, vol.48, p.643–649.

[254] В действительности общепринятый русский перевод этого термина отсутствует. Такой перевод должен выражать идею **плетения** и быть однокоренным с соответствующими греческими, латинскими и немецкими словами ($\pi\lambda\grave{\varepsilon}\varkappa\omega$, $\pi\lambda\varepsilon\varkappa\tau\grave{o}\varsigma$ — **симплектический**, **плетизм**; `plexus` — **плексус**, или `Flechte`, `flechten`), но в русском языке слово **плетение** = `plaid` (**плед**) подразумевает двумерную картинку с идущими в *двух* направлениях нитями. С другой стороны, термин **сплетение**, **сплетающий** уже используется по крайней мере в двух совершенно других устойчивых смыслах: `Kranzprodukt`, `wreath product` и `intertwining`. Поэтому я перевожу `braid` как **заплетение**. Кстати, чтобы разнести идеи **сплетения** и **переплетения**, было бы полезно переводить `intertwining operator` как **переплетающий оператор**, `intertwining number` как **число переплетения** и т.д.

[255] W.Chow, On the algebraic braid group. – Ann. Math. 1948, vol.49, p.654–658.

§ ?. Группы треугольника

Один из важнейших примеров группы, заданной образующими и соотношениями — это группа треугольника

$$T(k,l,m) = \langle x, y \mid x^k = y^l = (xy)^m = 1 \rangle.$$

Это задание можно переписать и чуть иначе, более симметрично, в терминах трех образующих:

$$T(k,l,m) = \langle x, y, z \mid x^k = y^l = z^m = xyz = 1 \rangle.$$

Это группа, которую Коксетер–Мозер обозначают (k,l,m). Оказывается, по своему строению эти группы разбиваются на три радикально различных случая, в зависимости от значения $\dfrac{1}{k} + \dfrac{1}{l} + \dfrac{1}{m}$. Если это значение > 1, то группа $T(k,l,m)$ называется **сферической**, если оно $= 1$ — **эвклидовой**, а если < 1 — **гиперболической**. Группа $T(k,l,m)$ истолковывается геометрически как группа, порожденная поворотами на углы $2\pi/k$, $2\pi/l$ и $2\pi/m$ вокруг вершин треугольника с углами $\pi/k, \pi/l, \pi/m$. Сферический случай соответствует сумме углов треугольника $> 2\pi$, эвклидов — сумме углов 2π и, наконец, гиперболический — сумме углов $< 2\pi$. Ясно, что треугольники с такой суммой углов существуют на сфере $\mathbb{S}^2$, эвклидовой плоскости $\mathbb{R}^2$ и плоскости Лобачевского $\mathbb{H}^2$, соответственно.

1. Сферические треугольники. Классификация сферических треугольных групп сразу получается из классификации конечных групп вращений сферы, которую мы получили в Главе I.

Теорема. *Группа $T(k,l,m)$ в том и только том случае конечна, когда*

$$\frac{1}{k} + \frac{1}{l} + \frac{1}{m} > 1,$$

в этом случае ее порядок равен $2klm/n$, где

$$n = klm\left(\frac{1}{k} + \frac{1}{l} + \frac{1}{m} - 1\right) = kl + km + lm - klm.$$

Таким образом, единственными сферическими треугольными группами являются $T(2,2,m)$, $T(2,3,3)$, $T(2,3,4)$ и $T(2,3,5)$. Формула для порядка проверяется с учетом площади сферического треугольника с углами $\pi/k, \pi/l, \pi/m$. По самому определению $T(2,2,m) \cong D_m$ — это диэдральная группа, остальные группы столь же легко отождествить.

Задача. Докажите следующие изоморфизмы,

$$T(2,3,2) \cong S_3, \quad T(2,3,3) \cong A_4, \quad T(2,3,4) \cong S_4, \quad T(2,3,5) \cong A_5.$$

Первые три из этих изоморфизмов были установлены в 1882 году фон Диком[256], а четвертый еще в 1856 году Гамильтоном[257]. Как отмечают Коксетер–Мозер, результат Гамильтона представляет собой одно из первых заданий

[256] W.von Dyck, Gruppentheoretischen Studien. – Math. Ann., 1882, Bd.20, S.1–45.

[257] W.R.Hamilton, Memorandum respecting a new system of roots of unity. – Phil. Mag., 1856, vol.12, p.446??

групп, встречающихся в литературе, причем сам Гамильтон был в восторге от этого своего достижения!

Ответ. Укажем пары образующих этих групп, удовлетворяющие требуемым соотношениям. Для первых трех групп выбрать такие образующие совсем легко:

$$S_3 = \langle (12), (123) \rangle, A_4 = \langle (12)(34), (123) \rangle, S_4 = \langle (12), (234) \rangle,$$

для A_5 можно взять, например, $A_5 = \langle (12)(45), (135) \rangle$. С другой стороны, оценка порядка групп $T(2,3,m)$, например, при помощи алгоритма Коксетера-Тодда, показывает, что порядки групп $T(2,3,m)$ при $m = 2,3,4,5$ не превышают $6, 12, 24, 60$, соответственно.

Эвклидовы треугольники. Большой интерес представляют также эвклидовы треугольники $(2,3,6)$, $(2,4,4)$, $(3,3,3)$. Первый из этих треугольников — прямоугольный треугольник с острыми углами $\pi/3$ и $\pi/6$, второй — равнобедренный прямоугольный треугольник, а третий — равносторонний треугольник. Соответствующие группы отвечают покрытиям плоскости ...

Теорема. *Группы $T(2,3,6)$, $T(2,4,4)$ и $T(3,3,3)$ являются расширениями свободной абелевой группы $\mathbb{Z}^2$ при помощи циклической группы C_6, C_4 или C_3, соответственно.*

Гиперболические треугольники. Все остальные группы треугольников являются гиперболическими. Это самый трудный и интересный случай.

§ ?. Гурвицевы группы

$$T(2,3,7) = \langle x, y \mid x^2 = y^3 = (xy)^7 = 1 \rangle$$

Задача (Лич[258]) Докажите, что

$$T(2,3,7) \cong \langle u, v \mid (uv)^2 = (u^{-1}v)^3 = v^7 = 1 \rangle$$

Решение. Связь между этими представлениями устанавливается, например, следующим образом: $u = [y^{-1}, x] = y^2xyx$, $v = (xy)^3$. В этом случае $x = v^3uv^{-2}$, $y = v^3uv^{-4}$

Проверка конечности или бесконечности конкретных групп, заданных образующими и соотношениями, часто превращается в весьма серьезную проблему, требующую привлечения компьютеров, либо серьезного математического аппарата, далеко выходящего за пределы собственно комбинаторной теории групп. Например, рассмотрим следующую фактор-группу группы $T(2,3,7)$:

$$T(2,3,7,m) = \langle x, y \mid x^2 = y^3 = (xy)^7 = [x,y]^m = 1 \rangle$$

Следующая теорема была доказана только в 1992–93 годах[259,260,261], с использованием достаточно изощренных гомологических и геометрических методов.

[258] J.Leech, Generators for certain normal subgroups of $(2,3,7)$. – Proc. Cambridge Phil. Soc., 1965, vol.61, p.321–332.

[259] D.F.Holt, W.Plesken, A cohomological criterion for a finitely presented group to be infinite. – J. London Math. Soc., 1992, vol.45, p.469–480.

[260] J.Howie, R.M.Thomas, The groups $(2,3,p;q)$; asphericity and a conjecture of Coxeter. – J. Algebra, 1993, vol.154, p.289-309.

[261] M.Edjvet, An example of an infinite group. – in: Discrete Groups and Geometry, London Math. Soc. Lect. Note Ser., vol 173, 1992, p.66-74.

Теорема. *Группа $T(2,3,7,m)$ в том и только том случае конечна, когда $m \geq 9$.*

В случае, когда эта группа конечна, отождествить ее не слишком сложно, эта группа тривиальна при $m = 1, 2, 3, 5$; вот чему она изоморфна в оставшихся случаях:

$$T(2,3,7,4) \cong \mathrm{PSL}(2,7), \quad T(2,3,7,6) \cong T(2,3,7,7) \cong \mathrm{PSL}(2,13).$$

и, наконец, $T(2,3,7,8) \cong (C_2)^6\,\mathrm{PSL}(2,7)$ является нерасщепляющимся расширением C_2^6 при помощи $\mathrm{PSL}(2,7)$ (порядок этой группы равен 10752).

§ ?. Обобщенные группы треугольника

Обобщенная группа треугольника

$$\langle x, y \mid x^k = y^l = w(x,y)^m = 1 \rangle,$$

где $w(x,y)$ — циклически редуцированное слово в $\langle x \rangle * \langle y \rangle$, не являющееся степенью, в которое входят как x, так и y. Иными словами,

$$w(x,y) = x^{p_1} y^{q_1} \dots x^{p_s} y^{q_s},\ 0 < p_i < k,\ 0 < q_i < l,$$

для всех i. Обобщенная группа треугольника может быть бесконечна и в том случае, когда $\dfrac{1}{k} + \dfrac{1}{l} + \dfrac{1}{m} > 1$. Полностью конечные обобщенные группы треугольника классифицированы в работах[262,263]

§ ?. Дициклическая группа

Группа, заданная посредством

$$\langle x, y, z \mid x^2 = y^m = z^2 = xyz \rangle$$

называется **дициклической группой**. Коксетер–Мозер обозначают эту группу $\langle 2, 2, m \rangle$.

Задача. Докажите, что в дициклической группе $x^4 = y^{2m} = z^4 = (xyz)^2 = 1$.

Решение. Сокращая равенство $z^2 = xyz$ на z, мы видим, что $z = xy$. Таким образом, соотношение $x^2 = xyz$ принимает вид $x^2 = xyxy$ и, сокращая его на x, мы видим, что $x = yxy$ или, что то же самое, $y^{-1} = x^{-1}yx$. Теперь

$$x^2 = x^{-1}x^2x = x^{-1}y^mx = (x^{-1}yx)^m = y^{-m} = x^{-2},$$

как и утверждалось.

Таким образом, элемент $w = x^2 = y^m = z^2 = xyz$ является центральной инволюцией, которую мы обозначим через -1. По теореме фон Дика группа

[262] J.Howie, V.Metaftsis, R.M.Thomas, Finite generalized triangle groups. – Trans. Amer. Math. Soc., 1995, vol.347, p.3613–3623.

[263] L.Lévai, G.Rosenberger, B.Souvignier, All finite generalised triangle groups. – Trans. Amer. Math. Soc., 1995, vol.347, p.3625–3627.

треугольника $T(2,2,m)$ является фактор-группой соответствующей дициклической группы по ± 1

$$T(2,2,m) = \langle 2,2,m\rangle/\{\pm 1\}.$$

В частности, порядок $\langle 2,2,m\rangle$ равен $4m$. Из приведенного решения задачи видно, что дициклическую группу можно задать в терминах двух образующих, скажем, x и y:

$$\langle x,y \mid x^2 = y^m, x^{-1}yx = y^{-1}\rangle,$$

однако задание в терминах трех образующих симметричнее.

Наименьшая дициклическая группа $\langle 2,2,2\rangle$ это в точности **группа кватернионов**:

$$Q = \langle 2,2,2\rangle = \langle i,j,k \mid i^2 = j^2 = k^2 = ijk\rangle.$$

Как мы только что доказали, из этих соотношений автоматически вытекает, что $i^2 = j^2 = k^2 = ijk = -1$, а это и есть правило умножения кватернионных единиц в той форме, как его изначально выражал Гамильтон.

§ ?. Бинарные группы многогранников

В 1932 году Трелльфалль ввел в рассмотрение следующее расширение группы треугольника: группу

$$\overline{T}(k,l,m) = \langle x,y,z \mid x^k = y^l = z^m = xyz\rangle$$

Коксетер–Мозер обозначают эту группу через $\langle k,l,m\rangle$. По теореме фон Дика группа $T(k,l,m)$ является фактор-группой $\overline{T}(k,l,m)$. Таким образом, при $\dfrac{1}{k} + \dfrac{1}{l} + \dfrac{1}{m} \leq 1$ группа $\overline{T}(k,l,m)$ заведомо бесконечна. Оказывается, в тех случаях, когда $T(k,l,m)$ конечна, группа $\overline{T}(k,l,m)$ тоже конечна. А именно, можно показать[264], что элемент $w = x^k = y^l = z^m = xyz$ является (нетривиальной!) инволюцией. Таким образом, порядок групп $\overline{T}(2,3,3)$, $\overline{T}(2,3,4)$, $\overline{T}(2,3,5)$ равен 24, 48, 120, соответственно. Эти группы называются бинарной группой тетраэдра, бинарной группой октаэдра и бинарной группой икосаэдра, соответственно.

§ ?. Группы тетраэдра

Рассмотрим тетраэдр в трехмерном эвклидовом пространстве $\mathbb{R}^3$, сферическом пространстве или пространстве Лобачевского $\mathbb{H}^3$. Отражения относительно граней этого тетраэдра порождают группу изометрий этого пространства. Коксетер показал, что подгруппа этой группы, состоящая из преобразований, сохраняющих ориентацию, допускает следующее задание образующими и соотношениями:

$$\langle x,y,z \mid x^{m_1} = y^{m_2} = z^{m_3} = (xy^{-1})^{n_1} = (yz^{-1})^{n_2} = (zx^{-1})^{n_3} = 1\rangle.$$

Эта группа обозначается $T(m_1,m_2,m_3;n_1,n_2,n_3)$ и называется **группой тэтраэдра**. Для группы тэтраэдра естественно ставить те же самые вопросы,

[264] См., например, Коксетер–Мозер, стр.103–104.

что для группы треугольника. Следующий классический результат был получен Коксетером[265,266,267] в 1930-е годы, в процессе работы над классификацией групп, порожденных отражениями.

Теорема Коксетера. *Группа $T(m_1, m_2, m_3; n_1, n_2, n_3)$ в том и только том случае конечна, когда*

$$\det \begin{pmatrix} 1 & -\cos\left(\frac{\pi}{m_1}\right) & -\cos\left(\frac{\pi}{m_2}\right) & -\cos\left(\frac{\pi}{m_3}\right) \\ -\cos\left(\frac{\pi}{m_1}\right) & 1 & -\cos(\frac{\pi}{n_1}) & -\cos\left(\frac{\pi}{n_3}\right) \\ -\cos\left(\frac{\pi}{m_2}\right) & -\cos\left(\frac{\pi}{n_1}\right) & 1 & -\cos\left(\frac{\pi}{n_2}\right)) \\ -\cos\left(\frac{\pi}{m_3}\right) & -\cos\left(\frac{\pi}{n_3}\right) & -\cos\left(\frac{\pi}{n_2}\right) & 1 \end{pmatrix} > 0.$$

§ ?. Обобщенные группы тетраэдра

1. Обобщенные группы тэтраэдра. Эрнест Борисович Винберг ввел в рассмотрение следующее обобщение группы тэтраэдра. Он начал рассматривать **обобщенные группы тэтраэдра**, которые допускают копредставление:

$$\langle x, y, z \mid x^{m_1} = y^{m_2} = z^{m_3} = w_1(x,y)^{n_1} = w_2(y,z)^{n_2} = w_3(z,x)^{n_3} = 1\rangle,$$

где w_1 – циклически редуцированное слово в $\langle x\rangle * \langle y\rangle$, в которое входят как x, так и y. Аналогично, w_2 – циклически приведенное слово в $\langle y\rangle * \langle z\rangle$, в которое входят как y, так и z и, наконец, w_3 – циклически приведенное слово в $\langle z\rangle * \langle x\rangle$, в которое входят как z, так и x. Кроме того, мы предполагаем, что $m_1, n_2, m_3, n_1, n_2, n_3 \geq 2$, причем m_1, m_2, m_3 могут принимать и значение ∞. В этом параграфе мы будем рассматривать свойства этих групп, зависящие не от выбора слов w_1, w_2, w_3, а лишь от степеней $m_1, n_2, m_3, n_1, n_2, n_3 \geq 2$, при этом любая обобщенная группа тэтраэдра, as above, будет обозначаться через $G(m_1, m_2, m_3; n_1, n_2, n_3)$. Сформулируем несколько общих результатов о конечности групп $G(m_1, m_2, m_3; n_1, n_2, n_3)$.

Теорема. *Обобщенная группа тэтраэдра $G(m_1, m_2, m_3; n_1, n_2, n_3)$ бесконечна в каждом из следующих случаев:*

1) $\dfrac{1}{m_1} + \dfrac{1}{m_2} + \dfrac{1}{m_3} + \dfrac{1}{n_1} + \dfrac{1}{n_2} + \dfrac{1}{n_3} \leq 2$;

2) $\dfrac{1}{n_1} + \dfrac{1}{n_2} + \dfrac{1}{n_3} \leq 1$;

3) $\dfrac{1}{m_1} + \dfrac{1}{m_2} + \dfrac{1}{n_1} < 1$, $\dfrac{1}{m_2} + \dfrac{1}{m_3} + \dfrac{1}{n_2} < 1$ *или* $\dfrac{1}{m_3} + \dfrac{1}{m_1} + \dfrac{1}{n_3} < 1$;

4) $n_1 = n_2 = n_3 = 2$ *и* $\dfrac{1}{m_1} + \dfrac{1}{m_2} \leq \dfrac{1}{2}$, $\dfrac{1}{m_2} + \dfrac{1}{m_3} \leq \dfrac{1}{2}$, *или* $\dfrac{1}{m_3} + \dfrac{1}{m_1} \leq \dfrac{1}{2}$.

---

[265] H.S.M.Coxeter, The polytopes with regular prismatic vertex figures. – Proc. London Math. Soc., 1932, vol.34, p.126–189.

[266] H.S.M.Coxeter, Discrete groups generated by reflections. – Ann. Math., 1934, vol.35, p.588–621.

[267] H.S.M.Coxeter, The complete enumeration of finite groups of the form $R_i^2 = (R_i R_j)^{k_{ij}} = 1$. – J. London Math. Soc., 1935, vol.10, p.21–35.

Первый случай получается совмещением результатов[268,269], три других содержатся в[270].

2. Эквивалентные задания. Назовем два задания обобщенной группы тэтраэдра эквивалентными, если одно из них получается из другого цепочкой следующих операций:

• Заменить образующую u порядка m_i на образующую u^h, где $h \perp m_i$;

• Переставить образующие x, y, z;

• Заменить соотношение $w(u,v)^{n_i} = 1$ на соотношение $z(u,v)^{n_i} = 1$, где $z(u,v)$ — циклически редуцированное слово, сопряженное с $w(u,v)$;

• Заменить соотношение $w(u,v)^{n_i} = 1$ на соотношение $z(u,v)^{n_i} = 1$, где $z(u,v)$ — обратное к $w(u,v)$ слово, в свободной группе, порожденной u и v;

• Если u — образующая порядка 2, v — образующая порядка m_i, а $h, k \perp m_i$, заменить соотношение $(uv^h)^2 = 1$ на соотношение $(uv^k)^2 = 1$.

Оказывается, если в обобщенной группе тэтраэдра выполняется хотя бы одно из неравенств $n_1 \geq 3$, $n_2 \geq 3$ или $n_3 \geq 3$, то такая группа либо эквивалентна обыкновенной группе тэтраэдра[271], либо одной из шести ислючительных групп.

Теорема. *Если выполняется хотя бы одно из неравенств $n_1 \geq 4$, $n_2 \geq 4$ или $n_3 \geq 4$, то обобщенная группа тэтраэдра $G(m_1, m_2, m_3; n_1, n_2, n_3)$ эквивалентна обычной группе тэтраэдра.*

§ ?. Группы Царанова

§ ?. Группы фон Дика

Вообще, пусть

$$T(m_1, \dots, m_s) = \langle x_1, \dots, x_s \mid x_1^{m_1} = \dots = x_s^{m_s} = x_1 \dots x_s = 1 \rangle.$$

Следующий изоморфизм был доказан в

$$A_5 = \langle x, y, z \mid x^3 = y^3 = z^3 = (xy)^2 = (xz)^2 = (yz)^2 = 1 \rangle$$

§ ?. Фуксовы группы

$$\Big\langle x_1, \dots, x_s, y_1, \dots, y_t, u_1, v_1, \dots, u_g, v_g \mid x_1^{m_1} = \dots = x_s^{m_s} = 1, \prod_{i=1}^{s} x_i \prod_{j=1}^{t} y_j \prod_{h=1}^{g} [u_h, v_h] = 1 \Big\rangle.$$

[268] B.Fine, J.Howie, F.Roehl, G.Rosenberger, The generalized retrahedron group. – In: Geometric Group Theory, de Gruyter, 1995, p.99–119.

[269] R.M.Thomas, Cayley graphs and group presentations. – Math. Proc. Cambridge Phil. Soc., 1988, vol.103, p.385–387.

[270] M.Edjvet, G.Rosenberger, M.Stille, R.Thomas, On certain finite generalized retrahedron group. – In: Computational and Geometric Aspects of Modern Algebra, Cambridge Univ. Press, 2000, p.54–65.

[271] M.Edjvet, J.Howie, G.Rosenberger, R.Thomas, Finite generalized tetrahedron groups with a high-power relator. – Geom. Dedicata.

$$\mu(G) = 2g - 2 + \sum_{i=1}^{s} \left(1 - \frac{1}{m_i}\right) + l > 0.$$

§ ?. Группа Стейнберга

$$\mathrm{St}(n, q) = \langle x_{ij}(\xi), 1 \leq i \neq j \leq n, \xi \in R \mid R1, R2 \rangle.$$

§ ?. Теорема Стейнберга

Оказывается, в случае конечного поля

Теорема Стейнберга. *Группа* $\mathrm{St}(n, q)$ *изоморфна* $\mathrm{SL}(n, q)$. *Иными словами, группа* $\mathrm{SL}(n, q)$ *допускает следующее задание образующими и соотношениями:*

$$\mathrm{SL}(n, q) = \langle t_{ij}(\xi), 1 \leq i \neq j \leq n, \xi \in R \mid R1, R2 \rangle.$$

Теорема Стейнберга. *Группа* $\mathrm{SL}(n, K)$ *допускает следующее задание образующими и соотношениями*

§ ?. Амальгамированное произведение

§ ?. HNN-расширение

HNN-расширение называется так в честь знаменитых алгебраистов Грехема Хигмена, Бернарда Ноймана и Ханны Нойман, которые ввели эту конструкцию в 1949 году[272] Пусть $G = \langle X \mid R \langle$ — задание группы G образующими и соотношениями. Пусть, далее, $F, H \leq G$ суть две изоморфные подгруппы группы G, $\varphi : F \longrightarrow H$ — какой-то изоморфизм между ними. Определим группу

$$\langle X, y \mid R, \forall h \in H, yhy^{-1} = \varphi(h) \rangle$$

Эта конструкция была использована для доказательства того, что всякая счетная группа может быть вложена в группу с 2 образующими.

§ ?. Алгоритм Коксетера–Тодда

273,274

[272]G.Higman, B.H.Neumann, H.Neumann, Embedding theorems for groups. – J. London Math. Soc., 1949, vol.24, p.247–254.

[273]H.C.M.Coxeter, J.A.Todd, Abstract definition for the symmetry groups of the regular polytopes in terms of two generators. I. The complete groups. – Proc. Cambridge Phil. Soc., 1936, vol.32, p.194–200.

[274]H.C.M.Coxeter, The abstract groups $G^{m,n,p}$. – Trans. Amer. Math. Soc., 1939, vol.45, p.73–150.

§ ?. Теорема о свободе

Если у группы образующих больше, чем соотношений, то такая группа бесконечна. Сейчас мы установим значительно более точное утверждение. Рассмотрим группу

$$\langle x_1, \dots, x_n \mid w_1, \dots, w_m \rangle$$

с n образующими и m соотношениями. Назовем $d = n - m$ **дефицитом** этого задания. Следующий замечательный результат доказан Николаем Семеновичем Романовским[275] В частном случае групп с одним соотношением эта теорема была ранее доказана Магнусом.

Теорема о свободе. *Если $d \geq 0$, то среди порождающих $x_1, \dots, x_n$ найдутся d элементов, свободно порождающих свободную группу F_d ранга d.*

Приведем типичный пример результата, который легко доказывается при помощи гомологических или топологических соображений, непосредственное доказательство которого, использующее лишь методы теории групп весьма трудно.

Теорема Столлингса–Суона. *Виртуально свободная группа без кручения свободна.*

[275]Н.С.Романовский, – Алгебра и Логика, 1977, т.16, N.1, с.88–97.

Тема ?: ОСНОВНЫЕ КОНСТРУКЦИИ НАД ГРУППАМИ

Мы уже встречались с понятием прямого произведения групп. В этой главе мы возвращаемся к детальному анализу этого понятия, его вариантов и обобщений, в особенности важнейшей во всей теории групп конструкции полупрямого произведения. Кроме того, мы изучаем несколько других важнейших конструкций, позволяющих строить новые группы из уже известных, а именно, понятия индуктивного и проективного предела, сплетения и скрюченного произведения.

§ ?. Внутренние прямые произведения

Пусть H, F – две группы. В предыдущих главах мы неоднократно пользовались понятием прямого произведения $H \times F$ этих групп. По определению, $G = H \times F$ является прямым произведением H и F как множеств, а операции в G вводятся покомпонентно, т.е. $(h_1, f_1)(h_2, f_2) = (h_1h_2, f_2f_2)$, $(h, f)^{-1} = (h^{-1}, f^{-1})$ и $1 = (1, 1)$.

1. Взаимный коммутант нормальных подгрупп. Предположим, однако, что H, F с самого начала вложены в некоторую группу G. В этом случае определено произведение HF по Минковскому, которое, вообще говоря, не является погруппой в G. В этом параграфе мы выясняем, при каких условиях на H, F отображение $H \times F \longrightarrow G$, $(h, f) \mapsto hf$ является изоморфизмом.

Лемма. *Пусть $H, F \trianglelefteq G$. Тогда $[H, F] \leq F \cap H$.*

Доказательство. Пусть $h \in H$, $f \in F$, образуем их коммутатор $g = [h, f] = hfh^{-1}f^{-1}$. Переписывая g в виде $g = h(fh^{-1}f^{-1})$ и пользуясь тем, что H нормальна, получаем $g \in H$. С другой стороны, переписывая g в виде $g = (hfh^{-1})f^{-1}$ и пользуясь нормальностью F, мы видим, что $g \in F$. Таким образом, всегда $[h, f] \in H \cap F$.

Напомним, что про подмножества $A, B \subseteq G$ говорят, что они **коммутируют в целом**, если $AB = BA$. Однако нас будет интересовать следующее гораздо более сильное условие. Говорят, что подмножества $A, B \subseteq G$ **коммутируют поэлементно**, если $ab = ba$ для любых $a \in A$, $b \in B$.

Следствие. *Если нормальные подгруппы $H, F \trianglelefteq G$ пересекаются по 1, то они поэлементно коммутируют.*

Доказательство. В самом деле, по лемме для любых двух элементов $h \in H$, $f \in F$ имеем $[h, f] \in H \cap F = 1$, но это и значит, что h и f коммутируют.

Задача. Докажите, что если $F, H \leq G$, причем $Fh = hF$ для каждого $h \in H$, $fH = Hf$ для каждого $f \in F$ и, кроме того, $F \cap H = 1$, то подгруппы F и H поэлементно коммутируют.

2. Внутреннее прямое произведение. Сейчас мы введем одно из важнейших понятий теории групп, которое послужит нам образцом для нескольких обобщений.

Определение. *Группа G называется* **внутренним прямым произведением** *своих подгрупп $H, F \leq G$, если выполняются три следующих условия:*

D1. $\langle H, F\rangle = G$;

D2. $H \cap F = 1$;

D3. $H, F \trianglelefteq G$.

Внутреннее прямое произведение канонически изоморфно внешнему.

Теорема. *Если G внутреннее прямое произведение своих подгрупп $H, F \leq G$, то сопоставление $\varphi : (h, f) \mapsto hf$ задает изоморфизм $H \times F \longrightarrow G$.*

Доказательство. По условиям 2 и 3 из определения внутреннего прямого произведения H и F поэлементно коммутируют (следствие из леммы ?). Таким образом,

$$\varphi(h_1h_2, f_1f_2) = (h_1h_2)(f_1f_2) = (h_1f_1)(h_2f_2) = \varphi(h_1, f_1)\varphi(h_2, f_2)$$

и, значит, φ действительно является гомоморфизмом. Теперь условия 1 и 3 гарантируют нам, что $G = \langle H, F\rangle = HF$, так что гомоморфизм сюръективен. С другой стороны, если $(h, f) \in \mathrm{Ker}(\varphi)$, то $hf = 1$ и, значит, по условию 2, $h = f^{-1} \in H \cap F = 1$. Таким образом, ядро этого гомоморфизма тривиально.

Доказанная теорема утверждает, что если G является внутренним прямым произведением своих подгрупп H и F, то каждый элемент $g \in G$ **единственным образом** представляется в виде $g = hf$, где $h \in h$, $f \in F$. Так как h и f коммутируют, можно было бы говорить также о представлении g в виде $g = fh$.

Задача. Докажите, что если $G = F \times H$, то каждая промежуточная подгруппа A, $F \leq A \leq G$, имеет вид $A = F \times (A \cap H)$.

Задача. Для того, чтобы группа G была прямым произведением нормального делителя $H \trianglelefteq G$ и некоторой дополнительной подгруппы F, необходимо и достаточно, чтобы существовала ретракция ??? $f : G \longrightarrow H$, т.е. такой гомоморфизм, что $f(h) = h$ для всех $h \in H$

Задача. Пусть G абелева группа и $H \trianglelefteq G$ – такая нормальная подгруппа, что $G/H \cong \mathbb{Z}$. Тогда $G \cong H \times \mathbb{Z}$.

3. Обобщение на конечное число сомножителей. Рассмотрим, как понятие внутреннего прямого произведения обобщается на несколько множителей. Только обобщение условия D2 требует некоторой осторожности.

Определение. *Группа G называется* **внутренним прямым произведением** *своих подгрупп $H_1, \ldots, H_n \leq G$, если выполняются три следующих условия:*

D1. $\langle H_1, \ldots, H_n\rangle = G$;

D2. $H_i \cap \widetilde{H}_i = 1$ *для всех* $i = 1, \ldots, n$, *где* $\widetilde{H}_i = H_1 \ldots \widehat{H}_i \ldots H_n$ *есть произведение всех H_j, кроме H_i;*

D3. $H_i \trianglelefteq G$ *для всех* $i = 1, \ldots n$.

Проверка следующего утверждения предоставляется читателю в качестве упражнения.

Теорема. *Если G является внутренним прямым произведением своих подгрупп $H_1, \ldots, H_n \leq G$, то сопоставление $\varphi : (h_1, \ldots, h_n) \mapsto h_1 \ldots h_n$ задает изоморфизм $H_1 \times \ldots \times H_n \longrightarrow G$.*

Задача. Докажите, что условие D2 можно выразить еще следующим образом: если $h_1 \ldots h_n = 1$, для $h_i \in H_i$, то $h_1 = \ldots = h_n = 1$.

Задача. Докажите, что в предположении D1 и D2 условие D3 можно заменить на более слабое условие $H_1 \ldots H_i \cap H_{i+1} = 1$ для всех $1 \leq i \leq n - 1$.

§ ?. Почти прямое произведение

В теории бесконечных групп (особенно групп с дополнительными структурами, таких как топологические группы, алгебраические группы, группы Ли), условие $H \cap F = 1$ в определении прямого произведения обычно оказывается слишком ограничительным. Для того, чтобы применять топологические соображения как правило достаточно того, чтобы любой элемент из G имел *конечное число* представлений вида $g = hf$, $h \in H$, $f \in F$, а не единственное такое представление. Это оправдывает следующее определение.

Определение. *Говорят, что группа G является* **почти прямым произведением** *своих подгрупп $H, F \leq G$, если выполняются три следующих условия:*

D1. $\langle H, F\rangle = G$;

D2. $|H \cap F| < \infty$;

D3. $H, F \trianglelefteq G$.

Примеры. $G = \mathrm{GL}(n, K)$, $H = \mathrm{SL}(n, K)$, $F = C(G) = K^*e$ – группа скалярных матриц. Тогда все эти условия выполнены, $H \cap F \cong \mu_n$ – группа корней n-й степени из 1 в поле K.

§ ?. Центральное произведения

В этом параграфе мы обсудим еще одно ослабление условия 2 в определении прямого произведения.

Центральное произведение.

Определение. *Говорят, что группа G является* **центральным произведением** *своих подгрупп $H, F \leq G$, если выполняются три следующих условия:*

D1. $\langle H, F\rangle = G$;

D2. $[H, F] = 1$;

D3. $H, F \trianglelefteq G$.

В этом случае обычно пишут $G = H \circ F$. Как мы знаем, $[H, F] \subseteq H \cap F$, так что если $H \cap F = 1$, то $[H, F] = 1$. Тем самым, прямое произведение является частным случаем центрального. Легко видеть, что из условия $[H, F] = 1$ вытекает, что $H \cap F = C(H) \cap C(F) \leq C(G)$. В случае $G = H \circ F$ каждый элемент представляется в виде произведения $g = hf$, но такое представление не единственно, для любого $x \in H \cap F$ его можно переписать в виде $g = (hx)(x^{-1}f)$.

Тензорное произведение линейных групп.

Например, $\mathrm{SO}(4, \mathbb{R}) = \mathrm{SO}(3, \mathbb{R}) \circ \mathrm{SO}(3, \mathbb{R}) = \mathrm{SO}(3, \mathbb{R}) \circ \mathrm{SO}(3, \mathbb{R})/\{\pm 1\}$

§ ?. Ограниченные прямые произведения

В этом параграфе мы опишем конструкцию ограниченного прямого произведения, которая является совместным обобщением понятий прямого произведения и прямой суммы.

Ограниченное прямое произведение. Мы будем называть **парой групп** пару (G, H), где G группа, а $H \leq G$ – подгруппа в G ('группа с выделенной подгруппой'). Если (G_1, H_1) и (G_2, H_2) – две пары множеств, то **морфизмом** (G_1, H_1) в (G_2, H_2) называется такой *гоморфизм групп* $f : G_1 \longrightarrow G_2$, что $f(H_1) \leq H_2$.

Рассмотрим произвольное семейство пар (G_i, H_i), $i \in I$.

Определение. *Положим*

$$\prod\nolimits_{H_i} G_i = \left\{(g_i) \in \prod G_i \mid g_i \in H_i \text{ для почти всех } i \in I\right\},$$

где все произведения берутся по $i \in I$. *Пара* $\left(\prod_{H_i} G_i, \prod H_i\right)$ *называется* **ограниченным прямым произведением** *семейства* (G_i, H_i), $i \in I$.

Существование ограниченного прямого произведения сразу следует из существования прямого произведения и аксиомы подмножеств. Ограничения канонических проекций pr_i с $\prod G_i$ на $\prod_{H_i} G_i$ по прежнему обозначаются через pr_i. Ясно, что если множество индексов I конечно, то $\prod_{H_i} G_i = \prod G_i$, поэтому эта конструкция отличается от конструкции прямого произведения лишь для бесконечного числа сомножителей.

§ ?. Слабые прямые произведения/прямые суммы

Определение. *Ограниченное прямое произведение семейства пар* $(G_i, 1)$ *называется их* **слабым прямым произведением** *и обозначается* $\underline{\prod} G_i$. *В случае, когда все группы* G_i *абелевы, их слабое прямое произведение обычно обозначается через* $\bigoplus G_i$ *или* $\coprod G_i$ *и называется их* **прямой суммой**.

Таким образом, по определению $\underline{\prod} G_i$ состоит из всех функций $x : I \longrightarrow \bigcup G_i$ таких, что $x_i \in G_i$ *с конечным носителем*, т.е. таких, что $x_i = 1$ для всех i, кроме конечного их числа.

Мы уже отмечали, что многие писатели в области теории групп называют слабое прямое произведение групп просто *прямым произведением* и обозначают его $\prod G_i$; при этом то, что мы называем прямым произведением называется *декартовым произведением* и обозначается $\overline{\prod} G_i$. Такое словоупотребление имеет некоторый субстрат. Дело в том, что формально именно слабое прямое произведение обладает теми *свойствами* D1 – D3, которыми мы характеризовали внутреннее прямое произведение. А именно, читатель без труда докажет следующий результат.

Теорема. *Группа* G *тогда и только тогда изоморфна* **слабому прямому произведению** *своих подгрупп* $H_i \leq G$, $i \in I$, *когда выполняются три следующих условия:*

D1. $\langle H_i, i \in I\rangle = G$;

D2. $H_i \cap \widetilde{H}_i = 1$ *для всех* $i = 1, \ldots, n$, *где* $\widetilde{H}_i = \langle H_j, j \in I, j \neq i\rangle$ *есть произведение всех* H_j, *кроме* H_i;

D3. $H_i \trianglelefteq G$ *для всех* $i \in I$.

Однако в общих вопросах мы бескомпромиссно придерживаемся не внутренней, а *теоретико-категорной* точки зрения, а с точки зрения универсального свойства именно декартово произведение является прямым произведением в категории групп $\mathcal{G}r$ и в категории $\mathcal{A}b$ абелевых групп. В то же время прямая сумма является *копроизведением*, а вовсе не прямым произведением в категории $\mathcal{A}b$ абелевых групп! Поэтому принятая новосибирскими писателями терминология вводит в заблуждение.

§ ?. Подпрямые произведения

Говорят, что G – **подпрямое произведение** групп F и H, если $G \leq F \times H$, причем проекции G на каждую из компонент сюръективны. Это определение легко обобщается на любое число сомножителей. Основной пример подпрямых произведений задается следующей теоремой.

Теорема Ремака. *Пусть $H_i \trianglelefteq G$, $i \in I$, – семейство нормальных подгрупп группы G и $H = \cap H_i$, $i \in I$. Тогда G/H – подпрямое произведение G/H_i, $i \in I$.*

Доказательство. Рассмотрим отображение

$$\varphi : G \mapsto \prod_{i \in I} G/H_i, \qquad g \mapsto (gH_i)_{i \in I}.$$

Ясно, что $\mathrm{Ker}(\varphi) = H$ и, хначит, мы получаем мономорфизм $G/H \longrightarrow \prod G/H_i$, $i \in I$. Так как $H \subseteq H_i$, то проекция $G/H \longrightarrow \prod G/H_i \longrightarrow G/H_j$, $gH \mapsto gH_j$ сюръективна для каждого j.

§ ?. Полупрямые произведения

Конструкция прямого произведения весьма ограничительна, так как в ней подгруппы H и F поэлементно коммутируют. Имеется много важных примеров групп, которые очень похожи на прямые произведения по отношению к двум своим подгруппам, но в которых эти подгруппы не коммутируют. Рассмотрим, например, группу собственных движений эвклидова пространства. Каждое такое движение представляется в виде композиции трансляции и вращения, причем единственным образом. Однако трансляции и вращения не коммутируют. Сейчас мы детально обсудим это обобщение, которое является одной из важнейших конструкций позволяющих собирать неабелевы группы из абелевых кусков.

1. Полупрямое произведение. Следующее определение *почти* совпадает с определением внутреннего прямого произведения. Однако условие 3 здесь ослаблено так, что симметрия между H и F нарушается и их функции в этой конструкции различны.

Определение. *Говорят, что группа G является* **полупрямым произведением** *своих нормального делителя H и дополнительной подгруппы $F \leq G$, если выполняются три следующих условия:*

SD1. $\langle H, F\rangle = G$;

SD2. $H \cap F = 1$;

SD3. $H \trianglelefteq G$.

Чтобы обозначить, что G является полупрямым произведением нормального делителя H и дополнительной подгруппы F, используется специальный знак `threetimes`, существующий в двух модификациях: `\leftthreetimes` $\leftthreetimes$ и `\rightthreetimes` $\rightthreetimes$. А именно, в этом случае пишут $G = H \leftthreetimes F$ или $G = F \rightthreetimes H$. Обратите внимание, что ножка всегда направлена в сторону нормального делителя.

По-прежнему, из условий 1 и 3 следует, что $\langle H, F\rangle = HF = FH$, так что любой элемент $g \in G$ представляется как в виде $g = hf$, так и в виде $g = h'f'$, причем из условия 2 вытекает, что как то, так и другое представления единственны. Однако, в отличие от прямого произведения, мы можем гарантировать лишь, что $[H, F] \leq H$, так что коммутативности здесь, вообще говоря, нет. Тем не менее, множитель из F определен однозначно. В самом деле, ясно, что $g = hf = f(f^{-1}hf) = fh^f$, тем самым $f' = f$, $h' = h^f$.

2. Примеры полупрямых произведений в S_n и $\mathrm{GL}(n,K)$.

- $S_n = \mathrm{C}_2 \leftthreetimes A_n$.
- В симметрической группе $G = S_4$ есть нормальный делитель $V \trianglelefteq S_4$ и подгруппа $S_3 \leq S_4$, состоящая из перестановок, оставляющих на месте 4. Легко видеть, что $V \cap S_3 = 1$, а $VS_3 = S_4$. Таким образом, $S_4 = S_3 \leftthreetimes V$. В свою очередь, по предыдущему примеру $S_3 = \mathrm{C}_2 \leftthreetimes \mathrm{C}_3$. Таким образом, $S_4 = (C_2 \leftthreetimes C_3) \leftthreetimes V$, причем все три подгруппы, из которых собирается S_4, абелевы. Именно это разложение группы S_4 отвечает за разрешимость уравнений степени 4 в радикалах.
- $\mathrm{GL}(n,K) = \mathrm{SL}(n,K) \rtimes K^*$.
- $B = D \leftthreetimes U$
- $N = D \rtimes S_n$.

3. Голоморф группы. Можно ли включить группу G в какую-то большую группу, в которой *все* автоморфизмы группы G становятся внутренними? Такая конструкция была предложена Гельдером(??). А именно, рассмотрим полупрямое произведение

$$\mathrm{Hol}(G) = \mathrm{Aut}(G) \leftthreetimes G$$

называемое **голоморфом** группы G. Таким образом, по определению элементами голоморфа являются пары (φ, h), где $\varphi \in \mathrm{Aut}(G)$, $h \in G$, причем произведение двух таких пар определяется как

$$(\varphi, h)(\psi, g) = (\varphi\psi, \psi^{-1}(h)g).$$

§ ?. Аффинная группа

1. Аффинная группа. Проанализируем теперь подробно пример, который упоминался в самом начале предыдущего параграфа. Рассмотрим подгруппу в $\mathrm{GL}(n+1,R)$, состоящую из матриц, последняя строка которых совпадает с соответствующей строкой единичной матрицы:

$$\mathrm{Aff}(n,R) = \left\{ \begin{pmatrix} h & u \\ 0 & 1 \end{pmatrix} \mid h \in \mathrm{GL}(n,R), u \in R^n \right\}.$$

Получающаяся группа называется **аффинной группой** степени n над кольцом R, ее можно представлять себе как группу всех аффинных преобразований свободного модуля R^n ранга n, порожденную всеми трансляциями $x \mapsto x + u$, $u \in R^n$, и всеми автоморфизмами $x \mapsto hx$, $h \in \mathrm{GL}(n,R)$. В самом деле, матрица

$$\begin{pmatrix} h & u \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} e & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} h & 0 \\ 0 & 1 \end{pmatrix}$$

изображает аффинное преобразование $x \mapsto hx + u$, получающееся последовательным выполнением обратимого линейного преобразования $x \mapsto hx$ и трансляции $x \mapsto x + u$. Заметим, что трансляции и автоморфизмы не перестановочны, так как, скажем, выполнение тех же преобразований в другом порядке дает $x \mapsto hx + hu$, а это совпадает с $x \mapsto hx + u$ **только** если $hu = u$. При этом композиции аффинных преобразований отвечает умножение матриц:

$$\begin{pmatrix} h & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} g & v \\ 0 & 1 \end{pmatrix} \begin{pmatrix} hg & xv + u \\ 0 & 1 \end{pmatrix}.$$

$\mathrm{Aff}(n,R)=\mathrm{GL}(n,R)\leftthreetimes R^n$

Группы движений. Приведем несколько примеров групп движений аналогичных аффинной группе.

• **Группа эвклидовых движений.** Рассмотрим подгруппу в $\mathrm{Aff}(n,\mathbb{R})$, состоящую из тех матриц $\begin{pmatrix} h & u \\ 0 & 1 \end{pmatrix}$, для которых $h\in O(n,\mathbb{R})$.

• **Группа собственных движений эвклидовой плоскости.** Положим

$$m(a,b,\varphi)=\begin{pmatrix} \cos(\varphi) & \sin(\varphi) & a \\ -\sin(\varphi) & \cos(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Задача. Вычислить $m(a,b,\varphi)m(c,d,\psi)$.

• **Группа собственных движений плоскости Лобачевского.** Положим

$$m(a,b,\varphi)=\begin{pmatrix} \mathrm{ch}(\varphi) & \mathrm{sh}(\varphi) & a \\ \mathrm{sh}(\varphi) & \mathrm{ch}(\varphi) & b \\ 0 & 0 & 1 \end{pmatrix}.$$

Задача Вычислить $m(a,b,\varphi)m(c,d,\psi)$.

§ ?. Расширения групп, расщепляющиеся и нерасщепляющиеся расширения

§ ?. Теорема Шура–Цассенхауза

Как мы убедились в предыдущем пункте, не любое расширение групп расщепляется. Сейчас мы дадим простое *достаточное* условие расщепляемости. Напомним, что подгруппа H конечной группы G называется **холловской**, если ее порядок взаимно прост с ее индексом. Оказывается, любой *холловский* нормальный делитель конечной группы G задает *единственное* разложение этой группы в полупрямое произведение.

Теорема Шура. *Любая холловская нормальная подгруппа H группы G дополняема.*

Доказательство. Будем доказывать теорему индукцией по порядку $n=|G|$ группы G. Пусть P – какая-то силовская подгруппа в H. Аргумент Фраттини состоит в том, что $G=HN_G(P)$. По теореме об изоморфизме, $G/H\cong N_G(P)/H\cap N_G(P)$. Если $N_G(P)\neq G$, то по индукционному предположению существует дополнение F холловской нормальной подгруппы $H\cap N_G(P)$ в $N_G(P)<G$. Так как $F\cong G/H$, то F автоматически будет дополнением к H в G.

Таким образом, в дальнейшем мы можем и будем предполагать, что все силовские подгруппы группы H нормальны в G. Предположим, что $p||H|$, H не является p-группой и пусть P – ее силовская p-подгруппа. Тогда $1<P<H$, $P\trianglelefteq G$, – нетривиальный нормальный делитель группы G собственным образом содержащийся в H. Таким образом, по индукционному предположению холловская нормальная подгруппа H/P в G/P допускает нормальное дополнение K/P. Так как $|K|<|G|$, то еще раз применяя индукционное предположение, мы построим дополнение F к холловской нормальной подгруппе P в K. Так как $F\cong K/P\cong G/H$, то F будет дополнением к H в G.

Это значит, что нам остается лишь рассмотреть случай, когда сама H является нормальной силовской p-подгруппой группы G. Так как коммутант $[H,H]$ является вполне характеристической подгруппой в H, то он нормален в G. Это значит, что если $[H,H]\neq 1$, то, как и выше, применяя индукционное предположение к группе $G/[H,H]$ холловскому нормальному делителю $H/[H,H]$ в ней, мы сможем построить дополнение к H в G. Это значит, что мы можем считать, что H *абелева*. В действительности, рассматривая вместо коммутанта

подгруппу в H, порожденную p-ми степенями элементов, которая тоже является вполне характеристической, мы могли бы даже считать, что H *элементарная* абелева группа E_{p^m}, и свести задачу к изучению подгрупп в $\mathrm{GL}(m,p)$, но нам это не понадобится. Вместо этого мы проведем классическое вычисление, доказывающее тривиальность группы $H^2(G/H,H)$.

Пусть, наконец, H является абелевой нормальной силовской p-подгруппой. Тогда группа G действует на H сопряжениями, причем, так как H абелева, то сама она лежит в ядре этого действия. Таким образом, мы получаем действие G/H на H. Возьмем произвольное (теоретико-множественное!) сечение ψ канонической проекции $\pi : G \longrightarrow G/H$, т.е. *отображение* $\psi : G/H \longrightarrow G$ такое, что $\pi(\psi(x)) = x$ для любого $x \in G/H$. Так как для $h \in H$ и $x \in G/H$ значение $\psi(x)h\psi(x)^{-1}$ не зависит от выбора сечения ψ, в дальнейшем мы будем писать просто xhx^{-1}. Вообще говоря, изначально отображение ψ не является гомоморфизмом, мы как раз и хотим показать, что его можно подправить на элементы H так, чтобы получить (теоретико-групповое!) расщепление канонической проекции π, т.е. *гомоморфизм* $\varphi : C/H \longrightarrow G$, такой, что $\pi(\varphi(x)) = x$ для любого $x \in G/H$. Для этого определим отображение

$$\rho : G/H \times G/H \longrightarrow H, \qquad \rho(x,y) = \psi(x)\psi(y)\psi(xy)^{-1}.$$

Легко видеть, что ρ удовлетворяет следующему **уравнению 2-коцикла**:

$$x\rho(y,z)x^{-1}\rho(x,yz) = \rho(xy,z)\rho(x,y),$$

для всех $x,y,z \in G/H$. Зафиксируем теперь какое-то m такое, что $m|G:H| \equiv 1 \pmod{|H|}$ – именно в этом месте используется взаимная простота порядка $|H|$ и индекса $|G:H|$ подгруппы H! Это позволяет нам положить

$$\sigma(x) = \prod x\rho(x^{-1},x)^m x^{-1},$$

где произведение берется по всем $x \in G/H$. Тогда

$$\rho(x,y) = x\sigma(y)x^{-1}\sigma y\sigma(xy)^{-1},$$

иными словами, коцикл ρ является **когранице**й. Но это, как раз, и значит, что мы можем подправить сечение ψ до группового гомоморфизма, полагая $\varphi(x) = \sigma(x)^{-1}\psi(x)$ – проверьте, что это действительно гомоморфизм! Осталось положить $F = \varphi(G/H)$, это и будет искомое дополнение к H в G.

Теорема Цассенхауза. *Все дополнения к холловской нормальной подгруппе H группы G сопряжены в G.*

Эти две результата часто объединяют в одну теорему, которая в этом случае обычно называется теоремой Шура–Цасенхауза.

§ ?. Факторизации и скрюченное произведение

В этом параграфе мы изложим более сложную конструкцию, которая является дальнейшим обобщением полупрямого произведения групп.

Факторизации группы. Предположим, что группа G допускает **факторизацию**. Это значит, что найдутся две подгруппы $F,H \leq G$ такие, что каждый элемент $g \in G$ допускает *единственное* представление в виде $g = ux$, где $u \in F$, $x \in H$. Это значит, в частности, что каждое произведение вида xu, $x \in H$, $u \in F$, тоже можно переписать в виде $xu = vy$, где $v \in F$, $y \in H$. Так как элементы $v = v(x,u) \in F$ и $y = y(x,u) \in H$ здесь определены однозначно, мы получаем два отображения $H \times F \longrightarrow F$ и $H \times F \longrightarrow H$, которые обычно обозначаются как $(x,u) \mapsto {}^x u$ и $(x,u) \mapsto x^u$, соответственно. Итак, $xu = {}^x u x^u$.

Пусть теперь $x,y \in H$, $u,x \in F$. Посчитаем произведения xyu и xuv двумя способами. Ясно, что $(xy)u = {}^{xy}u(xy)^u$, а $x(yu) = x^y uy^u = {}^x({}^y u)(x)^{{}^y u}y^u$. В силу единственности это означает, что ${}^{xy}u = {}^x({}^y u)$ и $(xy)^u = (x)^{{}^y u}y^u$. Аналогично $x(uv) = {}^x(uv)x^{uv}$, а $(xu)v = {}^x u x^u v = {}^x u^{x^u} v \cdot (x^u)^v$. Снова в силу единственности можно заключить $x^{(uv)} = {}^x u^{x^u} v$ и $x^{uv} = (x^u)^v$. Кроме того, из равенств $1u = u1$ и $x1 = 1x$ следует, что $1^u = 1$, ${}^1 u = u$ и ${}^x 1 = 1$, $x^1 = x$, соответственно.

Соотношения ${}^{xy}u = {}^x({}^y u)$ и ${}^1 u = u$ в точности означают, что $(x,u) \mapsto {}^x u$ является *левым* действием H на F. Соотношения же $x^{uv} = (x^u)^v$ и $x^1 = x$ означают, что $(x,u) \mapsto x^u$ является *правым* действием F на H. Остальные же четыре условия являются новыми и мотивируют следующее определение.

Определение. *Говорят, что (F, H) образуют* **сочетающуюся пару** *групп, если H действует на F слева, а F действует на H справа, причем ${}^x1 = 1$, $1^u = 1$, а действия связаны тождествами*

$$(xy)^u = (x)^{{}^y u} \cdot y^u, \qquad {}^x(uv) = {}^x u \cdot {}^{x^u} v$$

Теорема. *Пусть (F, H) – сочетающаяся пара групп. Тогда операция*

$$(u, x)(v, y) = (u \cdot {}^x v, x^v \cdot y)$$

задает на $F \times H$ структуру группы.

Доказательство. Ясно, что $(1, 1)$ является единицей этого действия. Проверим теперь ассоциативность. Для этого рассмотрим $u, v, w \in F$ и $x, y, z \in H$. Тогда

$$((u, x)(v, y))(w, z) = (u \cdot {}^x v, x^v \cdot y)(w, z) = (u^x v \cdot {}^{x^v y} w, (x^v y)^w z),$$

в то время как

$$(u, x)((v, y)(e, z)) = (u, x)(v \cdot {}^y w, y^w \cdot z) = (u^x (v^y w), x^{v^y w} y^w z).$$

Однако ${}^x(v^y w) = {}^x v \cdot {}^{x^v}({}^y w) = {}^x v \cdot {}^{x^v y} w$. Аналогично, $(x^v y)^w = (x^v)^w y^w = x^{v^y w} y^w$.

Осталось доказать обратимость всех элементов. Равенство $(u, x)(v, y) = (1, 1)$ эквивалентно $u^x v = 1$, $x^v y = 1$. Первое равенство дает, ${}^x v = u^{-1}$ или, что то же самое, $v = {}^{x^{-1}}(u^{-1})$. Точно так же, из второго равенства получаем $y = (x^v)^{-1} = \left(x^{\left({}^{x^{-1}} u^{-1}\right)}\right)^{-1}$. Осталось проверить, что $(v, y)(u, x) = (1, 1)$, когда v и y принимают эти значения. В самом деле, пусть $(v, y)(u, x) = (w, z)$. Умножая это равенство слева на (u, x), получим $(u, x) = (u, x)(w, z) = (u^x w, x^w z)$, откуда следует, что $u = u^x w$, и, тем самым, ${}^x w = 1$, так что $w = {}^{x^{-1}} 1 = 1$. Аналогично, $x = x^w z = xz$ и, тем самым, $z = 1$. Таким образом, действительно (u, x) обратим и

$$(u, x)^{-1} = \left({}^{x^{-1}}(u^{-1}), \left(x^{\left({}^{x^{-1}} u^{-1}\right)}\right)^{-1}\right),$$

что и заканчивает доказательство.

Определение. *Построенная в теореме группа называется* **скрюченным произведением** *F и H и обозначается $F \bowtie H$.*

Ясно, что F и H вкладываются в $F \bowtie H$ посредством отображений $F \longrightarrow F \bowtie H$, $u \mapsto (u, 1)$, и $H \longrightarrow F \bowtie H$, $x \mapsto (1, x)$.

§ ?. Индуктивный предел

Пусть I — **фильтрованное вверх** частично упорядоченное множество. Это условие означает, что для любых $i, j \in I$ существует $h \in I$ такое, что $i, j \leq h$. Рассмотрим семейство групп G_i, $i \in I$ и предположим, что для каждой пары $i \leq j$ задан гомоморфизм $\varphi_i^j : G_i \longrightarrow G_j$ такой, что $\varphi_i^i = \mathrm{id}_{G_i}$ и для любых трех индексов $i \leq j \leq h$ выполняется равенство $\varphi_j^h \varphi_i^j = \varphi_i^h$. Семейство групп G_i вместе с семейством гомоморфизмов φ_i^j называется **фильтрованным вверх семейством** или **проективным семейством** групп (или иногда **прямым спектром** или **индуктивным спектром** групп).

Комментарий. С точки зрения теории категорий индуктивное семейство представляет собой просто ковариантный функтор из частично упорядоченного множества I, рассматриваемого как категория, в категорию групп $\mathcal{G}r$. Аналогичную конструкцию можно рассмотреть для любой категории $\mathcal{C}$, скажем для категории множеств $\mathcal{S}et$, категории абелевых групп $\mathcal{A}b$, категории колец $\mathcal{R}ing$, категории топологических пространств $\mathcal{T}op$, и т.д.

Сейчас мы построим новую группу $G = \varinjlim G_i$, называемую **индуктивным пределом** или **прямым пределом** групп G_i. Для

Универсальное свойство.

Конструкция индуктивного предела. Фактор-группа слабого прямого произведения по подгруппе, определямой соотношениями.

Бесконечные объединения. Важнейший пример индуктивных примеров дается бесконечными объединениями фильтрующихся семейств подгрупп. Пусть группа G есть объединение своих подгрупп G_i, $I \in I$. Скажем, что $i \leq j$ в том и только том случае, когда $G_i \leq G_j$, а в качестве гоморфизма φ_i^j возьмем вложение G_i в G_j. Предположим, что для любых G_i, G_j найдется такая подгруппа G_h из того же семейства, что $G_i, G_j \leq G_h$. Тогда группа G является индуктивным пределом подгрупп G_i относительно вложений.

• Каждая группа есть индуктивный предел своих конечно порожденных подгрупп.

• Квазициклическая группа $\mu_{p^\infty} = \varinjlim \mu_{p^m}$ есть индуктивный предел конечных групп μ_{p^m}, корней из 1 степени p^m, относительно обычных вложений.

• Предельная линейная группа $\mathrm{GL}(R) = \varinjlim \mathrm{GL}(n, R)$ есть индуктивный предел своих подгрупп $\mathrm{GL}(n, R)$ относительно вложений

$$\mathrm{GL}(n, R) \longrightarrow \mathrm{GL}(m, R), \qquad x \mapsto \begin{pmatrix} x & 0 \\ 0 & e \end{pmatrix},$$

для всех $m \geq n$.

• Стринги

§ ?. Проективный предел

Пусть I — **фильтрованное вниз** частично упорядоченное множество. Это условие означает, что для любых $i, j \in I$ существует $h \in I$ такое, что $h \leq i, j$. Рассмотрим семейство групп G_i, $i \in I$ и предположим, что для каждой пары $i \leq j$ задан гомоморфизм $\varphi_i^j : G_i \longrightarrow G_j$ такой, что $\varphi_i^i = \mathrm{id}_{G_i}$ и для любых трех индексов $i \leq j \leq h$ выполняется равенство $\varphi_j^h \varphi_i^j = \varphi_i^h$. Семейство групп G_i вместе с семейством гомоморфизмов φ_i^j называется **фильтрованным вниз семейством** или **проективным семейством** групп (или иногда **обратным спектром** или **проективным спектром** групп).

Комментарий. С точки зрения теории категорий проективное семейство представляет собой просто *ковариантный* функтор из частично упорядоченного множества I, рассматриваемого как категория, в категорию групп $\mathcal{G}r$. Как и для индуктивных семейств аналогичную конструкцию можно рассмотреть для любой категории $\mathcal{C}$, скажем для категории множеств $\mathcal{S}et$, категории абелевых групп $\mathcal{A}b$, категории колец $\mathcal{R}ing$, категории топологических пространств $\mathcal{T}op$, и т.д. Многие авторы, однако, предпочитают рассматривать проективное семейство как *контравариантный* функтор из фильтрованного *вверх* частично упорядоченного множества в категорию групп или другую категорию. В этом случае они считают, что все стрелки направлены в противоположную сторону и, в частности, гомоморфизм $\varphi_j^i : G_i \longrightarrow G_j$ сопоставляется парам $i \geq j$.

Универсальное свойство.

Конструкция проективного предела. Подгруппа прямого произведения определямая соотношениями.

Примеры.

• аддитивная группа целых p-адических чисел $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ является проективным пределом групп $\mathbb{Z}/p^n\mathbb{Z}$ относительно проекций $\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}/p^m\mathbb{Z}$, $x \mapsto x^{p^{n-m}}$

• Унитреугольная группа $U(\mathbb{N}, R) = \varprojlim U(n, R)$ является проективным пределом групп $U(n, R)$ относительно проекций $U(n+1, R) \longrightarrow U(n, R)$, которое сопоставляет каждой матрице матрицу с обрезанными последней строкой и последним столбцом.

Сравнение индуктивного и проективного пределов. Индуктивный предел, как правило, значительно больше инъективного

Прямое произведение

$$\prod_{i\in I} G_i = \varprojlim \prod_{i\in J} G_i$$

является *проективным* пределом по всем *конечным* подмножествам $J \subseteq I$. Для сранения, слабое прямое произведение

$$\prod_{i\in I} G_i = \varprojlim \prod_{i\in J} G_i$$

является *индуктивным* пределом по всем *конечным* подмножествам $J \subseteq I$.

§ ?. Сплетение

§ ?. Тензорное произведение абелевых групп

Пусть A, B – две авелевы группы. Сейчас мы построим абелеву группу $A \otimes B$, называемую **тензорным произведением** абелевых групп A и B. Группа $A \otimes B$ порождена **разложимыми тензорами** $a \otimes b$, $a \in A$, $b \in B$. Разложимые тензоры билинейны по каждому аргументу:

$$\text{A1} \qquad (a_1 + a_2) \otimes b = a_1 \otimes b + a_2 \otimes b,$$
$$\text{A2} \qquad a \otimes (b_1 + b_2) = a \otimes b_1 + a \otimes b_2.$$

Иными словами, $A \otimes B$ можно рассматривать как *абелеву* группу с образующими $a \otimes b$, $a \in A$, $b \in B$, заданную соотношениями A1 и A2. То, что это группа абелева, означает, что, кроме того,

$$a_1 \otimes b_1 + a_2 \otimes b_2 = a_2 \otimes b_2 + a_1 \otimes b_1.$$

По определению каждый элемент $A \otimes B$ является суммой разложимых тензоров, т.е. имеет вид

$$a_1 \otimes b_1 + a_2 \otimes b_2 + \dots a_m \otimes b_m$$

для некоторого $m \in \mathbb{N}_0$ и некоторых $a_i \in A$, $b_i \in B$. Для общего кольца мы дополнительно требовали бы, чтобы $na \otimes b = n(a \otimes b) = a \otimes nb$, но для кольца $\mathbb{Z}$ это автоматически следует из аксиом A1 и A2.

Задача. Докажите, что $C_m \otimes C_n \cong C_{\gcd(m,n)}$.

§ ?. Тензорное произведение линейных групп

(H, U), (G, V)

Глава ?: АБЕЛЕВЫ ГРУППЫ

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. Тем не менее, нам хочется использовать эту теорему уже сейчас, до и независимо от общей теории. Поэтому в настоящем параграфе мы дадим непосредственное доказательство основной теоремы о конечных абелевых группах. Эта теорема была опубликована в 1879 году Фробениусом и Штикельбергером, причем их оригинальная статья занимала 46 страниц **большого формата** (в Journal für die reine und angewandte Mathematik). Наше доказательство будет несколько короче.

§ ?. Свободные абелевы группы

Пусть $x_1, \dots, x_n$ – элементы абелевой группы G. Рассмотрим отображение $\mathbb{Z}^n \longrightarrow G$, сопоставляющее набору $(m_1, \dots, m_n)$ целых чисел **линейную комбинацию** $m_1x_1 + \dots + m_nx_n \in G$ элементов $x_1, \dots, x_n$ с коэффициентами $(m_1, \dots, m_n)$. Линейная комбинация называется **тривиальной**, если $m_1 = \dots = m_n = 0$. Элементы $x_1, \dots, x_n$ называются **линейно независимыми**, если все нетривиальные линейные комбинации $x_1, \dots, x_n$ отличны от 0, т.е. если $m_1x_1 + \dots + m_nx_n \in G$ влечет $m_1 = \dots = m_n = 0$. Иными словами, элементы $x_1, \dots, x_n$ линейно независимы, если задаваемое ими отображение $\mathbb{Z}^n \longrightarrow G$ инъективно. В противном случае элементы $x_1, \dots, x_n$ 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 $x/y \notin \mathbb{Q}$.

Определение. *Абелева группа F называется* **свободной**, *если в ней существует линейно независимая система образующих.*

Линейно независимая система образующих называется **базисом** группы F. Таким образом, свободная группа это в точности абелева группа, в которой существует базис. Если $x_1, \dots, x_n$ – базис группы F, то отображение $\mathbb{Z}^n \longrightarrow F$, $(m_1, \dots, m_n) \mapsto m_1x_1 + \dots + m_nx_n$, биективно.

Теорема. *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

$$\psi(x) = \psi(m_1x_1 + \ldots + m_nx_n) = \\ = m_1\psi(x_1) + \ldots + m_n\psi(x_n) = m_1g_1 + \ldots + m_ng_n = \varphi(x).$$

Теорема. *Любые два базиса свободной абелевой группы F содержат одинаковое количество элементов.*

Доказательство. В самом деле, если $x_1, \ldots, x_n$ – базис F, а $y_1, \ldots, y_m$ – любая система элементов, то каждый из элементов y_i может быть выражен как линейная комбинация $x_1, \ldots, x_n$. Таким образом, $(y_1, \ldots, y_m) = (x_1, \ldots, x_n)a$ для некоторой матрицы $a \in M(n, m, \mathbb{Z})$. Если $y_1, \ldots, y_m$ в свою очередь является базисом группы F, то по той же причине $(x_1, \ldots, x_n) = (y_1, \ldots, y_m)b$ для некоторой матрицы $b \in M(m, n, \mathbb{Z})$. Таким образом, $(x_1, \ldots, x_n) = (x_1, \ldots, x_n)ab$ и $(y_1, \ldots, y_m) = (y_1, \ldots, y_m)ba$. Так как $x_1, \ldots, x_n$ и $y_1, \ldots, y_m$ базисы, то $ab = e \in \mathrm{GL}(n, \mathbb{Z})$ и $ba = e \in \mathrm{GL}(m, \mathbb{Z})$. Однако над кольцом $\mathbb{Z}$ не существует неквадратных двусторонне обратимых матриц.

§ ?. 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'.

Группа G называется **группой кручения**, если $T(G) = G$, и **группой без кручения**, если $T(G) = 0$. Любая конечная группа является группой кручения, а свободная группа – группа без кручения.

§ ?. Примарное разложение

Пусть $p \in \mathbb{P}$, $p||G|$. Обозначим через $G(p)$ множество всех элементов группы G, порядок которых равен p^m, $m \in \mathbb{N}$.

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 $(xy)^{p^n} = 1$.

Пусть G – конечная абелева группа. Подгруппа $G(p)$ называется **p-примарной компонентой** группы G. Разложение, существование которого утверждается в следующей теореме, называется **примарным разложением** (Primärzerlegung).

Теорема. *Если $p_1, \dots, p_s$ – все простые, делящие порядок группы G, то*

$$G = G(p_1) \oplus \dots \oplus G(p_s).$$

Доказательство. Докажем вначале единственность разложения. Пусть $x_i \in G(p_i)$, $x_1 \dots x_s = 1$. 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, $x_j = e$.

Докажем теперь существование разложения – ДОКАЗАТЬ!!!

§ ?. Разложение на циклические слагаемые

В неявном виде следующий результат был известен уже Гауссу, первые явные доказательства были даны в 1869 году Шерингом и в 1879 году Фробениусом и Штикельбергером.

Теорема. *Каждая конечная абелева группа является прямой суммой примарных циклических групп.*

Доказательство. Достаточно доказать, что любая абелева группа G, *не являющаяся* примарной циклической, допускает нетривиальное разложение в прямую сумму. По лемме ? 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 $x \in \operatorname{Ker}(\varphi) = H$, 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, $|G| = p|pG| = p^2|p^2 G| = \dots = p^{l-1}|p^{l-1} G| = p^l = |A|$, так что уже сама группа G является циклической, вопреки предположению.

элементарные 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

§ ?. Подгруппы свободной группы

В действительности классификацию конечно порожденных групп можно доказать иначе, так как мы это сделаем в Главе ? в контексте конечно порожденных модулей над кольцом главных идеалов. А именно, пусть G – любая абелева группа с системой образующих $g_1, \ldots, g_n$. Рассмотрим свободную абелеву группу F с базисом $x_1, \ldots, x_n$ той же мощности. Как мы знаем из § ?, существует гомоморфизм $\varphi : F \longrightarrow G$.

Теорема. *Каждая подгруппа свободной абелевой группы F является свободной абелевой группой ранга не превосходящего ранг F.*

Тема ?. ТЕОРЕМЫ СИЛОВА

Сейчас мы обсудим арифметические результаты, связывающие строение конечной группы с ее порядком.

§ 1. Центр p-группы, существование элемента порядка p, нормализаторное условие

Пусть $p \in \mathbb{P}$ – простое число.

Определение. *Конечная группа G называется* **p-группой**, *если $|G| = p^m$ для некоторого $m \in \mathbb{N}$.*

Следующее простое утверждение является ключом к десяткам арифметических фактов о конечных группах.

Лемма. *Пусть конечная группа G действует на конечном множестве X. Предположим, что индексы всех собственных подгрупп в G делятся на p. Тогда $|X^G| \equiv |X| \pmod{p}$.*

Доказательство. В самом деле, для любого элемента $x \in X$ имеется естественная биекция между его орбитой Gx и фактором по стабилизатору G/G_x. Орбита Gx в том и только том случае одноэлементна, когда $x \in X^G$ или, что то же самое, когда $G_x = G$. Во всех остальных случаях G_x – собственная подгруппа в G и, значит, $|Gx| = |G/G_x| = |G : G_x|$ делится на p. Утверждение леммы вытекает теперь из того, что X является дизъюнктным объединением различных орбит.

В частности, условие леммы выполнено для любой конечной p-группы $G \neq 1$.

Следствие 1. *Пусть конечная p-группа $G \neq 1$ действует на конечном множестве X. Тогда $|X^G| \equiv |X| \pmod{p}$.*

Применим это соображение к случаю, когда G действует на себе сопряжениями. В этом случае $X = G$ – это сама группа G, а множество X^G неподвижных точек – это в точности центр $C(G)$ группы G.

Следствие 2. *Если $G \neq 1$ – конечная p-группа, то $C(G) \neq 1$.*

Доказательство. В самом деле, по лемме $|C(G)| \equiv |G| \equiv 0 \pmod{p}$, а, так как $1 \in C(G)$, то в G имеется хотя бы один нетривиальный центральный элемент $g \neq e$.

Это утверждение можно уточнить.

Задача. Пусть G – конечная p-группа и $H \trianglelefteq G$, $H \neq 1$. Тогда $H \cap C(G) \neq 1$.

В большинстве учебников в этом месте не ссылаются на лемму, а переписывают ее доказательство на языке сопряженных классов. В самом деле, пусть X – система представителей сопряженных классов группы G (т.е. трансверсаль к отношению сопряженности в G). Тогда G является дизъюнктным объединением классов x^G, $x \in X$, причем класс x^G находится в естественном биективном соответствии с фактором по централизатору $G/C_G(x)$. Это позволяет нам написать следующее **классовое уравнение** (Klassengleichung, class equation)

$$|G| = \sum_{x \in X} |G : C_G(x)| = |C(G)| + \sum_{x \in X \setminus C(G)} |G : C_G(x)|,$$

из которого следует, что порядок $C(G)$ делится на p вместе с остальными слагаемыми. Однако часто удобно использовать лемму и в случае, когда порядок X не делится на p.

В действительности, эту формулу можно применить и к доказательству следующего фундаментального факта, являющегося слабой формой теоремой Коши (см. § 3 по поводу более общей формулировки и другого доказательства теоремы Коши).

Теорема Коши. *Если $p||G|$, то в G существует элемент g порядка p.*

Доказательство. Будем вести доказательство индукцией по $|G|$. Предположим, что для всех групп меньшего порядка теорема уже доказана. Если в G существует собственная подгруппа H, индекс которой взаимно прост с p, то по индукционному предположению уже в H найдется элемент порядка p. Поэтому можно считать, что индексы всех собственных подгрупп в G делятся на p и мы оказываемся в ситуации, рассмотренной в лемме. Рассматривая, как и в Следствии 2, действие G на себе сопряжениями, мы видим, что $p||C(G)|$. Существование в $C(G)$ элемента порядка p вытекает теперь из структурной теории конечных абелевых групп.

Приведем еще одну важную иллюстрацию использования нашей леммы. А именно, сейчас мы докажем, что конечные p-группы удовлетворяют **нормализаторному условию**: каждая собственная подгруппа отлична от своего нормализатора.

Следствие 3. *Если G конечная p-группа и $H < G$, то $H < N_G(H)$.*

Доказательство. Если $H \trianglelefteq G$, то $N_G(H) = G$, так что доказывать нечего. Пусть, поэтому, $N_G(H) < G$. Обозначим через X множество подгрупп в G, сопряженных с H. Тогда H лействует на X сопряжением. Число одноэлементных орбит сравнимо с $|X| = |G : N_G(H)|$ по модулю p и, значит, делится на p. Так как одна такая орбита, а именно, $\{H\}$, существует, то существует еще по крайней мере одна такая орбита $\{gHg^{-1}\} \neq \{H\}$, где $g \in G$, Таким образом, $hgHg^{-1}h^{-1} = gHg^{-1}$ для любого $h \in H$ или, что то же самое, $g^{-1}hgHg^{-1}h^{-1}g = H$. Тем самым, $g^{-1}hg \in N_G(H)$. Но так как $g^{-1}Hg \neq H$, то найдется такое $h \in H$, что $g^{-1}hg \notin H$. Но это и значит, что $H < N_G(H)$.

Задача. Докажите, что каждая максимальная подгруппа конечной p-группы нормальна в ней и имеет индекс p.

§ 2. Принцип инволюций

В действительности лемма предыдущего параграфа имеет весьма небанальные приложения уже для частного случая $p = 2$. Специалисты по теории групп называют **инволюцией** элемент порядка 2, т.е. такой $h \in G$, что $h^2 = 1$, но $h \neq 1$ (стоит отметить, что большинство остальных алгебраистов называет инволюцией элемент, порядок которого *делит* 2, а чтобы подчеркнуть, что $h \neq 1$, говорят о **нетривиальной инволюции**!) Если группа G действует на множестве X, то под действием инволюции h множество X разбивается на *одноэлементные* орбиты $\{x\}$, отвечающие **инвариантным элементам** $x = hx$, и двухэлементные орбиты $\{x, y\}$, отвечающие **энантиоморфным парам** x, y, где $y = hx \neq x$. Лемма предыдущего параграфа в применении к инволюциям

означает, $|X^h| \equiv |X| \pmod 2$. Тем самым, если h, g – любые две инволюции, то $|X^h| \equiv |X^g| \pmod 2$. В частности, если инволюция h имеет на X *нечетное количество* неподвижных точек, то и любая другая инволюция g имеет на X по крайней мере одну неподвижную точку. Это несложное соображение, называемое **принципом инволюций**, имеет далеко идущие следствия.

Теорема Ферма. *Любое простое $p \equiv 1 \pmod 4$ представимо в виде суммы двух квадратов. Иными словами, найдутся такие $m, n \in \mathbb{N}$, что $p = m^2 + n^2$.*

Доказательство Цагира. (Взято из файла Involutions на домашней странице harald.fripentinger@kfunigraz.ac.at.) Рассмотрим множество

$$X = \{(x, y, z) \mid x, y, z \in \mathbb{N}, x^2 + 4yz = p\}.$$

Легко видеть, что отображение $h : X \longrightarrow X$ заданное посредством

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z), & \text{если } x < y - z, \\ (2y - x, y, x - y + z), & \text{если } y - z < x < 2y, \\ (x - 2y, x - y + z, y), & \text{если } 2y < x, \end{cases}$$

является инволюцией (проверьте!). Ясно, что у этой инволюции ровно одна неподвижная точка на X, а именно, $(1, 1, l)$, где $p = 4l + 1$. По принципу инволюций тогда инволюция $g : X \longrightarrow X$, $(x, y, z) \mapsto (x, z, y)$, тоже имеет по крайней мере одну неподвижную точку (m, n, n), так что $p = m^2 + 4n^2$, как и утверждалось.

§ 3. Количество подгрупп p-группы

В настоящем параграфе мы обсудим чуть более рафинированные следствия леммы $|X^G| \equiv |X| \pmod p$. Содержание этого пункта воспроизводит стр.75–77 книги [Ro].

1. Количество подгрупп порядка p. Мы продолжаем считать, что G – конечная p-группа. Рассуждение, возникающее в доказательстве следующей леммы, уже встречалось нам в Главе 3, когда мы доказывали, что в группе с двумя классами сопряженных элементов не может быть элементов конечного порядка.

Лемма. *Если $H \trianglelefteq G$, $|H| = p$, то $H \leq C(G)$.*

Доказательство. В самом деле, пусть $H = \langle h \rangle$, $h^p = 1$, такая подгруппа, что $gHg^{-1} = H$, однако, вопреки ожиданиям, $ghg^{-1} \neq h$. Ясно, что это возможно только при $p \geq 3$. Пусть $ghg^{-1} = h^m$ для некоторого $1 < m < p$. Тем самым, $h = g^p h g^{-p} = h^{m^p}$ и, значит, $h^{m^p - 1} = 1$, так что $p | m^p - 1$. С другой стороны, теорема Ферма утверждает, что $p | m^{p-1} - 1$ и, значит, $p | m^{p-1}$, противоречие.

Предложение 1. *Количество $r_1(G)$ подгрупп порядка p в конечной p-группе G сравнимо с 1 по модулю p.*

Доказательство. Обозначим через X множество всех подгрупп порядка p в G. Орбита группы $H \in X$ относительно действия G сопряжениями в том и только том случае одноэлемента, когда $H \trianglelefteq G$, а по предыдущей лемме все такие подгруппы центральны. Таким образом, количество подгрупп порядка p в G сравнимо с количеством *центральных* подгрупп порядка p по модулю p. Это значит, что нам осталось лишь посчитать подгрупп порядка p в *абелевой* группе $C(G)$. Все элементы порядка p в группе $C(G)$ вместе с 1 образуют группу $F \leq C(G)$ изоморфную элементарной абелевой группе E_{p^m}. Каждый $\neq 1$ элемент F порождает единственную подгруппу порядка p, причем каждая подгруппа порядка p в F порождается ровно $p - 1$ своими элементами. Таким образом, всего в $C(G)$ имеется

$$\frac{p^m - 1}{p - 1} = p^m + \ldots + p + 1$$

подгрупп порядка p.

Следствие. *Если G конечная p-группа и $|F| = p^s < |G|$, то количество подгрупп в G порядка p^{s+1}, содержащих F сравнимо с 1 по модулю p.*

Доказательство. Пусть $F \leq H \leq G$, $|H| = p^{s+1}$. Тогда F нормальна в H (например, потому что $|H : F| = p$ – наименьший простой делитель $|H|$). Тем самым, $H \leq N_G(F)$. Это значит, что количество подгрупп H равно количеству подгрупп порядка p в p-группе $N_G(F)/F$, которое, как мы знаем, сравнимо с 1 по модулю p.

Слежующий результат двойственен к Предложению 1 и легко получается как его следствие.

Предложение 2. *Количество подгрупп индекса p в конечной p-группе G сравнимо с 1 по модулю p.*

Доказательство. Пусть $H < G$ подгруппа индекса p. Тогда $x^p \in H$ для любого $x \in G$. Тем самым, все подгруппы индекса p содержат подгруппу $F = \langle x^p \mid x \in G\rangle$. Таким образом, количество подгрупп индекса p в G равно количеству подгрупп в фактор-группе G/F, которая изоморфна элементарной абелевой группе E_{p^m}. Рассматривая E_{p^m} как m-мерное векторное пространство над полем $\mathbb{F}_p$, мы видим, что количество подгрупп индекса p равно количеству подгрупп порядка p равно $p^m + \ldots + p + 1$.

2. Количество подгрупп порядка p^s. Сформулированные в предыдущем пункте предложении легко обобщается на подгруппы произвольного порядка.

Теорема. *Количество $r_s(G)$ подгрупп порядка $p^s||G|$ в конечной p-группе G сравнимо с 1 по модулю p.*

Доказательство. Сейчас мы покажем, что для любого s такого, что $p^s < |G|$ выполняется сравнение $r_s(G) \equiv r_{s+1} \pmod p$, так что наше утверждение получается индукцией по s, если учесть, что по теореме предыдущего пункта $r_1(G) \equiv 1 \pmod p$. Мы могли бы взять в качестве базы индукции $r_0(G) = 1$, но Предложение 1 предыдущего пункта нужно нам для доказательства следствия, на котором основан индукционный шаг.

В самом деле, пусть $H_1, \ldots, H_q$, $q = r_s(G)$, суть все подгруппы порядка p^s, а $F_1, \ldots, F_t$, $t = r_{s+1}(G)$, суть все подгруппы порядка p^{s+1}. Пусть H_i содержится в l_i из подгрупп $F_1, \ldots, F_t$, а F_j содержит в m_j из подгрупп $H_1, \ldots, H_q$. Подсчитывая двумя способами порядок множества

$$\{(H, F) \mid |H| = p^s, |F| = p^{s+1}, H < F\},$$

получаем

$$l_1 + \ldots + l_q = m_1 + \ldots + m_t.$$

По следствию из Предложению 1 имеем $l_i \equiv 1 \pmod p$, а по Предложению 2 имеем $m_j \equiv 1 \pmod p$. Таким образом, $q \equiv t \pmod p$, как и утверждалось.

Задача. Докажите, что количество нормальных подгрупп порядка p^s конечной p-группы G сравнимо с 1 по модулю p.

Следствие. *Для любого $p^s||G|$, группа G содержит нормальную подгруппу H порядка p^s.*

§ 4. Решения уравнения $x^n = e$, теоремы Коши и Фробениуса

В этом параграфе G обозначает конечную группу, $p \in \mathbb{P}$ – простое число, а $n \in \mathbb{N}$ – произвольное натуральное число. Мы интересуемся решениями уравнения $x^n = e$ в группе G.

1. Теорема Коши. Точная формулировка теоремы Коши такова.

Теорема Коши. *Если $p||G|$, то число решений в G уравнения $x^p = 1$ делится на p.*

Доказательство Маккея[276]. Образуем множество

$$X = \{(g_1, \ldots, g_p) \mid g_i \in G, g_1 \ldots g_p = e\}.$$

[276] J.H.McKay, Another proof of Cauchy's group theorem. – Amer. Math. Monthly, 1959, vol.66, p.119.

Ясно, что $|X| = |G|^{p-1}$ делится на p. Циклическая группа $C_p = \langle\sigma\rangle$ действует на этом множестве посредством длинного цикла `RotateRight`:

$$\sigma(g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}).$$

В самом деле, $g_p g_1 \ldots g_{p-1} = g_p(g_1 \ldots g_p)g_p^{-1} = g_p e g_p^{-1} = e$. Все орбиты C_p на X имеют порядок 1 или p, причем порядок орбиты в том и только том случае равен 1, когда $g_1 = \ldots = g_p = g$, где $g^p = e$. Это значит, что число решений уравнения $x^p = 1$ в группе G равно $|X_0|$. Но ведь по Лемме ?, выполняется сравнение $|X_0| \equiv |X| \pmod p$.

Замечание (Авиноам Манн). Если $p \not| |G|$, то доказательство Маккея показывает, что $|G|^{p-1} \equiv 1 \pmod p$. Таким образом, мы получили еще одно доказательство теоремы Ферма!

Ю.И.Манин сказал: "хорошее доказательство – это доказательство, которое делает нас умнее". Доказательство Маккея действительно делает нас умнее. Оно сообщает нам важный общий принцип, что, если под рукой нет множества, на котором действует группа, нужно создать такое множество. Кроме того, оно показывает, что в действительности, часто значительно проще доказать более точный или более сильный результат, чем то, к чему мы первоначально стремились. В частности, мы получили новый подход к доказательству следующего факта, который нам уже известен.

Следствие 1. *Если $p||G|$, то в G существует элемент g порядка p.*

Доказательство. По теореме число решений уравнения $x^p = e$ делится на p. Однако это уравнение имеет по крайней мере одно решение, а именно $x = e$. Тем самым, оно имеет и нетривиальное решение $x = g \neq e$.

Следствие 2. *Если $p||G|$, то количество подгрупп порядка p в G сравнимо с 1 по модулю p.*

Доказательство. Пусть $P_1, \ldots, P_m$ – все различные подгруппы порядка p в G. Ясно, что $P_1 \cup \ldots \cup P_m = G(p)$, где $G(p) = \{g \in G \mid g^p = e\}$ – множество решений уравнения $x^p = e$. Так как $P_i \cap P_j = \{e\}$ для любых $i \neq j$, то $|G(p)| = |P_1 \cup \ldots \cup P_m| = m(p-1) + 1$. По теореме Коши это число делится на p.

2. Теорема Фробениуса. Можно спросить себя, верен ли аналог теоремы Коши для решений уравнения $x^n = e$? Это действительно так, хотя доказательство этого факта уже значительно труднее.

Теорема Фробениуса. *Если $n||G|$, то число решений в G уравнения $x^n = 1$ делится на n.*

К сожалению, из теоремы Фробениуса не следует, что в G найдется элемент порядка n. Для того, чтобы убедиться в этом, достаточно посмотреть на четверную группу $V = C_2^2$, в которой нет элементов порядка 4, или на симметрическую группу S_3, в которой нет элементов порядка 6. Теорема Фробениуса утверждает лишь, что число элементов, порядки которых **делят** n сравнимо с 0 по модулю n.

Упомянем также следующее усиление теоремы Фробениуса, которое, фактически, и доказывается в [Холл], теорема 9.1.1.

Теорема Фробениуса–Холла. *Для любого класса сопряженных элементов C группы G, число решений уравнений $x^n = c$, $c \in C$, делится на* $\gcd(n|C|, |G|)$.

§ 5. Теоремы Силова

Пусть, как обычно, G – конечная группа, а $p \in \mathbb{P}$ – простое число. Пусть $|G|_p$ – наибольшая степень p, делящая порядок группы G. Иными словами, $|G|_p = p^m$, где $p^m \mid |G|$, а $p^{m+1} \not| |G|$.

Определение. *Любая подгруппа $P = S_p(G) \leq G$ порядка p^m называется* **Силовской p-подгруппой**. *Множество силовских p-подгрупп в G обозначается через* $\mathrm{Syl}_p(G)$.

Наибольшая степень p, делящая $|G|$ часто обозначается также через $|G|_p$. Таким образом, по определению $|P| = |G|_p$ так что индекс $|G : P|$ взаимно прост с p. Подгруппа в G, являющаяся p-силовской для какого-то p обычно называется просто **силовской**. Следующий факт, доказанный в 1872 году Силовом[277] является *самым* важным арифметическим утверждением о конечных группах[278].

Теорема Силова. *Пусть G – конечная группа, $p \in \mathbb{P}$. Тогда*

$\mathbf{E}_p$: *в G существуют p-силовские подгруппы;*

$\mathbf{C}_p$: *все силовские p-подгруппы в G сопряжены;*

$\mathbf{D}_p$: *любая p-подгруппа содержится в некоторой силовской;*

$\mathbf{F}_p$: *число силовских p-подгрупп сравнимо с 1 по модулю p.*

Иногда частям этой теоремы дают отдельные названия. В учебниках утверждение о существовании Силовских подгрупп обычно называется **первой теоремой Силова**, утверждение об их сопряженности – **второй теоремой Силова**, а утверждение об их количестве – **третьей теоремой Силова** (см., например, [Ha]). В действительности, утверждение $\mathbf{F}_p$ было доказано в 1895 году Фробениусом. Обозначение $\mathbf{E}_p$ является сокращением от Existence, а $\mathbf{C}_p$ – от Conjugacy, насколько я понимаю, буквы $\mathbf{D}_p$ и $\mathbf{F}_p$ выбраны по принципу близости в алфавите. Доказательство всех этих результатов будет вестись индукцией по $|G|$. Предположим, что для всех групп меньшего порядка теорема уже доказана.

Доказательство первой теоремы Силова. Если G – абелева, наше утверждение следует из теории конечно-порожденных абелевых групп. Если $p||C(G)|$, то фактор-группа $G/S_p(C(G))$ имеет меньший порядок, чем G и, следовательно, по индукционному предположению в ней существует силовская p-подгруппа,

[277] **Людвиг Силов** (12.12.1832, Христиания (Осло) – 07.09.1918) – замечательный норвежский математик. Не получив (как и Абель!) работу в университете, с 1855 работал школьным учителем, вначале в Христиании, потом в Фредрикхальде (с нагрузкой 25 аудиторных часов в неделю!) В 1862–63 годах Силов читал в университете лекции по теории Галуа и группам подстановок. В это время его учеником становится Софус Ли. Теорема Силова была доказана в 1872 году и в том же году опубликована в Math. Annalen. Жордан написал Силову, что много думал о его теореме и считает ее 'одним из главных пунктов теории перестановок'. Следующие 8 лет Силов работал над подготовкой нового издания трудов Абеля. Только в 1898 году, после ухода на пенсию как школьный учитель по ходатайству Ли Силов был зачислен экстраординарным профессором. Еще одним знаменитым учеником Силова был Сколем.

[278] Л.А.Шеметков, Два направления в развитии теории непростых конечных групп. – Успехи. Мат. Наук, 1975, т.30, N.2, с.179–198. Первый параграф этой статьи содержит биографию Силова, а второй – детальное обсуждение теоремы Силова и ее обобщений.

полный прообраз которой в G будет силовской подгруппой. Будем поэтому считать, что $p \nmid |C(G)|$. Рассмотрим орбиты G относительно действия на себе внутренними автоморфизмами. Пусть X – какая-то система представителей классов сопряженных элементов. Записывая, как в § ? формулу для порядка группы

$$|G| = |C(G)| + \sum_{x \in X \setminus C(G)} |G : C_G(x)|,$$

и вспоминая, что теперь $|G|$ делится на p, а $|C(G)|$ – нет, мы видим, что в G найдется *нецентральный* элемент x такой, что $|G : C_G(x)|$ взаимно просто с p. По индукционному предположению в $C_G(x)$ существует силовская подгруппа $P = S_p(C_G(x))$, а так как $|C_G(x)|_p = |G|_p$, то P продолжает оставаться силовской p-подгруппой и в G.

Доказательство второй теоремы Силова. Мы докажем $\mathbf{C}_p$ одновременно с $\mathbf{D}_p$. Очевидно, для этого достаточно доказать, что если $P = S_p$ – фиксированная силовская p-подгруппа в G, а $H \leq G$ – *любая* p-подгруппа, то H сопряжена в G с некоторой подгруппой в P. В самом деле, H действует на множестве $X = G/P$ правых смежных классов G по P левыми сдвигами. Так как H является p-группой, а $|X| = |G : P|$ взаимно просто с p, то по лемме § ? $|X^H| \not\equiv 0 \pmod{p}$, так что, в частности, $X^H \neq \varnothing$. Иными словами, существует такой смежный класс xP, что $HxP = xP$. Перенося в этом равенстве x в левую часть, видим, что $x^{-1}HxP = P$, так что $x^{-1}Hx \leq P$, что и требовалось доказать.

Доказательство третьей теоремы Силова. Рассмотрим действие силовской p-подгруппы P сопряжениями на множестве X всех силовских p-подгрупп. Класс $\{Q\}$, $Q \in X$ в том и только том случае одноэлементен, когда P нормализует Q. Однако в этом случае PQ является p-подгруппой и, значит, обязана совпадать с P. Таким образом, к этого действия имеется единственный одноэлементный класс, в то время как порядки всех остальных классов делятся на p.

Третья теорема Силова допускает следующее обобщение в духе результатов § 2 о количестве подгрупп в конечных p-группах.

Задача. Пусть $p^s || |G|$. Докажите, что количество подгрупп порядка p^s в G сравнимо с 1 по модулю p.

Упражнение. Силовская p-подгруппа P группы G в том и только том случае является единственной силовской p-подгруппой, когда $P \trianglelefteq G$.

Упражнение. Опишите силовские подгруппы прямого произведения $H \times G$.

Упражнение. Докажите, что если $H \leq G$, а P и Q – две p-силовские подгруппы группы H, то они не могут содержаться в одной и той же силовской подгруппе группы G.

§ 6. Доказательство Виландта

Сейчас мы дадим еще одно доказательство первой теоремы Силова. Это доказательство было открыто Виландтом в 1859 году, до этого стандартным доказательством теоремы Силова считалось доказательство Фробениуса. Как отмечает Джозеф Ротман ([Ro], стр.80), доказательство Виландта совершенно удивительно, так как оно не использует ничего из установленного нами ранее, кроме связи орбит и стабилизаторов, в том числе и теорему Коши. Таким образом, это доказательство дает, в частности, еще одно, третье, доказательство теоремы Коши (в [Ro] она так и доказывается!) Это доказательство опирается на следующее элементарное свойство биномиальных коэффициентов ([Ro], Лемма 4.16 или [Ro], стр.39).

Лемма. *Пусть $p \not| m$. Тогда для всех $l \leq 1$ биномиальный коэффициент $\binom{p^l m}{p^l}$ не делится на p.*

Доказательство. В самом деле,

$$\binom{p^l m}{p^l} = \frac{m(p^m - 1)\dots(p^l m - p^l + 1)}{1 \cdot 2 \cdot \dots \cdot (p^l - 1)}.$$

Рассмотрим рациональное число $\dfrac{p^l m - i}{i}$, $1 \leq i < p^l$. Если $p^j | i$, то $j < l$ и $p^j | p^l m - i$. С другой стороны, если $p^j | p^l m - i$, то $j < l$ и $p^j | i$. Таким образом, $v + p(i) = v_p(p^l m - i)$, что и требовалось доказать.

Доказательство Виландта. Пусть $|G| = p^l m$, где $p \not| m$. Обозначим через X множество всех подмножеств порядка p^l в G. Количество таких подмножеств равно $\binom{p^l m}{p^l}$ и по лемме оно не делится на p. Заставим группу G действовать на X сдвигами: для любого $A \in X$ имеем $gA = \{ga \mid a \in A\}$. Так как $p \not| |X|$, то существует орбита, порядок которой не делится на p. Возьмем $A \in Y$, содержащееся в такой орбите и рассмотрим его стабилизатор $H = G_A \leq G$. Тогда $|A| = |G : H|$ не делится на p и, значит, $|H|$ делится на p^m. С другой стороны, для любого $a \in A$ и любого $g \in H$ имеем $ga \in gA = A$. При этом, для двух любых $h, g \in H$ из того, что $ha = ga$ следует $h = g$, так что $|H| \leq |A| = p^m$. Но это и значит, что $|H| = p^m$.

§ 7. Нормализатор силовской подгруппы

Аргумент Фраттини. *Пусть $H \trianglelefteq G$ и P – силовская p-подгруппа H. Тогда $G = HN_G(P)$.*

Доказательство. Для любого $g \in G$ подгруппа $gPg^{-1} \leq gHg^{-1} = H$ является силовской подгруппой в H. Так как силовские подгруппы в H сопряжены, то найдется такое $h \in H$, что $gPg^{-1} = hPh^{-1}$ и, следовательно, $h^{-1}gPg^{-1}h = P$. Это значит, что $h^{-1}g \in N_G(P)$ и, окончательно, $g = h(h^{-1}g) \in HN_G(P)$.

Задача. Пусть $H \trianglelefteq G$, P – силовская p-подгруппа в G. Покажите, что

i) $H \cap P$ силовская p-подгруппа в H;

ii) HP/H силовская p-подгруппа в G/H.

Справедливо ли i), если не предполагать, что подгруппа H нормальна?

Теорема. *Если P – силовская подгруппа конечной группы G, то $N_G(P)$ абнормальная в G.*

§ 8. Силовские подгруппы в S_n

В качестве иллюстрации сейчас мы опишем силовские подгруппы симметрических групп. Для этого нам придется ввести еще одну важнейшую конструкцию над группами перестановок.

1. Сплетение групп перестановок. Пусть $F \leq S_m$ и $H \leq S_n$ – группы перестановок множеств $X = \underline{m}$, $Y = \underline{n}$. Обозначим через $F \wr H$ подгруппу в симметрической группе S_{mn}, рассматриваемой как группа перестановок множества $X \times Y$, состоящую из всевозможных перестановок вида

$$(x, y) \mapsto (\pi_y(x), \sigma y), \qquad \pi_y \in F,\ \sigma \in H.$$

Группа $F \wr H$ называется **сплетением** групп перестановок F и H. Иными словами, мы представляем себе множество $F \times H$ как прямоугольную таблицу, столбцы которой занумерованы элементами множества X, а строки –

элементами множества Y. При этом общий элемент сплетения действует следующим образом: в каждом столбце действует какой-то элемент группы F (в каждом столбце свой!) и, кроме того, столбцы переставляются между собой при помощи какого-то элемента множества H. Таким образом, общий элемент группы $F \times H$ описывается следующим набором из $n+1$ перестановки $\theta = (\pi_1, \ldots, \pi_n, \sigma)$. Ясно, что при $m, n \geq 2$ эта группа импримитивна: два элемента одного столбца остаются под действием любого элемента группы $F \times H$ в одном столбце. Тем самым, столбцы этой таблицы являются блоками импримитивности группы $F \times H$.

Задача. Покажите, что если F и H транзитивны, то $F \wr H$ тоже транзитивна.

Ясно, что группа $F \times H$ содержит подгруппу $D(F)$, состоящую из всех перестановок, оставляющих на месте все столбцы и действующих в каждом столбце некоторым элементом из F (зависящим от столбца!). Во введенных выше обозначениях группа $D(F)$ состоит в точности из всех элементов θ, для которых $\sigma = 1$. Эта группа изоморфна F^n и является нормальным делителем в $F \times H$, причем фактор-группа по ней изоморфна H. С другой стороны, ясно, что $F \times H$ содержит изоморфную H подгруппу, состоящую из всех θ, для которых $\pi_1 = \ldots = \pi_n = 1$. Легко видеть, что $F \times H = D(F) \leftthreetimes H$. В частности, порядок $F \times H$ равен $|F|^n|H|$.

Тем самым, сплетение групп перестановок не может быть коммутативным, так как порядок $H \times F$ равен $|F| \cdot |H|^m$. В то же время, легко проверить, что оно ассоциативно, в том смысле, в котором может быть ассоциативной операция над группами, т.е. с точностью до *изоморфизма*. Иными словами, если G – третья группа перестановок, действующая на множестве Z, то $(F \wr H) \wr G \cong F \wr (H \wr G)$. Более того, если отождествить каждое из множеств $(X \times Y) \times Z$ и $X \times (Y \times Z)$ с $X \times Y \times Z$, то эти группы даже *совпадают*, так что в дальнейшем мы будем писать просто $F \wr H \wr G$. Тем самым, понятие сплетения может быть распространено на случай произвольного конечного числа групп перестановок. В самом деле, если $G_1, \ldots, G_r$ – группы перестановок, причем сплетение групп перестановок в количестве $r-1$ штуки уже определено, то, *как обычно*, мы полагаем $G_1 \wr \ldots \wr G_r = (G_1 \wr \ldots \wr G_{r-1}) \wr G_r$.

2. Силовские подгруппы в S_n. Определим, прежде всего, чему равен *порядок* $|S_n|_p$ силовской подгруппы в S_n, или, что то же самое, чему равна наибольшая степень простого числа p, делящая $n!$.

Лемма. *Наибольшая степень p делящая $n!$ равна p^m, где*

$$m = v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Доказательство. В самом деле, среди чисел от 1 до n ровно $\left\lfloor \frac{n}{p} \right\rfloor$ делятся на p, ровно $\left\lfloor \frac{n}{p^2} \right\rfloor$ делятся на p^2, ровно $\left\lfloor \frac{n}{p^3} \right\rfloor$ делятся на p^3 и т.д.

В частности, силовская p-подгруппа симметрической группы S_{p^r} имеет порядок $p^{p^{r-1}+\ldots+p+1}$. Ясно, что $|S_p|_p = p$ и, тем самым, силовская p-подгруппа в S_p имеет вид C_p. Далее, $|S_{p^2}|_p = p^{p+1}$ так что в качестве силовской p-подгруппы в S_{p^2} можно взять $C_p \wr C_p$. Аналогичное вычисление убеждает, что в качестве

силовской p-подгруппы в S_{p^3} можно взять сплетение $C_p \wr C_p \wr C_p$ порядка p^{p^2+p+1}. Вообще для любого r силовская p-подгруппа в S_{p^r} имеет вид $C_p \wr \ldots \wr C_p$, где количество сплетаемых циклических факторов равно r.

Выразим теперь произвольное n в p-ичной системе счисления: $n = a_m p^m + \ldots + a_1 p + a_0$. Тогда порядок силовской подгруппы в S_n совпадает с порядком силовской подгруппы в подгруппе Юнга $(S_{p^m})^{a_m} \times \ldots \times (S_p)^{a_1}$. Таким образом, мы доказали следующий результат.

Теорема Калужнина. *Пусть $n = a_m p^m + \ldots + a_1 p + a_0$, где $0 \leq a_i < p$. Тогда в качестве силовской подгруппы в S_n можно взять*

$$\Big(\underbrace{C_p \wr \ldots \wr C_p}_{m} \Big)^{a_m} \times \ldots \times C_p^{a_1}.$$

§ 9. Группы порядка pq, метациклические группы

Теорема Силова является чрезвычайно мощным средством для изучения конечных групп.

1. Группы порядка pq. Сейчас мы полностью опишем группы порядка $n = pq$, где $p, q \in \mathbb{P}$, $p < q$. Мы настоятельно рекомендуем читателю, прежде, чем двигаться дальше, самостоятельно разобрать первый интересный случай.

Задача. Докажите, что единственная группа порядка $15 = 3 \cdot 5$ циклическая.

А теперь обобщим этот результат.

Теорема. *Группа G порядка $n = pq$, где $p, q \in \mathbb{P}$, $p < q$, является полупрямым произведением $C_p \leftthreetimes C_q$, для некоторого действия $C_p \longrightarrow \mathrm{Aut}(C_q)$ группы C_p на C_q. В частности, если $p \nmid q-1$, то единственная группа порядка pq это циклическая группа C_{pq}.*

Доказательство. Согласно первой теореме Силова в G существует силовская подгруппа P порядка p и силовская подгруппа Q порядка q. По третьей теореме Силова количество силовских q-подгрупп сравнимо с 1 по модулю q. Но ведь количество сопряженных с Q равно $|G : N_G(Q)|$ и, значит, обязано делить n, а никаких делителей вида $1 + mq$, $m \in \mathbb{N}$, у n не наблюдается. Это значит, что Q – единственная силовская q-подгруппа в G, так что $Q \trianglelefteq G$.

Итак, подгруппы P и Q имеют следующим условиям: $G = PQ$, $P \cap Q = 1$, $Q \trianglelefteq G$. Это в точности означает, что $G = P \leftthreetimes Q$. Такие полупрямые произведения параметризуются гомоморфизмами $\varphi : C_p \mapsto \mathrm{Aut}(C_q) \cong C_{q-1}$. Если $p \nmid q-1$, то таких гомоморфизмов, кроме тривиального, не существует. Таким образом, в этом случае $G = P \times Q \cong C_p \times C_q \cong C_{pq}$.

С другой стороны, если $p | q-1$, то существуют нетривиальные гомоморфизмы. Пусть $P = \langle x \rangle$, $Q = \langle y \rangle$. Так как Q нормальна, то $xyx^{-1} = y^r$ для некоторого $1 < r < q$. Итерируя эту формулу мы получаем $x^2yx^{-2} = xy^rx^{-1} = y^{r^2}$ и вообще $x^myx^{-m} = y^{r^m}$. Тем самым, $y = x^pyx^{-p} = y^{r^p}$ и, так как порядок y равен q, то $r^p \equiv 1 \pmod{q}$. Это условие на r является необходимым и достаточным для существования неабелевой группы G порядка pq с заданием

$$G = \langle x, y \mid x^p = 1, y^q = 1, xyx^{-1} = y^r \rangle.$$

При этом ясно, что замена r на r^l, $1 < l < p$, не меняет класса изоморфизма группы G, так как она отвечает замене образующей x на x^l.

Задача. Докажите, что C_6 и $D_3 = S_3$ являются единственными неизоморфными группами порядка 6. Найдите количество неизоморфных групп порядков 10, 14, 21, 22, 26 и 39.

2. Метациклические группы. Вообще, группа G, в которой есть циклическая нормальная подгруппа, фактор-группа по которой тоже циклическая, называется **метациклической**. Полученное в предыдущем пункте описание групп порядка pq легко обобщается на этот случай.

Задача. Пусть G конечная группа порядка mn в которой найдется нормальная подгруппа $H \trianglelefteq G$, $H \cong C_m$ такая, что $G/H \cong C_n$. Показать, что G может быть следующим образом задана образующими и соотношениями:

$$G = G(m, n, r, s) = \langle x, y \mid x^m = e, y^n = x^r, yxy^{-1} = x^s \rangle,$$

где r и s – такие целые, что $r(s-1)$ и $s^n - 1$ кратны m.

Указание. Как обычно, пусть $H = \langle x \rangle$ и $G/H = \langle yH \rangle$. Выразить $y^n x y^{-1}$ и $y x^r y^{-1}$ через степени x.

§ 10. Группы порядка p^3, экстраспециальные группы

В настоящем параграфе через p обозначается простое число. Как мы знаем, каждая группа порядка p^2 абелева. Сейчас мы воспроизведем полученную в 1893 году О.Гельдером[279] классификацию групп порядка p^3.

Определение. *Конечная p-группа называется* **экстраспециальной**, *если ее центр совпадает с коммутантом и имеет порядок p.*

Лемма. *Любая неабелева группа G порядка p^3 экстраспециальна.*

Доказательство. Так как центр p-группы нетривиален, то $|C(G)|$ делится на p. Однако фактор-группа по центру не может быть циклической, так как иначе G была бы абелевой. Это значит, что $|C(G)| = p$, а факторгруппа $G/C(G)$ имеет порядок p^2 и, тем самым, изоморфна $C_p \times C_p$. Однако коммутант является *наименьшей* подгруппой, фактор-группа по которой абелева, так что $[G, G] \leq C(G)$. Так как G неабелева, то $[G, G] \neq 1$. Это и значит, что $[G, G] = C(G)$ имеет порядок p.

Теорема. *Для каждого p имеется две неизоморфных неабелевых группы порядка p^3. Для $p = 2$ это диэдральная группа D_4 и группа кватернионов Q. Для нечетного p существуют ровно две таких группы, которые различаются тем, что в одной из них все элементы имеют порядок p, а вторая содержит элемент порядка p^2.*

Доказательство. Для $p = 2$ ситуация особая: если все элементы группы имеют порядок 2, то группа абелева. Поэтому в неабелевой группе порядка 8 есть элемент порядка 4 и нам уже известно, что имеется ровно две таких группы, D_4 и Q. Для нечетного p имеется следующая альтернатива: либо порядок всех элементов группы G равен p, либо в ней существует элемент порядка p^2.

Если все элементы G имеют порядок p, то возьмем элементы x, y, образы которых при факторизации по центру порождают $G/C(G)$. Тогда $x^p = y^p = 1$ и $z = [x, y] \in C(G)$. Равенство $z = 1$ невозможно, так как иначе группа G была бы абелевой. Это значит, что элемент z порождает $C(G)$ и, тем самым, группа G задается соотношениями

$$G = \langle x, y \mid x^p = 1, y^p = 1, [x, y]^p = 1, [x, y]x = x[x, y], [x, y]y = y[x, y] \rangle.$$

[279] O.Hölder, Die Gruppen der Ordnungen p^3, pq^2, pqr, p^4. – Math. Ann., 1893, Bd. 43, S.301–412.

Таким образом, все группы порядка p^3 и экспоненты p, изоморфны между собой.

С другой стороны, если в G есть элемент x порядка p^2, то порожденная им подгруппа $H = \langle x\rangle$ имеет индекс p в G, так что элемент x не может быть центральным. Возьмем произвольный элемент $y \notin H$, он не может коммутировать с x. Тем самым, $y^p \in H$, $yxy^{-1} = y^r$, $1 < r < p$. Как обычно, итерируя последнее соотношение, получаем $y^m x y^{-m} = x^{r^m}$ и, значит $y = y^p x y^{-p} = x^{r^p}$. Тем самым, $r^p \equiv 1 \pmod p)^2$. Так как, по теореме Ферма $r^p \equiv r \pmod p$, то $r \equiv 1 \pmod p$. Представим r в виде $r = 1 + sp$, и пусть $st \equiv 1 \pmod p$. Тогда $y^t x y^{-t} = x^{(1+sp)^t} = x^{1+stp} = x^{1+p}$. С другой стороны, $y^p \in H$ и, значит, $y^p = x^{pq}$ для некоторого q. Непосредственное вычисление (проведите его!) показывает, что $(yu^{-q})^p = 1$. Это значит, что заменяя, если нужно, y на $y^t x^{-q}$, мы можем с самого начала считать, что $y^p = 1$ и $yxy^{-1} = x^{1+p}$. Таким образом, в этом случае группа G задается образующими и соотношениями

$$G = \langle x, y \mid x^{p^2} = 1, y^p = 1, [x,y]^p = 1, [x,y]x = x[x,y], [x,y]y = y[x,y]\rangle.$$

Таким образом, с точностью до изоморфизма существует единственная группа порядка p^3, в которой есть элемент порядка p^2.

Построить неабелеву группу, все элементы которой имеют порядок p, совсем просто. Это, например, группа $U(3,p)$ верхних унитреугольных матриц над полем $K = \mathbb{F}_p$ из p элементов. В самом деле, это неабелева группа порядка p^3, а то, что при $p \geq 3$ все ее элементы имеют порядок p, проверяется непосредственным вычислением (в слегка замаскированном виде это вычисление проводится в Главе 3 – делимость биномиальных коэффициентов).

Построить модель группы с элементом порядка p^2 чуть сложнее. Пусть теперь K – поле характеристики 0 и ζ – первообразный корень степени p из 1. Рассмотрим следующие матрицы:

$$x = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ & & \ddots & & \\ 0 & 0 & \dots & 0 & 1 \\ \zeta & 0 & \dots & 0 & 0 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & \zeta & 0 & \dots & 0 \\ 0 & 0 & \zeta^2 & \dots & 0 \\ & & \ddots & & \\ 0 & 0 & 0 & \dots & \zeta^{p-1} \end{pmatrix}.$$

Непосредственное вычисление показывает, что $x^{p^2} = y^p = e$, а $x^p = [x,y] = \zeta e$ – скалярная матрица.

Группы порядка p^3 с элементом порядка p^2 допускают следующее обобщение.

Задача. Докажите, что при нечетном p для любого $n \geq 3$ существует *единственная* с точностью до изоморфизма неабелева группа G порядка p^n с циклической максимальной подгруппой, а именно, группа,

$$\langle x, y \mid x^{p^{n-1}} = y^p = 1, [x,y] = x^{p^{n-2}}\rangle.$$

Решение. Ничем, кроме арифметики, не отличается от случая $n = 3$, см., например, Холл, Теорема 12.5.1. на страницах 209–211. Заметим, что случай $p = 2$ *значительно* сложнее: для любого $n \geq 4$ кроме диэдральной

$$\langle x, y \mid x^2 = y^2 = 1, (xy)^{2^{n-1}} = 1\rangle$$

и **обобщенной кватернионной группы**

$$\langle x, y \mid x^{2^{n-1}} = 1, y^2 = x^{2^{n-2}}, yx = x^{-1}y\rangle$$

появляются еще две новых неабелевых группы порядка 2^n с элементом порядка 2^{n-1}.

Число неизоморфных групп порядка p^n довольно быстро растет.

порядок:	$2^4 = 16$	$2^5 = 32$	$2^6 = 64$	$2^7 = 128$	$2^8 = 256$
количество групп:	14	51	267	2328	56092

Результат для 2^7 получили в 1990 году R.James, M.F.Newman и E.A.O'Brien, а результат для 2^8 – в 1991 E.A.O'Brien, он же показал, что уже среди групп класса 2 имеется по крайней мере 8.000.000 неизоморфных групп порядка $2^9 = 512$. Тем самым, классификация всех групп порядка 512 представляется довольно сомнительным занятием. Для сравнения, как вычислили при помощи GAP Hans-Ulrich Beschke и Bettina Eick, имеется всего 199 неизоморфных групп порядка 1000. Грехем Хигмен (1960) и Чарльз Симс (1965) показали, что асимптотически число групп порядка p^n близко к $p^{2n^3/27}$.

§ 11. Теорема Диксона

В § 6 мы показали, что любая группа порядка pq, где $p < q$ два простых числа таких, что $p \not| (q-1)$, циклическая. Естественно возникает вопрос, для каких $n \in \mathbb{N}$ существует единственная группа порядка n?

1. Теорема Диксона. Ответ на этот вопрос дается следующей замечательной, но незаслуженно малоизвестной теоремой Диксона (в действительности Диксон в 1905 году описал те порядки n, для которых все группы порядка n абелевы). Следующее замечательно простое доказательство теоремы Диксона принадлежит Дитеру Юнгникелю[280].

Теорема Диксона. *Циклическая группа в том и только том случае является единственной группой порядка n, когда n взаимно просто с $\varphi(n)$.*

Доказательство. Необходимость почти очевидна. Ясно, что n должно быть свободно от квадратов, так как если n делится на p^2, то группа $\mathrm{C}_p \oplus C_{n/p}$ не является циклической. Пусть поэтому $n = p_1 \dots p_s$, где $p_1 < \dots < p_s$ различные простые. Если $n = pqm$, где $p < q$ – два простых таких, что $p|(q-1)$, то существует нетривиальное полупрямое произведение $C_p \leftthreetimes C_q$ и, таким образом, C_n снова не единственна. Это значит, что $\gcd(n, \varphi(n)) = 1$.

Обратно, пусть $\gcd(n, \varphi(n)) = 1$. В силу классификации конечных абелевых групп все абелевы группы порядка n циклические. Одним из основных методов используемых в доказательствах теорем про конечные группы является анализ **минимального контр-примера**. Итак, рассмотрим группу G *наименьшего порядка* n, являющуюся контр-примером к теореме Диксона. Так как $\gcd(m, \varphi(m)) = 1$ для любого делителя $m|n$ и так как по предположению все они удовлетворяют теореме Диксона, **все** подгруппы и фактор-группы G циклические. Ясно, что $C(G) = 1$. В самом деле, если $C(G) \neq 1$, то $G/C(G)$ циклическая и, следовательно, G абелева по упражнению ?.

Покажем прежде всего, что любая максимальная подгруппа является централизатором любого своего нетривиального элемента. В самом деле, пусть $H \leq G$ максимальная подгруппа и пусть $x \in H$, $x \neq 1$. Тогда так как H циклическая, то $C_G(x)$ содержит H, и, значит, в силу максимальности H он совпадает либо с H либо с G. Так как элемент x нецентральный, $C_G(x) = H$. В частности, это означает, что пересечение двух любых различных максимальных подгрупп в G тривиально. Действительно, если $H, F \leq G$ две *максимальные* подгруппы и $x \in H \cap F$, $x \neq 1$, то $H = C_G(x) = F$.

Покажем теперь, что максимальная подгруппа $H \leq G$ не может быть нормальной в G, иными словами, $N_G(H) = H$. В самом деле, пусть $|H| = m|n$ и $x \in G \setminus H$ нормализует H, по определению порядок x делит n. С другой стороны, порядок автоморфизма $\rho : h \mapsto xhx^{-1}$, который сопряжение при помощи x реализует на *циклической* группе $H \cong C_m$ порядка m, делит $|\operatorname{Aut}(H)| = \varphi(m)$. Так как по условию $\gcd(n, \varphi(m)) = 1$ (n бесквадратное!), то $\rho = \mathrm{id}_H$. Тем самым, x централизует H, а так как $G = \langle H, x\rangle$ элемент x лежит в центре G, что невозможно.

Рассмотрим наконец **все** n/m подгрупп, сопряженных к H (количество сопряженных равно индексу нормализатора). Так как любые две из них пересекаются по 1, то порядок их объединения X равен $(m-1)\frac{n}{m} + 1 = n - n/m + 1$. Так как $m < n$, то найдется элемент x не лежащий ни в одной подгруппе, сопряженной с H. Этот элемент, в свою очередь, лежит в какой-то максимальной подгруппе F, скажем, порядка, $l < n$, не сопряженной с H. По той же причине, что и для H, объединение Y всех сопряженных с F имеет порядок $n - n/l + 1$, причем $X \cap Y = 1$. Это значит, что $(n - n/m) + (n - n/l) = (|X| - 1) + (|Y| - 1) < |G| = n$ или, иными словами, $1/m + 1/l > 1$. Однако такое неравенство абсурдно, ибо из него вытекало бы, что $m = 1$ или $l = 1$, что противоречит определению m и l (порядки максимальных подгрупп в *неабелевой* группе G).

2. Первая тысяча непростых чисел таких, что $\gcd(n, \varphi(n)) = 1$**.** Представляется, что порядков n, в которых существует единственная группа, немного. В действительности дело обстоит иначе. Конечно, это так для всех простых $n = p$. Ниже мы приводим первую тысячу непростых порядков:

15, 33, 35, 51, 65, 69, 77, 85, 87, 91, 95, 115, 119, 123, 133, 141, 143, 145, 159, 161, 177, 185, 187, 209, 213, 215, 217, 221, 235, 247, 249, 255, 259, 265, 267, 287, 295, 299, 303, 319, 321, 323, 329,

[280] Dieter Jungnickel, On the uniqueness of the cyclic group of order n. – Amer. Math. Monthly, 1992, June–July, p.545–547.

335, 339, 341, 345, 365, 371, 377, 391, 393, 395, 403, 407, 411, 413, 415, 427, 435, 437, 445, 447, 451, 455, 469, 473, 481, 485, 493, 501, 511, 515, 517, 519, 527, 533, 535, 537, 545, 551, 553, 559, 561, 565, 573, 581, 583, 589, 591, 595, 611, 623, 629, 635, 649, 665, 667, 671, 679, 681, 685, 695, 697, 699, 703, 705, 707, 713, 717, 721, 731, 745, 749, 753, 763, 767, 771, 779, 781, 785, 789, 793, 795, 799, 803, 805, 807, 815, 817, 835, 843, 851, 865, 869, 871, 879, 885, 893, 895, 899, 901, 913, 917, 923, 933, 943, 949, 951, 957, 959, 965, 973, 985, 989, 995, 1001, 1003, 1007, 1037, 1041, 1043, 1057, 1059, 1067, 1073, 1077, 1079, 1099, 1105, 1111, 1115, 1121, 1133, 1135, 1139, 1141, 1145, 1147, 1149, 1157, 1159, 1165, 1167, 1169, 1173, 1177, 1189, 1195, 1199, 1203, 1207, 1211, 1219, 1235, 1241, 1243, 1245, 1247, 1253, 1257, 1261, 1267, 1271, 1273, 1285, 1293, 1295, 1309, 1313, 1315, 1329, 1333, 1335, 1337, 1339, 1343, 1345, 1347, 1349, 1351, 1353, 1357, 1363, 1383, 1385, 1387, 1391, 1393, 1397, 1401, 1403, 1411, 1415, 1417, 1437, 1441, 1457, 1463, 1465, 1469, 1473, 1479, 1495, 1501, 1507, 1509, 1513, 1517, 1527, 1529, 1535, 1537, 1541, 1547, 1551, 1561, 1563, 1565, 1577, 1585, 1589, 1591, 1603, 1605, 1615, 1631, 1633, 1639, 1643, 1645, 1649, 1651, 1661, 1671, 1679, 1685, 1687, 1689, 1691, 1695, 1707, 1717, 1727, 1729, 1735, 1739, 1745, 1749, 1757, 1761, 1763, 1765, 1769, 1779, 1781, 1793, 1795, 1797, 1799, 1807, 1817, 1819, 1829, 1835, 1837, 1841, 1843, 1851, 1853, 1855, 1865, 1883, 1885, 1891, 1895, 1897, 1903, 1909, 1915, 1919, 1921, 1923, 1927, 1937, 1939, 1941, 1943, 1945, 1947, 1955, 1957, 1959, 1961, 1963, 1969, 1977, 1981, 1985, 1991, 2001, 2021, 2031, 2033, 2045, 2047, 2049, 2051, 2055, 2059, 2065, 2071, 2077, 2091, 2093, 2095, 2101, 2103, 2117, 2119, 2123, 2147, 2149, 2157, 2159, 2165, 2167, 2171, 2173, 2177, 2183, 2185, 2191, 2195, 2201, 2215, 2219, 2227, 2229, 2231, 2235, 2245, 2249, 2257, 2261, 2263, 2279, 2283, 2285, 2291, 2315, 2317, 2319, 2321, 2323, 2327, 2335, 2343, 2345, 2353, 2363, 2369, 2387, 2391, 2395, 2397, 2405, 2407, 2413, 2419, 2427, 2429, 2431, 2435, 2443, 2449, 2453, 2461, 2463, 2465, 2471, 2479, 2481, 2483, 2489, 2491, 2495, 2497, 2501, 2505, 2507, 2509, 2513, 2515, 2517, 2519, 2533, 2537, 2545, 2555, 2561, 2563, 2567, 2569, 2571, 2573, 2581, 2587, 2589, 2595, 2599, 2603, 2611, 2615, 2623, 2627, 2629, 2641, 2643, 2651, 2661, 2669, 2681, 2685, 2701, 2703, 2717, 2723, 2733, 2735, 2737, 2739, 2743, 2747, 2755, 2759, 2761, 2765, 2771, 2773, 2779, 2785, 2787, 2795, 2807, 2813, 2815, 2821, 2823, 2827, 2829, 2831, 2839, 2841, 2845, 2849, 2859, 2863, 2867, 2869, 2881, 2885, 2893, 2899, 2905, 2911, 2913, 2921, 2923, 2929, 2931, 2933, 2935, 2941, 2949, 2951, 2955, 2959, 2965, 2977, 2981, 2983, 2987, 2993, 2995, 3007, 3009, 3013, 3017, 3029, 3031, 3035, 3039, 3043, 3047, 3053, 3055, 3057, 3059, 3065, 3071, 3073, 3077, 3085, 3091, 3093, 3095, 3097, 3101, 3103, 3107, 3113, 3115, 3127, 3131, 3133, 3139, 3145, 3147, 3149, 3151, 3157, 3161, 3173, 3183, 3193, 3199, 3215, 3223, 3227, 3233, 3235, 3239, 3247, 3263, 3265, 3269, 3273, 3277, 3281, 3287, 3291, 3293, 3295, 3309, 3317, 3327, 3333, 3335, 3337, 3341, 3349, 3353, 3365, 3367, 3377, 3379, 3383, 3385, 3395, 3397, 3401, 3405, 3409, 3415, 3419, 3421, 3427, 3431, 3439, 3443, 3453, 3473, 3487, 3489, 3493, 3495, 3497, 3503, 3515, 3521, 3523, 3531, 3543, 3545, 3551, 3553, 3561, 3563, 3567, 3569, 3579, 3585, 3587, 3589, 3595, 3599, 3601, 3605, 3611, 3619, 3621, 3635, 3647, 3649, 3651, 3653, 3655, 3657, 3661, 3665, 3667, 3669, 3679, 3683, 3687, 3689, 3695, 3707, 3713, 3715, 3729, 3731, 3737, 3743, 3745, 3749, 3763, 3777, 3781, 3785, 3787, 3791, 3799, 3809, 3811, 3815, 3817, 3827, 3831, 3835, 3839, 3841, 3845, 3849, 3855, 3859, 3865, 3867, 3869, 3893, 3899, 3901, 3903, 3921, 3935, 3937, 3941, 3945, 3949, 3953, 3957, 3959, 3961, 3973, 3977, 3979, 3983, 3985, 3991, 3995, 3997, 4009, 4031, 4033, 4035, 4037, 4039, 4043, 4045, 4061, 4071, 4081, 4083, 4085, 4087, 4089, 4097, 4101, 4103, 4109, 4115, 4117, 4119, 4121, 4123, 4135, 4141, 4145, 4147, 4151, 4163, 4169, 4171, 4181, 4183, 4187, 4189, 4193, 4195, 4199, 4207, 4213, 4223, 4227, 4233, 4237, 4247, 4249, 4255, 4265, 4267, 4277, 4279, 4281, 4285, 4291, 4295, 4299, 4303, 4307, 4309, 4313, 4315, 4317, 4321, 4323, 4331, 4333, 4343, 4353, 4355, 4369, 4379, 4381, 4385, 4387, 4393, 4395, 4399, 4403, 4411, 4415, 4427, 4429, 4433, 4435, 4439, 4443, 4453, 4461, 4465, 4469, 4471, 4479, 4487, 4497, 4499, 4501, 4505, 4511, 4521, 4529, 4531, 4533, 4535, 4537, 4539, 4541, 4543, 4553, 4559, 4569, 4571, 4573, 4577, 4579, 4589, 4595, 4601, 4607, 4611, 4619, 4627, 4631, 4633, 4645, 4659, 4661, 4667, 4677, 4681, 4685, 4687, 4697, 4699, 4709, 4713, 4717, 4727, 4735, 4739, 4741, 4745, 4747, 4749, 4755, 4757, 4763, 4765, 4769, 4771, 4777, 4781, 4795, 4803, 4811, 4819, 4821, 4829, 4835, 4837, 4839, 4841, 4843, 4847, 4849, 4853, 4857, 4859, 4865, 4867, 4873, 4879, 4883, 4885, 4891, 4897, 4899, 4911, 4915, 4917, 4921, 4927, 4939, 4945, 4963, 4979, 4981, 4985, 4991, 4997, 5001, 5015, 5017, 5027, 5029, 5033, 5035, 5045, 5053, 5057, 5063, 5065, 5069, 5071, 5083, 5089, 5091, 5095, 5111, 5123, 5127, 5129, 5131, 5137, 5141, 5143, 5149, 5151, 5161, 5163, 5165, 5173, 5177, 5183, 5191, 5195, 5199, 5205, 5207, 5213, 5215, 5221, 5245, 5249, 5251, 5257, 5263, 5267, 5269, 5287, 5291, 5293, 5295, 5311, 5315, 5317, 5321, 5327, 5339, 5345, 5353, 5357, 5359, 5361, 5363, 5365, 5369, 5371, 5377, 5383, 5385, 5389, 5395, 5401, 5411, 5423, 5429, 5433, 5435, 5447, 5453, 5457, 5459, 5461, 5465, 5469, 5473, 5485, 5489, 5495, 5497, 5509,

5511, 5515, 5533, 5539, 5541, 5543.

Таким образом, почти треть всех порядков меньших 5000 удовлетворяет условию теоремы Диксона.

§ 12. Холловские подгруппы

Для $\pi = \{2, 3\}$ в A_5 есть порожденная $(123)(45)$ подгруппа порядка 6, не содержащаяся ни в какой большей π-подгруппе. Кроме того, в A_5 есть холловская π-подгруппа A_4 порядка 12.

INDEX RERUM

Ein Buch ohne Index ist kein Buch.

Mommsen

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

Браун, К.
Брауэр (Brouwer), Люйтцен Эгбертус Ян
Брауэр (Brauer), Рихард
Бредон, Г.
Бурбаки (Bourbaki), Никола
Бургер (Burger), М.
Бусаркин, В.М.
Бьянки (Bianchi), Л.
Букур, И.
Бэр (Baer), Р.
Бюкенхаут (Buekenhout), Ф.
Бялыницки-Бируля (Białynicki-Birula), Анджей
Вавжинчик, А.
Вагнер (Wagner), Ашер (Отто)
ван дер Варден (van der Waerden), Бартельс
Веддербарн
Вейль (Weil), Андре
Вейль (Weyl), Герман
Венкатарамана
Венков, Борис Борисович
Верле, Ю.
Верфритц (Wehrfritz), Б.А.Ф.
Вессио (Vessiot), Э.
Вигнер (Wigner), Юджин
Виландт (Wilandt), Х.
Виленкин, Наум Яковлевич
Винберг Эрнест Борисович
да Винчи, Леонардо
Витт (Witt), Эрнст
Вольф (Wolf), Дж.
Вон-Ли (Vaughan-Lee), М.Р.
Воробьев, Е.М.
Воскресенский, Валентин Евгеньевич
Вульф
Вуссинг (Wussing), Х.
Вустер, У.А.
Гадолин, Аксель Вильгельмович
Галуа (Galois), Эварист
Гамильтон (Hamilton),
Гаусс (Gauss)
Гашюц (Gaschütz), В.
Гейзенберг (Heisenberg),
Гекке (Hecke),
Гельдер, Людвиг Отто
Гельдер Эрнст Отто
Гельфанд, Израиль Моисеевич
Гессель, Иоганн
Гильберт (Hilbert), Давид
Гирш ???
Гишарде, А.
Голд, А.
Головин, Олег Николаевич
Головина, Л.И.
Голод, Евгений Соломонович
Голубовский (Hołubowski), Вальдемар
Голубчик, Игорь Захарович
Гордеев, Николай Леонидович
Гордон, Г.
Горенстейн, Дэниел
Горчаков, Ю.М.
Граве, Дмитрий Алексеевич
Граев, М.И.
Грайс, Р.Л.
Гретцер, Джордж
Грехем (Graham), Р.Л.
Григорчук, Ростислав
Грин, Л.
Гриндлингер, Мартин Давидович
Гринлиф, Ф.
Громов, Михаил
Гроссман, И.
Гротендик (Grothendieck), Александр
Гроув (Grove),
Груневальд (Grunewald), Фритц
Грушко
Грюнберг (Gruenberg), Карл
Гуральник (Guralnick),
Гурвиц (Hurwitz), Адольф
Гуревич (Hurewicz), Уолтер
Гусман, Г.
Дали, Сальвадор
Дедекинд (Dedekind), Рихард
Де Кончини (De Concini), Коррадо
Делоне, Борис Николаевич
Деляну, А.
Джеймс (James), Гордон
Джеймс (James), Дональд
Дзакер (Zacher), Джованни
Диаконис, Перси
том Дик, Таммо
фон Дик (von Dyck), Вальтер
Диксон (Dixon), Джон
Диксон (Dickson), Леонард Эугениуш
Ди Мартино (Di Martino), Лино
Дицман, А.П.
Добер, П.
Дубровин, Борис
Дьедонне (Dieudonnè), Жан
Дынкин, Евгений Борисович
Дэн (Dehn), Макс
Жаке, Э.
Желобенко Дмитрий Павлович
Жордан (Jordan), Камилл
Залесский Александр Ефимович
Зейтц (Seitz), Вильгельм
Зейтц (Seitz), Гари
Зельманов, Ефим Исаакович
Зигель (Siegel), Карл Людвиг
Золотарев
Зонке, Леонард
Ито (Ito), Нобору
Ишханов, Владимир Ваганович
Калужнин, Лев Аркадьевич
Камерон (Cameron), Питер
ван Кампен (van Kampen), Э.Р.
Кантор (Kantor), Уиллиам

Фет, А.И.
Фиттинг
Фишер (Fischer), Бернд
Фларри, Р.
Фогт, Э.
Фокс (Fox), Р.
Фоменко, А.Т.
Фомин, А.Н.
Форд, Л.Р.
делла Франческо, Пьеро
Фраттини (Frattini)
Фрейденталь (Freudenthal), Ганс
Френкель, Игорь Борисович
Фрид (Fried), Эрвин
Фрикке
Фробениус, Фердинанд Георг
Фукс
Фукс (Fuchs László) , Ласло
Фултон (Fulton)
Фюрстенберг (Furstenberg), Хиллел
Хамермеш (Hamermesh), М.
Хамфри (Humphreys), Джеймс
Хан (Hahn), Алекс
Хан, Ф.
Харада (Harada)
Харари, Ф.
Харди, Гаральд Годфри
Хариш-Чандра (Harish-Chandra)
Хармс, Даниил
Харрис
Харрисон, М.
Хаусон
Хассе (Hasse), Хельмут
Хейне ,
Хелгасон, Сигурдур
Хельд (Held), Дитер
Хеннан, Э.
Хигмен (Higman), Грехем
Хигмен (Higman), Д.
Хилтон (Hilton), Питер
Хирш (Hirsch)
Хлебников, Велемир
Холдевай, Ч.-Д.
Холл (Hall), Джонатан
Холл (Hall), Маршалл
Холл (Hall), Филипп
Хопф (Hopf), Хайнц
Хохшильд (Hochschi?ld), Дж.
Хохштрассер (Hochstrasser), Р.
Хупперт (Huppert), Бертрам
Хьюзмоллер (Husemoller), Э.
Хьюитт (Hewitt), Э.
Цагир (Zagier), Дон??
Цассенхауз (Zassenhaus), Ханс
Цишанг (Zieschang), Х.
Цюлике, Л.
Чандлер (Chandler), Б.
Чеботарев, Николай Григорьевич
Чебышев, Пафнутий Львович
Черников, Сергей Николаевич
Чунихин
Шалев (Shalev), Анер
Шапиро, З.Я.
Шаталов, В.Е.
Шаттшнейдер (Schattschneider), Дорис
Шафаревич, Игорь Ростиславович
Шафрановский, Иларион И.
Шевалле (Chevalley), Клод
Шеметков, Леонид Аркадьевич
Шеринг
Шимура (Shimura), Горо
Ширвани (Shirvani), М.
Шлефли (Schläfli)
Шмелькин, Альфред Львович
Шмидт, Отто Юльевич
Шмидт, Роберт Анатолиевич
Шмидт (Schmidt), Роланд
Шпайзер (Speiser) , Андреас
Шрайер (Schreier), Отто
Штейнер (Steiner)
Штейниц (Steinitz)
Штерн, А.И.
Штикельбергер
Штрайтвольф (Streitwolf?), Г.
Шубников, А.В.
Шупп (Schupp),
Шур (Schur), Исайа
Эвклид
Эйзенхарт , Л.П.
Эйленберг (Eilenberg), Самуэль
Эйлер (Euler), Леонард
Эллиот, Дж.
Эльстродт, Ю.
Энгель (Engel)
Эшер (Escher), Морис
Юнг (Young)
Яковлев Анатолий Владимирович
Янко (Janko)