М. И. КАРГАПОЛОВ, Ю. И. МЕРЗЛЯКОВ

ОСНОВЫ ТЕОРИИ ГРУПП

ИЗДАНИЕ ТРЕТЬЕ,
ПЕРЕРАБОТАННОЕ И ДОПОЛНЕННОЕ

МОСКВА «НАУКА»
ГЛАВНАЯ РЕДАКЦИЯ
ФИЗИКО-МАТЕМАТИЧЕСКОЙ ЛИТЕРАТУРЫ
1982

22.144
К 22
УДК 512.8

Каргаполов М. И., Мерзляков Ю. И. **Основы теории групп.**— 3-е изд., перераб. и доп.— М.: Наука, 1982.— 288 с.

Книга посвящена изложению основ теории групп — одного из важнейших разделов современной алгебры. Помимо традиционного материала, относящегося к собственно основам теории групп, излагаются некоторые последние достижения в этой области, еще не получившие отражения в монографической литературе. Большое внимание уделяется примерам и упражнениям, разъясняющим основные понятия и результаты.

Для научных работников, аспирантов и студентов старших курсов университетов и пединститутов.

Михаил Иванович Каргаполов
Юрий Иванович Мерзляков

ОСНОВЫ ТЕОРИИ ГРУПП

Редактор Ф. И. Кизнер
Техн. редактор Е. В. Морозова
Корректор Н. Б. Румянцева

И. Б. № 12126

Сдано в набор 06.02.82. Подписано к печати 09.06.82. Т-06791.
Формат 84×108¹/₃₂. Бумага тип. № 1. Обыкновенная гарнитура.
Высокая печать. Условн. печ. л. 15,12. Уч.-изд. л. 15,24.
Тираж 11 800 экз. Заказ № 1420. Цена 1 р. 20 к.

Издательство «Наука»
Главная редакция физико-математической литературы
117071, Москва, В-71, Ленинский проспект, 15

2-я типография издательства «Наука»
121099, Москва, Шубинский пер., 10

К $\frac{1702030000-094}{053(02)-82}$ 29-82.

ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

В третьем издании добавлена глава 8, в которой обсуждаются важнейшие условия конечности — периодичность и локальная конечность, условия минимальности и максимальности, условие конечности ранга. Есть изменения и в других частях книги, иногда довольно значительные. Во избежание путаницы проводится четкое различие между степенью (группы, свободной в многообразии), размерностью (абелевой группы) и рангом группы.

Сегодня, когда я пишу это предисловие, исполняется пять лет со дня кончины Михаила Ивановича Каргаполова. Включение в книгу теоремы 25.2.1, «наиболее глубокой из теорем о разрешимых группах» [43],— дань его светлой памяти.

Я благодарен В. Я. Блощицыну, Ю. М. Горчакову, В. Д. Мазурову, Ю. В. Сосновскому, В. А. Чуркину и В. П. Шункову, беседы с которыми помогли мне в работе.

Новосибирск, Академгородок,
20 февраля 1981 г. *Ю. И. Мерзляков*

ИЗ ПРЕДИСЛОВИЯ КО ВТОРОМУ ИЗДАНИЮ

Настоящее издание отличается от предыдущего отдельными изменениями в разных местах книги. Больше внимания уделено, в частности, полициклическим и локально полициклическим группам — самым естественным обобщениям классического понятия конечной разрешимой группы.

Авторы

Новосибирск, Академгородок,
14 января 1976 г.

ИЗ ПРЕДИСЛОВИЯ К ПЕРВОМУ ИЗДАНИЮ

Эта книга — записки лекций по теории групп, читанных авторами в Новосибирском университете в 1968—1970 гг. Мы хотели изложить именно основы, не вдаваясь в детали и обходя трясину обобщений. Надеемся, что студент, желающий заниматься теорией групп и познакомившийся по этим запискам с ее основами, сможет быстро перейти к чтению специальной литературы по избранному вопросу.

Мы старались не переступать границу между абстрактной и схоластической теорией групп, по возможности поясняя высокие понятия простыми примерами. Четыре типа примеров сопровождают изложение: числа по сложению, числа по умножению, подстановки и матрицы. Для понимания основного текста достаточно знания общего курса алгебры, в примерах иногда используются более специальные сведения. Примеры и упражнения частично используются в основном тексте, поэтому их формулировки не следует пропускать при чтении, а решение откладывать слишком надолго.

В нескольких местах отмечены нерешенные вопросы. Достаточно полное собрание таких вопросов, отражающее интересы широкого круга специалистов по теории групп, можно найти в последнем издании «Коуровской тетради».

Авторы

Новосибирск, Академгородок,
3 февраля 1971 г.

ОБОЗНАЧЕНИЯ КЛАССИЧЕСКИХ ОБЪЕКТОВ

Для удобства читателя перечислим «персональные» обозначения классических объектов, закрепленные за ними на протяжении всей книги (рядом указаны номера страниц, где эти обозначения впервые вводятся и объясняются):

$\boldsymbol{A}_n$ 24
$\boldsymbol{A}_\pi$ 117
$\boldsymbol{B}_r(m)$ 214
$\mathbb{C}$ 19
$\mathbb{C}^*$ 20
$\mathbb{C}_n$ 20
$\mathbb{C}_{p^\infty}$ 20
$\boldsymbol{D}_n(K)$, $\boldsymbol{D}_n(K, \mathfrak{a})$ 20, 50
$\boldsymbol{F}(X)$ 123
$\boldsymbol{F}_n(X)$, $\boldsymbol{F}_n$ 124
$\boldsymbol{F}_\infty(X)$, $\boldsymbol{F}_\infty$ 124
$\boldsymbol{F}_V(X)$, $\boldsymbol{F}_\pi(\mathfrak{L})$ 138, 139
$\boldsymbol{GF}(q)$ 19
$\boldsymbol{GF}(q)^*$ 20
$\boldsymbol{GL}_n(K)$, $\boldsymbol{GL}_n(K, \mathfrak{a})$ 20, 50
$\boldsymbol{M}_n(K)$ 20
$\boldsymbol{O}_n(K)$, $\boldsymbol{O}_n(K, \mathfrak{a})$ 24, 50
$\boldsymbol{PSL}_n(K)$ 118
$\mathbb{Q}$ 19
$\mathbb{Q}^*$ 20
$\mathbb{Q}_p$ 19
$\mathbb{Q}_{p^\infty}$ 62
$\mathbb{R}$ 19
$\mathbb{R}^*$ 20
$\boldsymbol{S}(M)$ 20
$\boldsymbol{S}_n$ 20
$\boldsymbol{S}_\mu(M)$ 117
$\boldsymbol{SL}_n(K)$, $\boldsymbol{SL}_n(K, \mathfrak{a})$ 20, 50
$\boldsymbol{T}_n(K)$, $\boldsymbol{T}_n(K, \mathfrak{a})$ 20, 50
$\boldsymbol{U}_n$ 24
$\boldsymbol{UT}_n(K)$, $\boldsymbol{UT}_n(K, \mathfrak{a})$ 20, 50
$\boldsymbol{UT}_n^m(K)$, $\boldsymbol{UT}_n^m(K, \mathfrak{a})$ 24, 50
$\mathbb{Z}$ 19
$\mathbb{Z}^*$ 20
$\mathbb{Z}_n$ 19
$\mathbb{Z}_n^*$ 20
$\mathbb{Z}_{p^\infty}$ 62
$\boldsymbol{\Gamma}_n(m)$, $\boldsymbol{\Gamma}_n(\mathfrak{a})$ 50, 146

ВВЕДЕНИЕ

Почему квадрат кажется нам симметричной фигурой, круг — еще более симметричной, а цифра 4 совсем несимметричной? Чтобы ответить на этот вопрос, рассмотрим движения, совмещающие фигуру с нею самой. Легко понять, что таких движений для квадрата существует восемь, для круга — бесконечно много, а для цифры 4 лишь одно — тождественное, которое оставляет каждую точку фигуры на месте. Множество G различных движений, самосовмещающих данную фигуру, и служит характеристикой большей или меньшей ее симметричности: чем больше G, тем симметричнее фигура. Определим на множестве G композицию, т. е. действие над его элементами, по следующему правилу: если x, y — два движения из G, то результатом их композиции (иногда говорят «произведением») называется движение xy, равносильное последовательному выполнению сначала движения x, а затем движения y. Например, если x, y — отражения квадрата относительно диагоналей, то $x \cdot y$ — его поворот около центра на 180°. Очевидно, композиция на G обладает следующими свойствами: 1) $(xy)\,z = x\,(yz)$ для любых элементов x, y, z из G, 2) в G существует такой элемент e, что $xe = ex = x$ для любого x из G, 3) для любого x из G существует в G такой элемент x^{-1}, что $xx^{-1} = x^{-1}x = e$. Действительно, в качестве e можно взять тождественное движение, а в качестве x^{-1} — движение, обратное к x, т. е. возвращающее каждую точку фигуры из нового положения в старое.

Отвлечемся теперь от нашего примера и рассмотрим произвольное множество G, на котором задана композиция, т. е. для любых двух элементов x, y из G определен элемент xy снова из G. Если при этом выполняются условия 1), 2), 3), то множество G с заданной на нем композицией называется *группой*. Группы — один из основных типов

алгебраических систем, а теория групп — один из основных разделов современной алгебры.

Понадобилась работа нескольких поколений математиков, занявшая в общей сложности около ста лет, прежде чем идея группы выкристаллизовалась с ее сегодняшней ясностью. От Лагранжа, стихийно применявшего группы подстановок для решения алгебраических уравнений в радикалах (1771), через работы Руффини (1799) и Абеля (1824) к Эвариcту Галуа, в работах которого (1830) уже достаточно сознательно используется идея группы (им же впервые введен и сам термин),— вот путь, по которому развивалась эта идея в рамках теории алгебраических уравнений. Независимо и по другим причинам она возникла в геометрии, когда в середине XIX в. на смену единой античной геометрии пришли многочисленные «геометрии» и остро встал вопрос об установлении связей и родства между ними. Выход был указан «Эрлангенской программой» Клейна (1872), положившей в основу классификации геометрий понятие группы преобразований. Третий источник понятия группы — теория чисел. Отметим здесь работу Эйлера о вычетах, остающихся при делении степеней (1761), и работу Гаусса о композиции двоичных квадратичных форм (1801).

Осознание в конце XIX в. принципиального единства теоретико-групповых идей, существовавших к тому времени независимо в разных областях математики, привело к выработке современного абстрактного понятия группы (Кэли, Фробениус, ван Дик и др.). Это был один из самых ранних примеров абстрактной алгебраической системы. Он послужил во многих отношениях образцом при перестройке других областей алгебры и всей математики на рубеже XX в.— их путь уже не был столь извилистым и трудным. Изучение групп без предположения конечности и без каких бы то ни было предположений о природе элементов впервые оформилось в самостоятельную область математики с выходом книги О. Ю. Шмидта «Абстрактная теория групп» (1916).

В настоящее время теория групп является одной из самых развитых областей алгебры, имеющей многочисленные применения как в самой математике, так и за ее пределами — в топологии, теории функций, кристаллографии, квантовой механике и других областях матема-

тики и естествознания. Конечной целью собственно теории групп является описание всех групповых композиций.

Приведем несколько примеров применения групп в алгебре, в математике вообще и в естествознании.

1. Группы Галуа. Содержанием классической теории Галуа является применение теории групп к изучению полей в следующем духе. Пусть K — конечное, сепарабельное и нормальное расширение поля k. Автоморфизмы поля K, оставляющие элементы подполя k неподвижными, образуют группу G относительно их последовательного выполнения. Она называется *группой Галуа* расширения K/k. Основная теорема теории Галуа утверждает, что, сопоставляя каждой подгруппе $H \leqslant G$ ее неподвижное подполе $K^H = \{x \mid x \in K,\ x^h = x \text{ для всех } h \in H\}$, мы получим антиизоморфное отображение решетки подгрупп группы G на решетку промежуточных подполей, заключенных между k и K. Расширение K^H/k тогда и только тогда будет снова конечным, сепарабельным и нормальным, когда подгруппа H нормальна в G, причем в этом случае сужение автоморфизмов из G на K^H будет гомоморфизмом группы G на группу Галуа расширения K^H/k с ядром H.

Приложение к вопросу о разрешимости уравнений в радикалах осуществляется следующим образом. Пусть f — многочлен от X над полем k, K — поле разложения f. Пусть G — группа Галуа расширения K/k. Она называется группой Галуа многочлена f над полем k (ее элементы естественным образом изображаются подстановками корней уравнения $f(X) = 0$). Оказывается, уравнение $f(X) = 0$ тогда и только тогда решается в радикалах, когда группа Галуа многочлена f полициклическая.

Аналогом теории Галуа является теория Пикара — Вессио, изучающая средствами теории групп расширения дифференциальных колец и решающая, в частности, вопрос о разрешимости дифференциальных уравнений в квадратурах. Та роль, которую в теории Галуа играют группы подстановок, в теории Пикара—Вессио принадлежит алгебраическим группам матриц.

В указанных примерах группы возникают в форме групп автоморфизмов математических структур. Это не только одна из важнейших форм, но и вообще присущая только группам форма применения, обеспечивающая им особое положение в алгебре. Дело в том, что автоморфиз-

мы произвольных структур, говоря словами Галуа, всегда можно «группировать», тогда как определить на множестве автоморфизмов строение кольца или какой-нибудь другой полезной структуры удается лишь в специальных случаях.

2. Гомологические группы. Ведущей идеей теории гомологий является применение теории (абелевых) групп к изучению категории топологических пространств. Каждому пространству X сопоставляется семейство абелевых групп $H_0(X)$, $H_1(X)$, ... и каждому непрерывному отображению $f\colon X \to Y$ — семейство гомоморфизмов $f_n\colon H_n(X) \to H_n(Y)$, $n = 0, 1, 2, \ldots$ Изучение гомологических групп $H_n(X)$ и их гомоморфизмов средствами теории групп часто позволяет решить исходную топологическую задачу. Типичный пример — задача продолжения: можно ли отображение $g\colon A \to Y$, определенное на подпространстве A пространства X, продолжить на всё X, т. е. представить g как суперпозицию вложения $h\colon A \to X$ и некоторого непрерывного отображения $\bar{g}\colon X \to Y$? Если да, то в гомологиях должно быть $g_n = \bar{g}_n h_n$, т. е. каждый гомоморфизм $g_n\colon H_n(A) \to H_n(Y)$ можно пропустить через $H_n(X)$ с заданным множителем h_n. Если эта алгебраическая задача неразрешима, то, конечно, и исходная топологическая задача неразрешима.

Таким способом можно получать важные положительные результаты. В качестве иллюстрации наметим доказательство теоремы Брауэра о неподвижной точке: каждое непрерывное отображение f n-мерного шара E^n в себя обладает неподвижной точкой. Пусть, напротив, $f(x) \neq x$ для всех $x \in E^n$. Проведем луч с началом $f(x)$ через точку x. Пусть он протыкает сферу S^{n-1} в точке $\bar{g}(x)$. Очевидно, $\bar{g}$ непрерывно, так что задача продолжения тождественного отображения $g\colon S^{n-1} \to S^{n-1}$ до отображения $E^n \to S^{n-1}$ разрешима. При $n = 1$ это сразу дает противоречие. Пусть $n \geqslant 2$. Рассмотрим теорию гомологий с коэффициентами из группы $\mathbb{Z}$ целых чисел. Тогда $H_{n-1}(E^n) = 0$, $H_{n-1}(S^{n-1}) = \mathbb{Z}$, $h_{n-1} = 0$, $g_{n-1} = 1$. Ясно, что производная алгебраическая задача неразрешима. Это снова дает противоречие.

Гомологические группы иллюстрируют другой типичный путь применения групп — путь изучения неалгебраических объектов с помощью алгебраических систем, отражающих их поведение. Именно таков основной метод

алгебраической топологии. Впрочем, аналогичный метод и, в частности, гомологические группы успешно используются и для изучения самих алгебраических систем — например, в теории расширений групп.

3. Группы симметрий. Как было сказано выше, понятие группы позволяет в точных терминах охарактеризовать симметричность той или иной геометрической фигуры. Именно с таких позиций Е. С. Федоров (1890) решил задачу классификации правильных пространственных систем точек, являющуюся одной из основных задач кристаллографии. Плоских федоровских групп существует всего 17, они были найдены непосредственно. Пространственных же федоровских групп существует 230, и только теория групп позволила провести их исчерпывающую классификацию. Это был исторически первый случай применения теории групп непосредственно в естествознании.

Аналогичную роль играет теория групп в физике. Так, в квантовой механике состояние физической системы изображается точкой бесконечномерного векторного пространства. Если физическая система переходит из одного состояния в другое, то изображающая ее точка подвергается линейному преобразованию. Соображения симметрии и теория представлений групп линейными преобразованиями имеют здесь первостепенное значение.

Указанные примеры иллюстрируют классифицирующую роль теории групп всюду, где речь идет о симметрии. Изучая симметрию, по существу имеют дело с автоморфизмами систем (не обязательно математических), поэтому теория групп незаменима в этих вопросах. Ее классифицирующая роль велика и в самой математике — достаточно вспомнить об «Эрлангенской программе» Клейна.

Таким образом, лежащее в фундаменте современной математики понятие группы является весьма разносторонним орудием самой математики — оно используется как важнейшая составная часть ряда сложных алгебраических систем, как чуткий отражатель свойств различных объектов топологии, как испытательный полигон теории алгоритмов и многими иными путями. Вместе с тем группы — это мощный инструмент познания одной из наиболее глубоких закономерностей реального мира — симметрии.

Перечислим теперь некоторые важные классы групп.

Старейшей и по-прежнему интенсивно развивающейся ветвью теории групп является теория конечных групп. Важное место в ней занимает отыскание конечных простых групп, к которым относятся многие классические группы матриц над конечными полями, несколько серий групп автоморфизмов алгебр Ли, а также отдельные «спорадические» группы. На другом полюсе находятся конечные разрешимые группы, в них обычно интересуются специфическими системами подгрупп (холловых, картеровых и пр.), во многом определяющих строение самой группы. Часто конечные группы возникают в форме групп подстановок или матриц над конечными полями; изучению представлений матрицами и подстановками посвящено большое самостоятельное направление теории конечных групп.

Типичным методом исследования бесконечных групп является наложение на них условий конечности. Здесь наибольшее внимание привлекают периодические группы, локально конечные группы, группы с условием максимальности для подгрупп, группы с условием минимальности для подгрупп, конечно порожденные группы, группы конечного ранга, финитно аппроксимируемые группы.

При изучении абелевых групп важную роль играют полные абелевы группы, абелевы группы без кручения и периодические абелевы группы, а в них сервантные и примарные подгруппы. Исследование произвольной абелевой группы во многом сводится к теориям указанных классов с помощью теории расширений абелевых групп, развиваемой в основном гомологическими методами.

Более широкими по отношению к классу абелевых групп являются классы нильпотентных и разрешимых групп, теория которых также достаточно развита. Из обобщений нильпотентности и разрешимости отметим локальную нильпотентность, локальную разрешимость, нормализаторное условие, энгелевость, а также многочисленные классы групп, определяемые наличием в них нормальных систем того или иного типа.

Наконец, несколько больших самостоятельных разделов теории групп определяются внесением в группу дополнительных структур, согласованных с групповой операцией,— назовем здесь топологические группы, группы Ли, алгебраические группы, линейные группы.

Глава 1

ОПРЕДЕЛЕНИЕ И ВАЖНЕЙШИЕ ЧАСТИ ГРУППЫ

§ 1. Определение группы

1.1. Аксиоматика. Изоморфизм. Множества и функции на них — вот два типа объектов, к изучению которых сводится в конечном счете любая математическая теория. Если аргументы функции f пробегают множество M и она принимает при этом значения из того же самого множества, то f называется *алгебраической операцией* на M. Наука, изучающая алгебраические операции, называется *алгеброй*. При этом алгебру интересует только вопрос, к а к действует та или иная алгебраическая операция, и вовсе не интересует, н а ч е м она действует. Отвлечься от второго вопроса и сосредоточиться на первом позволяет понятие изоморфизма. Пусть заданы два множества с отмеченными на них алгебраическими операциями и можно установить взаимно однозначное соответствие между самими множествами и между множествами операций на них, причем соответственные операции будут функциями одинакового числа аргументов и при соответственных значениях аргументов будут принимать соответственные значения. Тогда эти множества с операциями называют *изоморфными*. Изоморфные объекты одинаково устроены в смысле операций, поэтому в алгебре их не различают или рассматривают как точные копии друг друга — подобно тому, как мы не различаем экземпляров одного и того же романа, напечатанных разным шрифтом и на разной бумаге, если интересуемся только содержанием романа. Разумно считать, что каждый класс изоморфных объектов как раз и выделяет в чистом виде некоторый тип алгебраических операций. Это сводит задачу алгебры — изучение алгебраических операций — к более осязаемой задаче изучения множеств с операциями с точностью до изоморфизма.

Некоторые виды алгебраических операций столь часто встречаются в математике, что их изучение стало предметом самостоятельных теорий. Именно таково по-

нятие группы — предмет теории групп. Группа — эт множество с одной бинарной (двуместной) операцией, под чиняющейся некоторым аксиомам. Значение бинарно операции f на паре элементов x, y удобно записывать н в виде $f(x, y)$, как для других операций, а в виде xfy — это экономит три символа и хорошо согласуется с канонических обозначениями числовых операций: мы ведь пишем $2 + 3 = 5$, а не $+(2, 3) = 5$. В теории групп бинарную операцию называют обычно умножением и обозначают точкой (которую почти всегда опускают), реже используют $+$, $\circ$, $*$ и другие символы. Запись операции точкой называют еще мультипликативной записью, а запись плюсом — аддитивной записью.

1.1.1. Определение. Множество G с бинарной операцией $\cdot$ называется *группой*, если:

1. Операция *ассоциативна*, т. е. $(ab)c = a(bc)$ для любых a, b, c из G.

2. Операция гарантирует единицу, т. е. в G существует такой элемент e — он называется *единицей*, — что $ae = ea = a$ для любого a из G.

3. Операция гарантирует обратные элементы, т. е. для любого a из G существует в G такой элемент x — он называется *обратным* к a,— что $ax = xa = e$.

1.1.2. Определение. Множество G с бинарной операцией $\cdot$ называется *группой*, если:

1. Операция ассоциативна.

2. Операция гарантирует левые и правые частные, т. е. для любых элементов a, b из G существуют в G такие элементы x, y — они называются соответственно *левым* и *правым частными* от деления b на a,— что $ax = b$, $ya = b$.

1.1.3. Упражнение. Определения 1.1.1 и 1.1.2 равносильны. Единица в любой группе G единственна. Для любого элемента a из G обратный к нему единствен (он обозначается a^{-1}). Для любых a, b из G оба частных от деления b на a единственны (они обозначаются: $a \backslash b$ — левое частное и b/a — правое частное).

Согласно общей концепции изоморфизма взаимно однозначное отображение φ одной группы в другую, сохраняющее произведение, называется *изоморфным*. Иными словами, отображение φ группы G в группу G^* (символически $\varphi: G \to G^*$) является изоморфным, если образы различных элементов различны (образ элемента a при ото-

бражении φ обозначаем a^{φ}):

$$a^{\varphi} \neq b^{\varphi} \text{ при } a \neq b \ (a, b \in G)$$

и образ произведения равен произведению образов:

$$(ab)^{\varphi} = a^{\varphi} b^{\varphi}.$$

Группы *изоморфны* (в символах $G \simeq G^*$), если существует изоморфизм одной из них *на* другую.

Например, множество G положительных действительных чисел — группа относительно обычного умножения чисел, множество G^* всех действительных чисел — группа относительно обычного сложения чисел, а отображение φ: $G \to G^*$, определяемое формулой $a^{\varphi} = \log a$,— изоморфизм G на G^*. Пользуясь логарифмической линейкой, мы просто пожинаем плоды этого изоморфизма.

Задача теории групп — изучение групповых операций или, иначе, изучение групп с точностью до изоморфизма. Теория групп была бы закрыта, если бы удалось составить каталог всех возможных групп с точностью до изоморфизма. К счастью для теории групп и к несчастью для приложений, составить такой каталог практически невозможно.

1.2. Примеры. Благодаря ассоциативности в группах элемент $(ab)c = a(bc)$ можно записывать просто как abc, по той же причине однозначно определено произведение n элементов $a_1 a_2 \ldots a_n$ — без указания скобок, но в указанном порядке. Произведение n элементов, равных a, называется *n-й степенью* элемента a и обозначается a^n. Полагают, далее, $a^0 = e$ и для $n < 0$ $a^n = (a^{-n})^{-1}$ или $a^n = (a^{-1})^{-n}$, что, как легко видеть, одно и то же.

1.2.1. Упражнение. Если a — произвольный элемент группы, m, n — целые числа, то $a^m a^n = a^{m+n}$, $(a^m)^n = a^{mn}$.

Может оказаться, что $a^n = e$ при некотором $n > 0$, тогда наименьшее n с этим условием называют *порядком* или *периодом* элемента a и обозначают $|a|$. Если $a^n \neq e$ при любом $n > 0$, то элементу a приписывают бесконечный порядок и пишут $|a| = \infty$.

1.2.2. Упражнение. Если $a^n = e$, то n делится на $|a|$.

1.2.3. Упражнение. Если элементы a, b перестановочны, т. е. $ab = ba$, и их порядки взаимно просты, то $|ab| = |a| \cdot |b|$.

1.2.4. Упражнение. Пусть элементы a, b перестановочны и имеют порядки m, n. Тогда в группе существует элемент — это уже не всегда будет произведение ab,— порядок которого равен наименьшему общему кратному чисел m, n.

Говорят, что G — группа *без кручения*, если любой ее неединичный элемент имеет бесконечный порядок. Если, напротив, порядки всех элементов группы конечны, то она называется *периодической*. Группа, содержащая неединичные элементы как конечного, так и бесконечного порядка, называется *смешанной*. Если порядки элементов периодической группы ограничены в совокупности, то их наименьшее общее кратное называется *периодом* или *показателем* группы. Пусть p — простое число. Периодическая группа, порядки элементов которой являются степенями числа p, называется *p-группой*. Группы, являющиеся p-группами при каком-нибудь простом p, носят общее название *примарных* групп. Мощность $|G|$ группы G называется *порядком* группы. Если эта мощность конечна, то группа G называется *конечной*, в противном случае — *бесконечной*. Если операция в группе G коммутативна, т. е. $ab = ba$ для любых a, b из G, то группа G называется *коммутативной* или *абелевой* — в честь Н. Г. Абеля. Часто коммутативную операцию записывают аддитивно и тогда изменяют терминологию и обозначения, пользуясь следующим словариком:

$\cdot$	$+$
умножение	сложение
произведение	сумма
единица	нуль
обратный	противоположный
степень	кратное
частное	разность
e или 1	0
a^{-1}	$-a$
a^n	na
a/b, $b\backslash a$	$a-b$

Группы вездесущи: теория Галуа и теория дифференциальных уравнений, алгебраическая топология и классификация элементарных частиц в физике, кристаллография и теория относительности, теория узлов, различные другие ветви топологии и теории функций — вот неполный перечень тех областей науки, где появляется понятие группы, причем не праздно «являет себя», а активно работает. Применениям теории групп в разных областях науки посвящены толстые книги, и мы отсылаем интересующихся к этим книгам. Приведем лишь несколько примеров из материала общего курса алгебры, которым мы ограничиваемся в этой книге. (Обозначения, набранные жирным и ажурным шрифтом, закрепляются за соответствующими «классическими» объектами до конца книги. Все они общеприняты — с точностью до нюансов — и широко употребляются в литературе; для удобства читателя полный список таких обозначений вынесен на стр. 8.)

1.2.5. Примеры. I. Множество элементов произвольного кольца K, рассматриваемое относительно операции сложения,— абелева группа. Она называется *аддитивной группой кольца* K. Мы будем обозначать ее той же буквой K, придерживаясь общего принципа, что буква обозначает множество, а какие на нем отмечены операции, должно быть ясно из контекста. В частности, аддитивные группы поля $\mathbb{C}$ комплексных чисел, поля $\mathbb{R}$ действительных чисел, поля $\mathbb{Q}$ рациональных чисел, кольца $\mathbb{Z}$ целых чисел — абелевы группы без кручения. Вообще, аддитивная группа поля нулевой характеристики не имеет кручения, а аддитивная группа поля положительной характеристики p имеет период p. Аддитивные группы конечного поля $\boldsymbol{GF}(q)$ из q элементов и кольца $\mathbb{Z}_n$ вычетов по модулю n — конечные абелевы группы, причем

$$|\,\boldsymbol{GF}(q)\,| = q, \quad |\,\mathbb{Z}_n\,| = n.$$

Пусть p — простое число. Рациональное число вида m/p^n, где m, n — целые числа, называется *p-ичной дробью*. Множество $\mathbb{Q}_p$ всех p-ичных дробей относительно обычного сложения чисел — абелева группа без кручения.

II. Множество всех обратимых элементов произвольного кольца K с единицей, рассматриваемое относительно операции умножения, является группой. Она называ-

ется *мультипликативной группой кольца* K и обозначается K^* (если $|K| \geqslant 2$, то множество K^* заведомо не содержит нуля и потому отлично от множества K). Если кольцо K коммутативно, то и группа K^* коммутативна. В частности, мультипликативные группы $\mathbb{C}^*$, $\mathbb{R}^*$, $\mathbb{Q}^*$, $\mathbb{Z}^*$, $\boldsymbol{GF}(q)^*$, $\mathbb{Z}_n^*$ абелевы. Множество $\mathbb{C}_n$ комплексных чисел, удовлетворяющих уравнению $x^n = 1$, с обычным умножением чисел — абелева группа. Пусть p — простое число. Множество $\mathbb{C}_{p^\infty}$ всех корней уравнений $x^{p^n} = 1$, $n = 1, 2, \ldots$, из поля комплексных чисел с обычным умножением — бесконечная абелева p-группа. Она называется *квазициклической группой типа* p^∞. Группы $\mathbb{Z}^*$, $\boldsymbol{GF}(q)^*$, $\mathbb{Z}_n^*$, $\mathbb{C}_n$ конечны, причем

$$|\mathbb{Z}^*| = 2, \quad |\boldsymbol{GF}(q)^*| = q - 1, \quad |\mathbb{Z}_n^*| = \varphi(n),$$
$$|\mathbb{C}_n| = n,$$

где φ — функция Эйлера, т. е. $\varphi(mn) = \varphi(m)\varphi(n)$ при взаимно простых m, n и $\varphi(p^k) = p^k - p^{k-1}$ при простом p.

III. Пусть M — множество, $\boldsymbol{S}(M)$ — совокупность всех взаимно однозначных отображений M на себя. Если в качестве умножения на $\boldsymbol{S}(M)$ взять последовательное выполнение отображений, то $\boldsymbol{S}(M)$ становится группой. В частности, при $M = \{1, \ldots, n\}$ эта группа превращается в группу всех подстановок n-й степени. В этом случае она называется *симметрической группой* n-й степени и обозначается $\boldsymbol{S}_n$. Группа $\boldsymbol{S}_n$ конечна и $|\boldsymbol{S}_n| = n!$. При $n > 2$ группа $\boldsymbol{S}_n$ неабелева.

IV. Множество $\boldsymbol{GL}_n(K)$ всех обратимых матриц степени n над коммутативным кольцом K с единицей является группой относительно обычного умножения матриц. Она называется *общей линейной* или *общей матричной* группой степени n над кольцом K. Очевидно, $\boldsymbol{GL}_n(K) = \boldsymbol{M}_n(K)^*$, где $\boldsymbol{M}_n(K)$ — кольцо всех матриц степени n над кольцом K. При $n \geqslant 2$ группа $\boldsymbol{GL}_n(K)$ неабелева. Рассмотрим еще в $\boldsymbol{GL}_n(K)$ подмножество $\boldsymbol{SL}_n(K)$ матриц с определителем 1, подмножество $\boldsymbol{D}_n(K)$ диагональных матриц, подмножество $\boldsymbol{T}_n(K)$ матриц с нулевым углом под главной диагональю и подмножество $\boldsymbol{UT}_n(K)$ матриц с нулевым углом под главной диагональю и с единицами по диагонали. Все перечисленные множества тоже являются группами относительно умножения матриц.

Их названия: *специальная линейная группа*, *диагональная группа*, *треугольная группа*, *унитреугольная группа*. Если в качестве K взято конечное поле $GF(q)$, то вместо $GL_n(K)$ пишут также $GL_n(q)$ и аналогично для других матричных групп.

1.2.6. Упражнение. $\mathbb{Z}_n \simeq \mathbb{C}_n$.

1.2.7. Упражнение. Группа $\mathbb{C}^*$ изоморфна группе всех невырожденных матриц вида $\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ с действительными коэффициентами, рассматриваемых относительно обычного умножения матриц.

1.2.8. Упражнение. $\mathbb{Q}_p \ncong \mathbb{Q}_q$ при $p \neq q$.

1.2.9. Упражнение. Если подстановка a из S_n представима в виде произведения независимых циклов длины $n_1, \ldots, n_k$, то ее порядок $|a|$ равен наименьшему общему кратному чисел $n_1, \ldots, n_k$.

Число примеров групп можно сильно увеличить, если указать какую-нибудь конструкцию, производящую из заданных групп новые группы. Теория групп имеет на вооружении разнообразные конструкции такого рода. Одна из самых простых, но важных конструкций состоит в следующем.

Пусть $G_1, \ldots, G_m$ — группы. Легко проверить, что множество $G = G_1 \times \ldots \times G_m$ последовательностей $\langle g_1, \ldots, g_m \rangle$, $g_\alpha \in G_\alpha$, с покомпонентным умножением

$$\langle g_1, \ldots, g_m \rangle \cdot \langle g_1', \ldots, g_m' \rangle = \langle g_1 g_1', \ldots, g_m g_m' \rangle$$

является группой. Ее называют *декартовым произведением* групп G_α, а сами G_α — его *множителями*. Это понятие легко распространить на случай произвольной совокупности множителей G_α, $\alpha \in I$. А именно, обозначим через

$$G = \prod_{\alpha \in I} G_\alpha$$

множество функций

$$f\colon I \to \bigcup_{\alpha \in I} G_\alpha$$

с условием, что $f(\alpha) \in G_\alpha$ для любого $\alpha \in I$. Легко проверить, что множество G с умножением по правилу $(fg)(\alpha) = f(\alpha)\, g(\alpha)$ является группой; она и называется *декартовым произведением* групп G_α. Значение функции f

в точке α называется *проекцией* или *компонентой* элемента f в множителе G_α. Множество

$$\operatorname{supp}(f) = \{\alpha \mid \alpha \in I,\ f(\alpha) \neq e\}$$

называется *носителем* или *суппортом* функции f. Ясно, что множество функций с конечными носителями из декартова произведения групп G_α само является группой относительно умножения функций. Эта группа называется *прямым произведением* групп G_α и обозначается через $\prod_{\alpha\in I} G_\alpha$ (без черты). Очевидно, для конечного числа множителей прямое и декартово произведения совпадают.

При аддитивной записи групповой операции вместо произведений говорят о суммах, вместо множителей — о слагаемых и пишут:

$$G = G_1 \oplus \ldots \oplus G_m,$$

$$G = \sum_{\alpha\in I} G_\alpha,\ G = \overline{\sum_{\alpha\in I}} G_\alpha.$$

1.2.10. Упражнение. $\mathbb{C}_m \times \mathbb{C}_n \simeq \mathbb{C}_{mn}$ при взаимно простых m, n.

1.2.11. Упражнение. $\boldsymbol{D}_n(K) \simeq K^* \times \ldots \times K^*$ (n раз).

1.2.12. Упражнение. Пусть a — элемент группы, имеющий конечный порядок n. Возьмем каноническое разложение числа n на простые множители

$$n = \prod_p p^{m(p)}$$

и положим $n_p = n/p^{m(p)}$. Элемент a^{n_p} имеет порядок $p^{m(p)}$, и существуют такие целые числа x_p, что

$$a = \prod_p a^{n_p x_p}.$$

§ 2. Подгруппы. Нормальные подгруппы

2.1. Подгруппы. Если часть H группы G замкнута относительно умножения, т. е. вместе с любыми двумя своими элементами a, b содержит и их произведение ab, то сужение умножения на H будет алгебраической операцией в H; говорят, что эта операция *индуцирована* умножением

из G. Если H является группой относительно индуцированной операции, то ее называют *подгруппой* группы G и пишут $H \leqslant G$. Если $H \leqslant G$ и $H \neq G$, то пишут $H < G$ (не путать со знаками $\subseteq$, $\subset$ для включения множеств!).

2.1.1. Упражнение. Для того чтобы часть H группы G была подгруппой, необходимо и достаточно, чтобы H была замкнута относительно умножения и обращения, т. е. вместе с любыми двумя своими элементами a, b содержала бы также ab и a^{-1}. Можно эти условия замкнутости записать еще так:

$$HH \subseteq H,\ H^{-1} \subseteq H,$$

если воспользоваться обычными обозначениями

$$AB = \{ab \mid a \in A,\ b \in B\},\ A^{-1} = \{a^{-1} \mid a \in A\}$$

для любых подмножеств A, B данной группы.

2.1.2. Упражнение. Произведение AB подгрупп A, B группы G тогда и только тогда само будет подгруппой, когда $AB = BA$.

2.1.3. Упражнение. Если A, B — конечные подгруппы, то

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

Во всякой группе множество, состоящее только из единицы, а также вся группа являются подгруппами. Подгруппы, отличные от единичной и всей группы, называются *собственными* или *истинными*.

Продолжая изучение групп I — IV из § 1, укажем в них некоторые подгруппы.

2.1.4. Примеры. I. Очевидно,

$$\mathbb{Z} < \mathbb{Q}_p < \mathbb{Q} < \mathbb{R} < \mathbb{C},$$
$$\mathbb{Z} = \bigcap \mathbb{Q}_p,$$
$$GF(p^m) \leqslant GF(p^n) \text{ при } m \mid n.$$

II. Очевидно,

$$\mathbb{Z}^* < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*,$$
$$\mathbf{C}_p < \mathbf{C}_{p^2} < \ldots < \mathbf{C}_{p^\infty},$$
$$\mathbf{C}_{p^\infty} = \bigcup \mathbf{C}_{p^n},$$
$$GF(p^m)^* \leqslant GF(p^n)^* \text{ при } m \mid n.$$

III. В симметрической группе S_n множество A_n всех четных подстановок — подгруппа. Она называется *знакопеременной группой* степени n. Очевидно, $|A_n| = \frac{1}{2}n!$

IV. При $n \geqslant 2$

$$SL_n(K) \leqslant GL_n(K),$$
$$D_n(K) < T_n(K),$$
$$UT_n(K) \leqslant T_n(K) < GL_n(K).$$

Отметим также в $GL_n(K)$ *ортогональную* подгруппу (штрих означает транспонирование):

$$O_n(K) = \{a \mid aa' = e\},$$

а при $K = \mathbb{C}$ еще *унитарную* подгруппу (черта означает взятие комплексно-сопряженного элемента к каждому элементу матрицы):

$$U_n = \{a \mid a\bar{a}' = e\}.$$

Наконец,

$$UT_n(K) = UT_n^1(K) \geqslant UT_n^2(K) \geqslant \ldots,$$

где $UT_n^m(K)$ — множество матриц из $UT_n(K)$ с $m-1$ нулевыми диагоналями выше главной.

2.2. Порождающие множества. Легко видеть, что пересечение любого множества подгрупп — подгруппа. Если M — произвольная часть группы G, то пересечение (M) всех подгрупп, содержащих M, называется подгруппой, *порожденной* множеством M, а само M — *порождающим множеством* подгруппы (M). Допуская вольность речи, иногда говорят, что элементы множества M являются *порождающими элементами* подгруппы (M). Подгруппу (M), особенно в сложных формулах, удобно обозначать также через гр (M). Группа, обладающая конечным порождающим множеством, называется *конечно порожденной*. Более общо и более точно, группа называется $\mathfrak{m}$-*порожденной*, если она обладает порождающим множеством мощности $\mathfrak{m}$.

2.2.1. Теорема. *Если M — подмножество группы G, то*

$$(M) = \{a_1^{\varepsilon_1} \ldots a_m^{\varepsilon_m} \mid a_i \in M,\ \varepsilon_i = \pm 1,\ m = 1, 2, \ldots\}.$$

Доказательство. Обозначим правую часть через H. Так как подгруппа (M) содержит все a_i из M

то $(M) \supseteq H$. С другой стороны, $HH \subseteq H$, $H^{-1} \subseteq H$, поэтому H — подгруппа, содержащая M. Отсюда $H \supseteq (M)$ и окончательно $H = (M)$.

В качестве иллюстрации укажем порождающие множества для групп I — IV из § 1. При этом мы пишем

$$(M) = (\ldots \mid \ldots),$$

если M задано в виде

$$M = \{\ldots \mid \ldots\},$$

т. е. опускаем фигурные скобки внутри круглых.

2.2.2. Примеры. I. Очевидно,

$$\mathbb{Z} = (1),$$
$$\mathbb{Z}_n = (1 \pmod n),$$
$$\mathbb{Q} = \left(\frac{1}{n} \,\middle|\, n = 1, 2, \ldots\right).$$

II. Очевидно,

$$\mathbb{Z}^* = (-1),$$
$$\mathbb{Q}^* = (-1, 2, 3, 5, 7, 11, \ldots),$$
$$\boldsymbol{GF}(q)^* = (\zeta_q),$$
$$\mathbb{C}_n = (\alpha_n),$$
$$\mathbb{C}_{p^\infty} = (\alpha_{p^m} \mid m = 1, 2, \ldots),$$

где ζ_q — первообразный корень уравнения $x^{q-1} = 1$ в поле $\boldsymbol{GF}(q)$,

$$\alpha_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

III. Из общего курса алгебры известно, что симметрическая группа $\boldsymbol{S}_n$ порождается своими транспозициями (ij). Так как $(ij) = (1i)(1j)(1i)$, то $\boldsymbol{S}_n$ порождается даже транспозициями $(12), (13), \ldots, (1n)$. Знакопеременная группа $\boldsymbol{A}_n$ порождается всевозможными тройными циклами (ijk), так как четная подстановка есть произведение четного числа транспозиций и

$$(ij)(ik) = (ijk), \quad (ij)(kl) = (ilj)(jkl).$$

IV. Пусть K — поле. Рассмотрим в $\boldsymbol{GL}_n(K)$ матрицы вида

$$t_{ij}(\alpha) = e + \alpha e_{ij}, \quad d(\beta) = e + (\beta - 1)e_{nn},$$
$$\alpha, \beta \in K, \ \beta \neq 0, \ i \neq j,$$

где e — единичная матрица, e_{ij} — матрица, содержащая на (i, j)-м месте 1, а на остальных местах нули. Матрицы $t_{ij}(\alpha)$ при $\alpha \neq 0$ называются *трансвекциями*. Покажем, что каждая матрица из $GL_n(K)$ представима в виде

$$t_1 \ldots t_r\ d(\beta) t_{r+1} \ldots t_s,$$

где t_i — трансвекции. Это будет означать, в частности, что

$$GL_n(K) = (t_{ij}(\alpha),\ d(\beta) \mid \alpha, \beta \in K,\ i \neq j), \tag{1}$$

$$SL_n(K) = (t_{ij}(\alpha) \mid \alpha \in K,\ i \neq j). \tag{2}$$

Действительно, умножение матрицы на трансвекцию справа равносильно добавлению к одному ее столбцу другого столбца, умноженного на скаляр из K, а умножение на трансвекцию слева равносильно аналогичному преобразованию строк; такие преобразования назовем *элементарными*. Пусть $a \in GL_n(K)$. Элементарными преобразованиями столбцов матрицы a можно добиться, чтобы было $a_{12} \neq 0$. Выполняя еще одно элементарное преобразование — добавляя к первому столбцу второй, умноженный на $\frac{1-a_{11}}{a_{12}}$, мы получим единицу на $(1, 1)$-м месте, а затем с ее помощью получим нули в первой строке и первом столбце нашей матрицы, за исключением $(1, 1)$-го места, где оставим единицу. Продолжая этот процесс применительно к правой нижней клетке степени $n - 1$, мы дойдем в конце концов до матрицы типа $d(\beta)$. Таким образом, $a = t_1 \ldots t_r\, d(\beta)\, t_{r+1} \ldots t_s$, где t_i — трансвекции, что и требовалось.

Аналогично доказывается, что

$$T_n(K) = (t_{ij}(\alpha),\ \operatorname{diag}(\beta_1, \ldots, \beta_r) \mid \alpha, \beta \in K,\ i < j), \tag{3}$$

$$UT_n^m(K) = (t_{ij}(\alpha) \mid \alpha \in K,\ j - i \geqslant m). \tag{4}$$

Полученные результаты позволяют определить $SL_n(K)$ над некоммутативными кольцами K, для которых обычное понятие определителя теряет смысл. А именно, для таких K формулу (2) принимают за определение. Далее, пусть K — тело. Аналогично предыдущему любую обратимую матрицу a над K можно представить в виде $a = t_1 \ldots t_r\, d(\beta)\, t_{r+1} \ldots t_s$, $\beta \neq 0$. Отметим для читателя, знакомого с понятиями коммутанта и фактор-группы, что образ элемента β при факторизации группы K^* по ком-

мутанту называется *определителем матрицы a в смысле Дьёдонне*.

2.2.3. Упражнение. Пусть $n \geqslant 2$, $p_1, \ldots, p_n$ — различные простые числа, $\bar{p}_i = p_1 \ldots p_{i-1} p_{i+1} \ldots p_n$. Тогда

$$\mathbb{Z} = \text{гр } (\bar{p}_1, \ldots, \bar{p}_n),$$

и ни один элемент из этого порождающего множества нельзя удалить.

2.2.4. Упражнение: $S_n = \text{гр } ((12), (12 \ldots n))$.

2.2.5. Упражнение:

$$SL_n(\mathbb{Z}) = \text{гр}\,(e + e_{ij} \mid 1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant n,\ i \neq j),$$

$$SL_n(\mathbb{Z}) = \text{гр}\,(e + e_{12},\ e_{12} + e_{23} + \ldots + e_{n-1,\,n} + (-1)^{n-1} e_{n1}).$$

Антиподом порождающих множеств является подгруппа Фраттини. Чтобы прийти к этому понятию, назовем подгруппу H группы G *максимальной подгруппой со свойством* σ, если H обладает свойством σ и не содержится ни в какой большей подгруппе с этим свойством. Если σ — свойство быть меньше всей группы, то максимальные подгруппы со свойством σ называются просто *максимальными*. Конечно, в группе может и не быть максимальных подгрупп — см. примеры ниже. По определению *подгруппа Фраттини* $\Phi(G)$ группы G — это пересечение всех ее максимальных подгрупп, если они существуют, и сама G — в противном случае.

Элемент x группы G назовем *непорождающим элементом* группы, если его можно удалить из любого порождающего множества группы G, в которое он входит.

2.2.6. Теорема. *Множество S всех непорождающих элементов группы G совпадает с подгруппой Фраттини $\Phi(G)$.*

Доказательство. а) $S \subseteq \Phi(G)$. Действительно, если G не содержит максимальных подгрупп, то утверждение тривиально. Пусть теперь $x \in S$, H — максимальная подгруппа из G. Если $x \notin H$, то $(x, H) = G$, $(H) \neq G$. Это противоречит включению $x \in S$. Значит, $x \in H$, $x \in \Phi(G)$.

б) $\Phi(G) \subseteq S$. Пусть, напротив, существует элемент $x \in \Phi(G)$, который вместе с некоторым множеством M

порождает G, но $(M) \neq G$. По лемме Цорна существуют подгруппы H, максимальные среди подгрупп, содержащих M и не содержащих x. Ясно, что все эти подгруппы просто максимальны. Но тогда они содержат $\Phi(G)$, а вместе с ней x, вопреки построению. Теорема доказана.

2.2.7. Примеры. I. В группе $\mathbb{Z}$ подгруппа (p) максимальна при любом простом p, поэтому $\Phi(\mathbb{Z}) = 0$. Легко сообразить, что в группе $\mathbb{Q}$ любой элемент является непорождающим, поэтому $\Phi(\mathbb{Q}) = \mathbb{Q}$.

II. Так как группа $\mathbb{C}_{p^\infty}$ совпадает с объединением подгрупп $\mathbb{C}_{p^n}$, $n=1, 2, \ldots$, то каждый ее элемент является непорождающим. Поэтому $\Phi(\mathbb{C}_{p^\infty}) = \mathbb{C}_{p^\infty}$.

III. Можно проверить, что подгруппа H_i группы $\boldsymbol{S}_n$, состоящая из всех подстановок, оставляющих символ i неподвижным, максимальна в $\boldsymbol{S}_n$. Так как пересечение $H_1 \cap \ldots \cap H_n$ равно 1, то $\Phi(\boldsymbol{S}_n) = 1$. Аналогично можно показать, что $\Phi(\boldsymbol{A}_n) = 1$.

IV. Выделим в группе $\boldsymbol{UT}_n(\mathbb{Z})$ подгруппу H_{ip}, состоящую из всех матриц x с условием $x_{i,i+1} \in (p)$, где $1 \leqslant i \leqslant n-1$, p — простое число. Можно проверить, что H_{ip} максимальна в $\boldsymbol{UT}_n(\mathbb{Z})$. Так как пересечение всех H_{ip} лежит в $\boldsymbol{UT}_n^2(\mathbb{Z})$, то $\Phi(\boldsymbol{UT}_n(\mathbb{Z})) \leqslant \boldsymbol{UT}_n^2(\mathbb{Z})$. В действительности можно доказать и обратное включение, т. е.

$$\Phi(\boldsymbol{UT}_n(\mathbb{Z})) = \boldsymbol{UT}_n^2(\mathbb{Z}).$$

2.3. Циклические и локально циклические группы. Ранг. Подгруппа (a), порожденная одним элементом a, называется *циклической*. По теореме 2.2.1 она состоит из всевозможных степеней порождающего элемента:

$$(a) = \{a^n \mid n = 0, \pm 1, \pm 2, \ldots\}.$$

Пример 2.2.2.I показывает, что $\mathbb{Z}$ и $\mathbb{Z}_n$ — циклические группы. Оказывается, этими группами исчерпываются — с точностью до изоморфизма — все циклические группы.

2.3.1. Теорема. *Любая бесконечная циклическая группа изоморфна группе $\mathbb{Z}$, любая циклическая группа конечного порядка n изоморфна группе $\mathbb{Z}_n$.*

Доказательство. Пусть (a) — бесконечная циклическая группа. Зададим отображение φ: $\mathbb{Z} \to (a)$, полагая $n^\varphi = a^n$. Оно взаимно однозначно: если бы при $n > m$ было $n^\varphi = m^\varphi$, т. е. $a^{n-m} = e$, то группа (a) ока-

залась бы конечной. Далее, $(n+m)^\varphi = n^\varphi m^\varphi$, т. е. φ — изоморфизм. Если (b), (c) — циклические группы конечного порядка n, то мы получим изоморфизм (b) на (c), если положим $b^k \mapsto c^k$, $0 \leqslant k \leqslant n-1$.

2.3.2. Теорема. *Любая подгруппа циклической группы — циклическая.*

Доказательство. Пусть (a) — циклическая группа порядка n, H — ее неединичная подгруппа (очевидно, единичная подгруппа — циклическая). Пусть m — наименьшее целое число с условием:

$$a^m \in H,\ 0 < m < n.$$

Очевидно, $(a^m) \subseteq H$. Покажем, что в действительности $(a^m) = H$. Возьмем в H произвольный элемент, он имеет вид a^k, $0 \leqslant k < n$. Поделим k на m с остатком: $k = mq + r$, $0 \leqslant r < m$. Тогда

$$a^r = a^k (a^m)^{-q} \in H.$$

По выбору чисел m, r отсюда следует, что $r = 0$ и $a^k \in (a^m)$. Аналогично доказывается цикличность подгрупп бесконечной циклической группы.

Группу называют *локально циклической*, если каждое ее конечное подмножество порождает циклическую подгруппу.

2.3.3. Упражнение. Доказать, что $\mathbb{Q}$ и $\mathbb{C}_{p^\infty}$ — локально циклические группы. В частности, они не допускают никакого конечного порождающего множества.

Более общо, назовем группу *локально $\mathfrak{m}$-порожденной*, если каждая ее конечно порожденная подгруппа является $\mathfrak{n}$-порожденной при некотором $\mathfrak{n} \leqslant \mathfrak{m}$. Наименьшая мощность $\mathfrak{m}$ с этим свойством называется *рангом* группы G. Ясно, что ранг группы всегда либо конечен, либо счетен (тогда он обозначается символом ∞). Таким образом, локально циклические группы — это в точности группы ранга 1. Разумеется, ранг группы не превосходит ее мощности, а ранг подгруппы не превосходит ранга группы.

2.3.4. Упражнение. Если G — прямое произведение p-групп G_p по различным простым числам p,

пробегающим некоторое множество π, то

$$\text{ранг } G = \sup_{p \in \pi} (\text{ранг } G_p).$$

Указание: учесть 1.2.12.

2.4. Смежные классы. С каждой подгруппой H группы G можно связать множества

$$gH = \{gh \mid h \in H\}, \quad g \in G,$$

которые называются *левыми смежными классами* группы G по подгруппе H. Аналогично определяются *правые смежные классы* Hg. Каждый элемент класса называется *представителем* этого класса. Легко видеть, что

$$aH = bH \Leftrightarrow a^{-1}b \in H, \tag{5}$$

$$Ha = Hb \Leftrightarrow ab^{-1} \in H. \tag{6}$$

Это позволяет другим путем прийти к понятию смежных классов. Именно, с подгруппой H свяжем отношение $\sim$ левой смежности — соответственно правой смежности — на множестве G, полагая по определению

$$a \sim b \Leftrightarrow a^{-1}b \in H \ (\textit{левая смежность})$$

и соответственно

$$a \sim b \Leftrightarrow ab^{-1} \in H \ (\textit{правая смежность}).$$

Легко проверяется, что эти отношения являются эквивалентностями на G, т. е. рефлексивны ($a \sim a$), симметричны ($a \sim b \Rightarrow b \sim a$) и транзитивны ($a \sim b$, $b \sim c \Rightarrow a \sim c$), а потому задают два разбиения группы G на непересекающиеся классы. В силу (5), (6) эти разбиения совпадают соответственно с разбиением на левые смежные классы и с разбиением на правые смежные классы. В частности, левые смежные классы попарно не пересекаются, и то же верно для правых классов.

Так как соответствие $gH \leftrightarrow Hg^{-1}$ взаимно однозначно, то мощность множества смежных классов не зависит от того, левые или правые классы рассматриваются. Она называется *индексом* подгруппы H в группе G и обозначается $|G : H|$.

2.4.1. Упражнение. $|\mathbb{Z} : (n)| = n$.

2.4.2. Упражнение. Группа $\mathbb{Q}$ не содержит собственных подгрупп конечного индекса.

2.4.3. Упражнение. $|S_n : A_n| = 2$ при $n \geqslant 2$.

2.4.4. Упражнение. Пусть A, B — подгруппы группы G. Тогда

$$|A : A \cap B| \leqslant |G : B|. \tag{7}$$

Указание: если $\sim_1$, $\sim_2$ — отношения левой смежности соответственно в G по B и в A по $A \cap B$, то второе является сужением на A первого отношения.

Каждый класс gH, Hg равномощен подгруппе H, как показывают взаимно однозначные соответствия $h \leftrightarrow gh$, $h \leftrightarrow hg$, $h \in H$. В частности, если группа G конечна, то ее порядок $|G|$ можно подсчитать, умножив мощность $|H|$ каждого класса на число $|G : H|$ всех классов. Так получается

2.4.5. Теорема (Лагранж). *Если H — подгруппа конечной группы G, то*

$$|G| = |H| \cdot |G : H|. \tag{8}$$

Из нее вытекает важнейшее следствие: порядок подгруппы всегда делит порядок группы. Так как $|a| = |(a)|$, то порядок всякого элемента тоже делит порядок группы.

2.4.6. Упражнение. Всякая группа простого порядка — циклическая.

2.4.7. Упражнение. Пусть A, B — подгруппы группы G, причем $A \leqslant B$. Индексы $|G : B|$, $|B : A|$ оба конечны тогда и только тогда, когда конечен индекс $|G : A|$. Если индекс $|G : A|$ конечен, то

$$|G : A| = |G : B| \cdot |B : A|. \tag{9}$$

Это обобщает теорему Лагранжа (она получается при $A = 1$).

2.4.8. Упражнение. Пересечение конечного числа подгрупп конечного индекса — снова подгруппа конечного индекса.

Указание: с помощью формул (7), (9) вывести формулу

$$|G : A \cap B| \leqslant |G : A| \cdot |G : B|. \tag{10}$$

2.4.9. Упражнение. Пересечение всех подгрупп конечного индекса группы $\mathbb{Q}_p$ совпадает с нулевой под-

группой. Аналогичное утверждение справедливо для любой другой собственной подгруппы группы $\mathbb{Q}$.

2.4.10. Упражнение. Подгруппами $\mathbb{C}_{p^n}$, $n = 1, 2, \ldots$, исчерпываются все собственные подгруппы квазициклической группы $\mathbb{C}_{p^\infty}$. В частности, квазициклическая группа не содержит собственных подгрупп конечного индекса.

Как показывает последнее упражнение, собственные подгруппы квазициклических групп конечны, хотя сами эти группы бесконечны. Каковы все бесконечные группы, собственные подгруппы которых конечны? Эта *проблема О. Ю. Шмидта*, поставленная в 30-е годы, оказалась чрезвычайно трудной. Разумеется, такие группы — назовем их для краткости *группами Шмидта* — обязаны быть периодическими. Будем говорить, что группа *локально конечна*, если все ее конечно порожденные подгруппы конечны. Как установил М. И. Каргаполов (Сиб. матем. ж., 1962, 4, № 1, с. 232—235), среди локально конечных групп единственными группами Шмидта являются квазициклические. Этим и объясняется трудность проблемы — приходится работать в классе периодических, но не локально конечных групп, где даже построение отдельных примеров сопряжено пока с очень большими усилиями — мы еще поговорим об этом более подробно в § 23. Лишь совсем недавно А. Ю. Ольшанский (Изв. АН СССР: Сер. матем., 1980, 44, № 2, с. 309—321) указал первый пример неквазициклических групп Шмидта — построенные им группы бесконечны, порождаются двумя элементами и все их собственные подгруппы имеют конечные и даже простые порядки.

2.5. Классы сопряженных элементов. Особенно важную роль в группах играют те подгруппы, относительно которых левые и правые смежные классы совпадают. Такие подгруппы называются нормальными. Точнее, говорят, что подгруппа H группы G *нормальна* в G и пишут $H \trianglelefteq G$, если $Hx = xH$ для любого x из G. Если $H \trianglelefteq G$ и $H \neq G$, то пишут $H \triangleleft G$.

Ясно, что условие $Hx = xH$ равносильно условию $x^{-1}Hx = H$. Говорят, что элемент a *сопряжен* с элементом b посредством элемента x, если $a = x^{-1}bx$. Часто используют степенные обозначения: $x^{-1}bx = b^x$. Легко про-

верить, что всегда

$$(ab)^x = a^x b^x, \ (a^x)^y = a^{xy}. \tag{11}$$

Если A, B — два подмножества группы, то обозначают

$$A^B = \{a^b \mid a \in A, \ b \in B\}.$$

Теперь можно сказать, что подгруппа H группы G тогда и только тогда нормальна в G, если вместе с каждым своим элементом она содержит и все элементы, сопряженные с ним посредством элементов из G, или, короче, если

$$H^G \subseteq H.$$

Первая из формул (11) показывает, что отображение группы G на себя по правилу $a \mapsto a^x$ (при фиксированном x из G) является изоморфизмом. Подмножество M^x называется *сопряженным* с подмножеством M в группе G. Теперь мы можем выразиться третьим способом: подгруппа тогда и только тогда нормальна, когда она совпадает со всеми своими сопряженными. По этой причине нормальные подгруппы называют еще самосопряженными. Употребительны также названия «нормальный делитель», «инвариантная подгруппа». Группы, не содержащие собственных нормальных подгрупп, называют *простыми*.

2.5.1. Примеры. I. II. Так как аддитивная и мультипликативная группы поля абелевы, то любая их подгруппа нормальна.

III. Так как любая подстановка, сопряженная с четной, снова четна, то $A_n \lhd S_n$.

IV. Пусть $n \geqslant 2$. Так как $\det(ab) = \det a \cdot \det b$, то матрица с определителем 1 переходит после сопряжения снова в такую же матрицу, поэтому $SL_n(K) \trianglelefteqslant GL_n(K)$. Так как при умножении треугольных матриц их диагональные элементы на одинаковых местах перемножаются, то $UT_n(K) \trianglelefteqslant T_n(K)$. В действительности можно проверить, что $UT_n^m(K) \trianglelefteqslant T_n(K)$ для любого $m = 1, 2, \ldots$

2.5.2. Упражнение. Если p — простое число, то $\mathbb{Z}_p$ — простая группа.

2.5.3. Упражнение. Если $|G : H| = 2$, то $H \lhd G$.

2.5.4. Упражнение. Если $A \trianglelefteqslant G$, $B \trianglelefteqslant G$, то $AB \trianglelefteqslant G$.

2.5.5. Упражнение. Может случиться, что $A \trianglelefteqslant B$, $B \trianglelefteqslant C$, но $A \not\trianglelefteqslant C$.

Пусть G — произвольная группа. Определим на ней отношение $\sim$, полагая $a \sim b$, если элементы a, b сопряжены в G. Легко проверяется, что это отношение — эквивалентность, т. е. рефлексивно ($a \sim a$), симметрично ($a \sim b \Rightarrow b \sim a$) и транзитивно ($a \sim b$, $b \sim c \Rightarrow a \sim c$). Поэтому G разбивается на непересекающиеся *классы сопряженных элементов* a^G. В частности, нормальными подгруппами будут такие подгруппы, которые состоят из нескольких полных классов сопряженных элементов.

В отличие от смежных классов классы сопряженных элементов не всегда равномощны. При вычислении их мощностей решающую роль играет понятие нормализатора. Пусть M — подмножество, H — подгруппа группы G. *Нормализатором* множества M в подгруппе H называется множество

$$N_H(M) = \{h \mid h \in H,\ M^h = M\},$$

которое, как легко проверить, является подгруппой в H. Если не указано, в какой подгруппе H берется нормализатор, то это означает, что он берется во всей группе G. Очевидно, подгруппа тогда и только тогда нормальна в группе, когда ее нормализатор совпадает со всей группой.

2.5.6. Теорема. *Если M — подмножество, H — подгруппа группы G, то мощность класса подмножеств, сопряженных с M элементами из H, равна индексу $|H : N_H(M)|$. В частности,*

$$|a^G| = |G : N_G(a)|.$$

Доказательство. Отобразим множества M^x, $x \in H$, на правые смежные классы группы H по подгруппе $N = N_H(M)$, полагая

$$(M^x)^\varphi = Nx \text{ для } x \in H.$$

Отображение φ однозначно, так как из $M^x = M^y$ следует $Nx = Ny$. Отображение φ переводит разные элементы в разные, так как из $Nx = Ny$ следует $M^x = M^y$. Наконец, φ — отображение *на*, так как каждое Nx имеет прообраз M^x. Теорема доказана.

2.5.7. Примеры. I. II. Так как аддитивная и мультипликативная группы поля абелевы, то любой их класс сопряженных элементов состоит из одного элемента.

III. Пусть M — множество. Два отображения из $S(M)$ тогда и только тогда сопряжены в $S(M)$, когда в разложении на независимые циклы они содержат одинаковое число циклов каждой длины, включая и одноэлементные циклы (здесь число и длина циклов понимаются в смысле мощности). Действительно, если

$$a = (\alpha_1\alpha_2 \ldots)(\beta_1\beta_2 \ldots)(\ldots)\ldots,$$
$$a' = (\alpha_1'\alpha_2' \ldots)(\beta_1'\beta_2' \ldots)(\ldots)\ldots,$$

причем циклы одинаковой длины выписаны друг против друга, то непосредственно проверяется, что $a' = a^x$, где

$$x = \begin{pmatrix} \alpha_1\alpha_2 \ldots \beta_1\beta_2 \ldots \\ \alpha_1'\alpha_2' \ldots \beta_1'\beta_2' \ldots \end{pmatrix}.$$

В частности, две подстановки из S_n тогда и только тогда сопряжены в S_n, когда они имеют одинаковое циклическое строение,— например, подстановка (12)(3456) сопряжена в S_6 с подстановкой (15)(2436) и не сопряжена с подстановкой (12)(345)(6). Что касается знакопеременной группы A_n, то элементы одинакового циклического строения составляют в ней либо 1, либо 2 равномощных класса сопряженных элементов — это легко усматривается из теоремы 2.5.6 и соотношения $|S_n : A_n| = 2$.

IV. Как помнит читатель, вопрос о сопряженности матриц занимает важное место в общем курсе алгебры. Для алгебраически замкнутых полей K вопрос о сопряженности элементов из $GL_n(K)$ исчерпывающим образом решается теоремой Жордана: две матрицы из $GL_n(K)$ тогда и только тогда сопряжены в этой группе, когда они приводятся к одинаковой жордановой форме.

2.5.8. Упражнение. Порядки сопряженных элементов (вообще, мощности сопряженных множеств) равны.

2.5.9. Упражнение. Пусть подстановка a из S_n разлагается на независимые циклы с длинами n_1 . . . . . n, $\sum n_i = n$. Вычислить $|N_{S_n}(a)|$.

2.5.10. Упражнение. Проверить формулу

$$d^{-1}(\beta)\,t_{ij}(\alpha)\,d(\beta)=\begin{cases}t_{in}(\alpha\beta) & \text{при } j=n,\\ t_{nj}\left(\frac{\alpha}{\beta}\right) & \text{при } i=n,\\ t_{ij}(\alpha) & \text{в остальных случаях.}\end{cases}$$

Пользуясь ею, убедиться, что в примере 2.2.2.IV можно считать $r=0$.

2.5.11. Упражнение. Нормализаторы всех элементов, сопряженных с данными, составляют класс сопряженных подгрупп.

2.5.12. Упражнение. В группе матриц вида $\begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix}$, $\alpha\neq 0$, над полем $\mathbb{Q}$ указать подгруппу, сопряженную с некоторой своей истинной подгруппой.

2.5.13. Упражнение. Если A — подгруппа конечного индекса группы G, то пересечение

$$N=\bigcap_{x\in G}A^x$$

является нормальной подгруппой конечного индекса в G.

Указание: воспользоваться теоремой 2.5.6 и упражнением 2.4.8.

§ 3. Центр. Коммутант

Мы видели, что произвольная группа может сильно отличаться по свойствам от числовых групп. Во многом это отличие связано с некоммутативностью. Отклонение от коммутативности измеряется центром и коммутантом: чем больше центр и чем меньше коммутант группы, тем ближе она к абелевым группам.

3.1. Центр. Пусть M — подмножество, H — подгруппа группы G. Мы назвали нормализатором M в H совокупность тех элементов из H, которые перестановочны с множеством M в целом. Можно рассмотреть также множество тех элементов из H, которые перестановочны с M поэлементно, т. е.

$$C_H(M)=\{x \mid x\in H,\ m^x=m \text{ для всех } m\in M\}.$$

Это множество называется *централизатором* множества M в подгруппе H и является, как нетрудно проверить,

нормальной подгруппой нормализатора $N_H(M)$. Если M состоит из одного элемента, то, конечно, его нормализатор и централизатор в H совпадают. Если не указано, в какой подгруппе H берется централизатор, то это означает, что он берется во всей группе G.

Централизатор всей группы G называется ее *центром* и обозначается $Z(G)$. Очевидно, группа тогда и только тогда абелева, когда она совпадает со своим центром. Ясно, что единица всегда лежит в центре. Если других центральных элементов группа не содержит, то она называется *группой с тривиальным центром* или даже *группой без центра*. Заметим еще, что любая подгруппа центра нормальна в группе.

Для иллюстрации вычислим центры в группах I — IV из § 1.

3.1.1. Примеры. I.II. Так как аддитивная и мультипликативная группы поля абелевы, то они совпадают со своим центром.

III. Очевидно, группы S_2 и A_3 абелевы и поэтому совпадают с центром. Далее, любая нетождественная подстановка из S_n, разложенная на независимые циклы, имеет вид $(ij\ldots)(\ldots)\ldots$ Непосредственно проверяется, что она не перестановочна с транспозицией (jk) при $n \geqslant 3$, а также с тройным циклом (jkl) при $n \geqslant 4$; здесь разные буквы обозначают разные символы. Значит, группы S_n при $n \geqslant 3$ и группы A_n при $n \geqslant 4$ имеют тривиальный центр.

IV. Пусть K — поле. Центры групп $GL_n(K)$, $SL_n(K)$ состоят из содержащихся в них скалярных матриц. Действительно, любая скалярная матрица, очевидно, лежит в центре. Обратно, если a — центральный элемент любой из этих групп, то он перестановочен со всеми трансвекциями $t_{ij} = t_{ij}(1)$, т. е. $at_{ij} = t_{ij}a$. Отсюда легко получаем, что

$$a_{ij} = 0,\ a_{ii} = a_{jj} \text{ при всех } i \neq j,$$

т. е. a — скалярная матрица. В этом и других подобных вычислениях мы советуем читателю записывать каждую матрицу x в виде $\sum x_{rs}e_{rs}$ и пользоваться известной таблицей умножения матричных единиц:

$$e_{ij}e_{rs} = \begin{cases} e_{is} & \text{при } j = r, \\ 0 & \text{при } j \neq r, \end{cases} \tag{1}$$

Аналогичные рассуждения показывают, что центр группы $\boldsymbol{T}_n(K)$, $|K| \neq 2$, состоит из всевозможных скалярных матриц, отличных от нулевой, а в группе $\boldsymbol{UT}_n^m(K)$ центральными будут в точности те матрицы, которые отличаются от матрицы e только правой верхней клеткой степени m. В частности,

$$Z(\boldsymbol{UT}_n(K)) = \boldsymbol{UT}_n^{n-1}(K) = \{t_{1n}(\alpha) \mid \alpha \in K\}. \qquad (2)$$

Диагональная группа $\boldsymbol{D}_n(K)$ абелева и потому совпадает с центром.

3.1.2. Упражнение. Найти централизатор диагональной матрицы в $\boldsymbol{GL}_n(K)$.

3.1.3. Упражнение. Централизатор нормальной подгруппы сам является нормальной подгруппой.

3.1.4. Упражнение. Если H — конечная нормальная подгруппа группы G, то индекс ее централизатора конечен.

Решение:

$$|G : C_G(H)| = |G : \bigcap_{x \in H} C_G(x)| \leqslant \prod_{x \in H} |G : C_G(x)| \leqslant |H|^{|H|}.$$

3.1.5. Упражнение. Группа матриц $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$, $\alpha \neq 0$, над полем, отличным от $\boldsymbol{GF}(2)$, имеет тривиальный центр.

3.1.6. Упражнение: $|Z(\boldsymbol{GL}_n(q))| = q - 1$, $|Z(\boldsymbol{SL}_n(q))| =$ н.о.д. $(n, q - 1)$.

3.1.7. Упражнение. Центр прямого (декартова) произведения совпадает с прямым (декартовым) произведением центров сомножителей.

3.2. Коммутант. Очевидно, элементы a, b группы G тогда и только тогда перестановочны, когда $a^{-1}b^{-1}ab = e$. Левая часть этого соотношения называется *коммутатором* элементов a, b — в указанном порядке — и обозначается $[a, b]$. Подгруппа, порожденная в G всевозможными коммутаторами, называется *коммутантом* группы G. Ясно, что группа тогда и только тогда коммутативна, когда ее коммутант равен единице, а в общем случае коммутант в некотором смысле измеряет отклонение от коммутативности.

Более общо, если L, M — подмножества группы G, то их *взаимным коммутантом* называют подгруппу

$$[L, M] = \text{гр}([a, b] \mid a \in L, b \in M).$$

Так как

$$[a, b]^x = [a^x, b^x],$$

то взаимный коммутант нормальных подгрупп — нормальная подгруппа. В частности, коммутант $[G, G]$ группы G — нормальная подгруппа. Беря коммутант от коммутанта и т. д., мы получим убывающую цепочку нормальных подгрупп

$$G \geqslant G' \geqslant G'' \geqslant \ldots,$$

которая называется *рядом коммутантов* группы G. Иногда коммутант называют производной группой, а ряд коммутантов — производным рядом.

Отметим полезные коммутаторные соотношения, проверяемые непосредственно:

$$[a, b]^{-1} = [b, a],\ [ab, c] = [a, c]^b\ [b, c],\ [a^{-1}, b] = [b, a]^{a^{-1}}. \tag{3}$$

Теперь, как обычно, проиллюстрируем новое понятие на группах I — IV из § 1.

3.2.1. Примеры. I.II. Так как аддитивная и мультипликативная группы поля абелевы, то их коммутанты равны единице.

III. Очевидно, $[S_2, S_2] = 1$, $[A_3, A_3] = 1$. Далее,

$$[A_4, A_4] = \{1,\ (12)(34),\ (13)(24),\ (14)(23)\}. \tag{4}$$

Действительно, непосредственно проверяется, что правая часть — подгруппа (она называется *четверной группой Клейна*). Эта подгруппа даже нормальна в A_4, так как содержит все подстановки типа $(**)(**)$, а при сопряжениях, как мы знаем, циклический тип подстановки не меняется. Так как A_n порождается всевозможными тройными циклами, то для включения $\subseteq$ ввиду формул (3) и нормальности правой части (4) достаточно проверить, что коммутаторы от тройных циклов лежат в правой части. Но это сразу вытекает из соотношений

$$[(ijk),\ (ijl)] = (ij)(kl),\ [(ijk),\ (ilj)] = (il)(jk),$$

которые проверяются непосредственно; здесь разные буквы обозначают разные символы. Эти же соотношения доказывают и обратное включение. Наконец,

$$[S_n, S_n] = A_n \text{ при любом } n, \tag{5}$$

$$[A_n, A_n] = A_n \text{ при } n \geqslant 5. \tag{6}$$

Действительно, коммутатор любых двух подстановок из S_n есть четная подстановка и потому лежит в A_n. С другой стороны,

$$(ijk) = [(ik), (ij)] = [(ikl), (ijm)],$$

где разные буквы обозначают разные символы. Так как A_n порождается тройными циклами, то всё доказано.

IV. Пусть K — поле. Всегда

$$[GL_n(K), GL_n(K)] = SL_n(K), \tag{7}$$

$$[SL_n(K), SL_n(K)] = SL_n(K), \tag{8}$$

за исключением группы GL_2 (2) в первой формуле и групп SL_2 (2), SL_2 (3) во второй формуле (отметим, что $GL_2(2) = SL_2(2)$, так что фактически исключительных групп две). Действительно, определитель коммутатора любых двух матриц равен 1, поэтому включения слева направо очевидны. С другой стороны, мы знаем, что $SL_n(K)$ порождается трансвекциями. Легко проверить, что

$$[t_{ik}(\alpha), t_{kj}(\beta)] = t_{ij}(\alpha\beta) \text{ при различных } i, j, k, \tag{9}$$

$$[t_{ij}(\alpha), \operatorname{diag}(\beta_1, \ldots \beta_n)] = t_{i_j}\left(\alpha\left(\frac{\beta_j}{\beta_i} - 1\right)\right). \tag{10}$$

Ввиду (9) обратные включения для $n \geqslant 3$ тоже справедливы. Пусть теперь $n = 2$. Так как при $|K| > 2$ можно в формуле (10) выбрать $\beta_1 \neq \beta_2$, то формула (7) доказана для всех групп, кроме GL_2 (2). Так как при $|K| > 3$ можно выбрать $\beta_1 \neq \beta_2$, $\beta_1\beta_2 = 1$, то формула (8) доказана для всех групп, кроме SL_2 (2), SL_2 (3). Отмеченные группы действительно исключительные — можно показать, что для них формулы (7), (8) несправедливы.

Аналогичным образом, используя формулы (3), (4) предыдущего параграфа и формулы (9), (10), получим, что

$$[T_n(K), T_n(K)] = UT_n(K) \text{ при } |K| > 2, \tag{11}$$

$$[UT_n^r(K), UT_n^s(K)] = UT_n^{r+s}(K). \tag{12}$$

При $|K| = 2$ первая формула неверна, но тогда $T_n(K) = UT_n(K)$, и можно пользоваться второй формулой.

3.2.2. Л е м м а. *Пусть G — произвольная группа, A, B — ее подгруппы, $H = \text{гр}\,(A, B)$. Тогда*

$$[A, B],\ A\,[A,\ B],\ B\,[A, B] \text{ нормальны в } H, \tag{13}$$

$$A\,[A, B]\cdot B\,[A, B] = H, \tag{14}$$

$$[A, B] = \text{гр}\,(\text{гр}\,(C^A))^B, \tag{15}$$

где $C = \{[a_i, b_j] \mid i \in I,\ j \in J\}$, если $A = \text{гр}\,(a_i \mid i \in I)$, $B = \text{гр}\,(b_j \mid j \in J)$.

Д о к а з а т е л ь с т в о. Второе из тождеств (3) показывает, что подгруппа A нормализует $[A, B]$, а тогда (13), (14) очевидны. Докажем (15). Так как $C \subseteq [A, B] \trianglelefteqslant H$, то вложение справа налево очевидно. Проверим обратное вложение $[A, B] \leqslant D$, где D обозначает правую часть (15). Нам надо проверить, что

$$[a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m}, b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n}] \in D \text{ при } \varepsilon_i = \pm 1,\ \delta_j = \pm 1.$$

Имеем

$$(a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m})^{b_j} = (a_{i_1}[a_{i_1}, b_j])^{\varepsilon_1} \ldots (a_{i_m}[a_{i_m}, b_j])^{\varepsilon_m} =$$

$$= a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m} f, \qquad f \in \text{гр}\,(C^A),$$

т. е.

$$[a, b_j] \in \text{гр}\,(C^A), \text{ где } a = a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m}.$$

Отсюда

$$(b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n})^a = (b_{j_1}[b_{j_1}, a])^{\delta_1} \ldots (b_{j_n}[b_{j_n}, a])^{\delta_n} =$$

$$= b_{j_1}^{\delta_1} \ldots b_{j_n}^{\delta_n} d, \qquad d \in D,$$

что и требовалось доказать.

Пусть теперь $a_1, a_2, \ldots, A_1, A_2, \ldots$ — соответственно элементы и подгруппы некоторой группы. Положим по индукции

$$[a_1, \ldots, a_{n+1}] = [[a_1, \ldots, a_n],\ a_{n+1}],$$

$$[A_1, \ldots, A_{n+1}] = [[A_1, \ldots, A_n],\ A_{n+1}]$$

при $n \geqslant 2$.

3.2.3. Л е м м а о т р е х к о м м у т а н т а х. *Пусть A, B, C — подгруппы некоторой группы, H — ее нормальная подгруппа. Если два из коммутантов*

$$[A, B, C],\ [B, C, A],\ [C, A, B]$$

лежат в H, то и третий лежит в H.

Доказательство вытекает из следующего красивого соотношения, проверяемого непосредственно (тождество Ф. Холла):

$$[a, b^{-1}, c]^b[b, c^{-1}, a]^c[c, a^{-1}, b]^a = 1. \qquad (16)$$

3.2.4. Упражнение. Найти ряды коммутантов групп S_3, S_4.

3.2.5. Упражнение. Найти коммутанты групп $SL_2(2)$, $SL_2(3)$.

3.2.6. Упражнение. Если A, B, C — нормальные подгруппы некоторой группы, то $[AB, C] = [A, C]\cdot[B, C]$.

3.2.7. Упражнение. Коммутант прямого произведения групп есть прямое произведение коммутантов сомножителей. Можно ли здесь прямые произведения заменить на декартовы?

3.2.8. Упражнение. Найти коммутант группы матриц $\begin{pmatrix}\alpha & \beta\\ 0 & 1\end{pmatrix}$, $\alpha \neq 0$, над полем и показать, что каждый элемент этого коммутанта — коммутатор.

Обращаем внимание читателя, что, вообще говоря, коммутант группы не исчерпывается коммутаторами. Существуют даже конечные группы, в которых произведение двух коммутаторов может не равняться никакому коммутатору. Мы закончим параграф примером такой группы с наброском доказательства.

3.2.9. Пример. Рассмотрим множество S из 10 символов со следующей таблицей умножения:

·	1	α	β	γ	δ	ϰ	λ	μ	ν	0
1	1	α	β	γ	δ	ϰ	λ	μ	ν	0
α	α	0	ϰ	λ	μ	0	0	0	0	0
β	β	0	0	ν	0	0	0	0	0	0
γ	γ	0	0	0	0	0	0	0	0	0
δ	δ	0	0	0	0	0	0	0	0	0
ϰ	ϰ	0	0	0	0	0	0	0	0	0
λ	λ	0	0	0	0	0	0	0	0	0
μ	μ	0	0	0	0	0	0	0	0	0
ν	ν	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0	0

Легко проверить, что умножение в S ассоциативно, т. е., как говорят, S — *полугруппа*. Пусть K — полугрупповое кольцо для S над полем GF (2), т. е. кольцо формальных комбинаций

$$n_1 1 + n_2\alpha + n_3\beta + n_4\gamma + n_5\delta + n_6\varkappa + n_7\lambda + n_8\mu + \\ + n_9\nu + n_{10}0$$

с коэффициентами из GF (2) относительно естественных операций сложения и умножения. Наконец, пусть G — множество всех матриц над K вида

$$a = \begin{pmatrix} 1 & x & y \\ 0 & 1 & x \\ 0 & 0 & 1 \end{pmatrix}.$$

Легко проверить, что G — группа порядка 2^{20}, причем если

$$b = \begin{pmatrix} 1 & u & v \\ 0 & 1 & u \\ 0 & 0 & 1 \end{pmatrix}, \text{ то } [a, b] = \begin{pmatrix} 1 & 0 & xu - ux \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad (17)$$

Назовем $xu - ux$ кольцевым коммутатором элементов x, u.

3.2.10. Упражнение. Элемент $\mu + \nu$ есть сумма двух кольцевых коммутаторов, но сам не является кольцевым коммутатором.

3.2.11. Упражнение. Используя (17) и предыдущее упражнение, указать в группе G произведение двух коммутаторов, не являющееся коммутатором.

Глава 2

ГОМОМОРФИЗМЫ

§ 4. Гомоморфизмы и фактор-группы

4.1. Определения. Согласно одному из исходных определений отображение группы в группу называется изоморфизмом, если оно взаимно однозначно и сохраняет операцию. Отказываясь от первого требования, приходим к понятию гомоморфизма: отображение φ группы G в группу G^* называется *гомоморфным* или *гомоморфизмом*, если $(ab)^\varphi = a^\varphi b^\varphi$ для любых элементов a, b из G.

4.1.1. Примеры. I. Отображение $\mathbb{Z} \to \mathbb{Z}_n$, сопоставляющее целому числу его вычет по модулю n, является гомоморфным. Пусть p — простое число, ε_n — первообразный корень степени p^n из 1 в поле комплексных чисел, причем $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ Отображение $\mathbb{Q}_p \to \mathbb{C}_{p^\infty}$, сопоставляющее p-ичной дроби $\frac{m}{p^n}$ комплексное число ε_n^m, хорошо определено и является гомоморфизмом.

II. Отображение $\mathbb{R}^* \to \mathbb{Z}^*$, сопоставляющее каждому числу из $\mathbb{R}^*$ его знак,— гомоморфизм.

III. Отображение $S_n \to \mathbb{Z}^*$, сопоставляющее каждой подстановке ее знак в зависимости от четности,— гомоморфизм.

IV. Гомоморфизмами будут: отображение $GL_n(K) \to K^*$, сопоставляющее матрице ее определитель; отображение $T_n(K) \to D_n(K)$, сопоставляющее треугольной матрице ее диагональ; отображение $UT_n^m(K) \to K \oplus \ldots \oplus K$ ($n - m$ раз), сопоставляющее матрице x строчку $\langle x_{1,\,m+1},\ x_{2,\,m+2},\ \ldots,\ x_{n-m,\,n}\rangle$.

Мы видим, что при гомоморфном отображении некоторые свойства алгебраической операции могут потеряться: некоммутативная группа может стать коммутативной, группа без кручения — периодической и т. д., хотя наиболее «памятные» свойства — конечность, коммутативность и т. п.— сохраняются при всех гомоморфизмах. Можно сказать, что гомоморфный образ группы G — это

воспоминание о ней, запечатлевшее с точки зрения очевидца-гомоморфизма наиболее существенные черты G. Лишенное некоторых деталей, оно неполно характеризует героиню, но, во-первых, именно поэтому его легче изучать, а во-вторых, опросив нескольких очевидцев, можно собрать и всю нужную информацию о G. Например, зная, что группы $\mathbb{Z}_2$, $\mathbb{Z}_3$, ... являются гомоморфными образами группы G, можно утверждать, что G бесконечна, хотя знание любого из этих образов в отдельности недостаточно для такого заключения.

4.1.2. Упражнение. Гомоморфный образ (нормальной) подгруппы — (нормальная) подгруппа. Сужение гомоморфизма на подгруппу — гомоморфизм подгруппы.

Пусть φ — гомоморфизм группы G в группу G^*. Множество всех элементов из G, отображающихся при φ в единицу, называется *ядром* гомоморфизма φ и обозначается $\operatorname{Ker}\varphi$. Ядро любого гомоморфизма является нормальной подгруппой. Действительно, пусть $\operatorname{Ker}\varphi = H$. Так как

$$(HH)^\varphi = H^\varphi H^\varphi = 1, \quad (H^{-1})^\varphi = (H^\varphi)^{-1} = 1,$$
$$(H^G)^\varphi = (H^\varphi)^{G^\varphi} = 1,$$

то

$$HH \subseteq H, \quad H^{-1} \subseteq H, \quad H^G \subseteq H.$$

Но это и означает, что $H \trianglelefteq G$. Далее, легко сообразить, что ядро гомоморфизма φ тогда и только тогда тривиально ($\operatorname{Ker}\varphi = 1$), когда φ — изоморфизм. В общем случае можно сказать, что ядро гомоморфизма измеряет его забывчивость: чем больше ядро, тем больше деталей забывает гомоморфизм. Самый забывчивый гомоморфизм помнит о группе только то, что в ней была единица.

Оказывается, ядрами гомоморфизмов исчерпываются все нормальные подгруппы в группе, т. е. любая нормальная подгруппа служит ядром некоторого гомоморфизма. Стандартный способ построения гомоморфизма с заданным ядром состоит в следующем. Пусть G — группа, H — ее нормальная подгруппа, G/H — множество классов G по H (сейчас нет нужды говорить о левых или правых классах — ввиду нормальности H они совпадают). Легко понять, что $aH \cdot bH = abH$, т. е. множество G/H замкнуто относительно поэлементного умножения классов. Легко проверить, что G/H — даже группа относительно этого

умножения; она называется *фактор-группой* группы G по нормальной подгруппе H. Единицей группы G/H является класс H, а обратным к классу aH — класс $a^{-1}H$. Подчеркнем, что класс aH является классом элементов в группе G, но в группе G/H он сам является элементом, а не классом. Непосредственно ясно, что отображение φ: $G \to G/H$ по правилу $g^{\varphi} = gH$ есть гомоморфизм. Такие гомоморфизмы называют *естественными*. Они и решают нашу задачу: ядром естественного гомоморфизма $G \to G/H$ служит как раз H.

4.1.3. Упражнение. Фактор-группа циклической группы — циклическая.

4.1.4. Упражнение. Фактор-группа G/H тогда и только тогда абелева, когда H содержит коммутант $[G, G]$.

Другой подход к понятию фактор-группы, отличный от приведенного в тексте, дает

4.1.5. Упражнение. Эквивалентность $\sim$ на группе G называется *конгруэнтностью*, если всегда

$$a \sim b,\ a' \sim b' \Rightarrow aa' \sim bb'.$$

Произведение двух классов конгруэнтных элементов — снова класс конгруэнтных элементов. Множество $G/\sim$ всех классов конгруэнтных элементов является группой относительно умножения классов. Она называется *фактор-группой* группы G по конгруэнтности $\sim$. Аналогичное понятие легко определить для произвольной системы с операциями.

4.1.6. Упражнение. Всевозможные конгруэнтности на группе находятся во взаимно однозначном соответствии с нормальными подгруппами из G. Именно, если $H \trianglelefteqslant G$ и если положить по определению

$$a \sim b \Leftrightarrow a^{-1}b \in H,$$

то отношение $\sim$ будет конгруэнтностью, а смежные классы G по H — классами конгруэнтных элементов. Обратно, если на G задана конгруэнтность $\sim$, то множество H элементов, конгруэнтных единице, будет нормальной подгруппой в G, а классы конгруэнтных элементов — смежными классами G по H. Таким образом, фактор-группы по конгруэнтностям совпадают с фактор-группами по нормальным подгруппам. В других системах с операциями

понятие фактор-систем по конгруэнтностям по-прежнему имеет смысл, хотя разумного аналога нормальных подгрупп может не существовать. Таким образом, для групп подход упражнения 4.1.5 равносилен подходу, приведенному в тексте, но в общей ситуации первый лучше.

4.1.7. (Факторизация и ранг.) *Если H — нормальная подгруппа группы G, то*

$$\text{ранг } G \leqslant \text{ранг } H + \text{ранг } G/H .$$

Доказательство. Пусть r, s — ранги групп H и G/H соответственно. Возьмем в G конечное подмножество M и рассмотрим в фактор-группе G/H подгруппу, порожденную элементами xH, $x \in M$. Так как она конечно порождена, то в гр (M) можно выбрать такое подмножество S мощности s, что

$$\text{гр } (xH \mid x \in M) = \text{гр } (xH \mid x \in S).$$

Зафиксируем для каждого $x \in M$ какую-нибудь запись

$$x = x_S x_H, \quad x_S \in \text{гр } (S), \quad x_H \in H.$$

Так как гр $(x_H \mid x \in M)$ — конечно порожденная подгруппа группы H, то она порождается некоторым подмножеством R мощности $\leqslant r$. Теперь ясно, что гр $(M) = \text{гр } (R \cup S)$, т. е. ранг $G \leqslant r + s$.

4.2. Теоремы о гомоморфизмах. Если G — группа, H — ее подгруппа, то обозначим через $L(G, H)$ совокупность всех подгрупп группы G, содержащих H. В частности, $L(G, 1)$ — совокупность всех подгрупп из G. Справедлива следующая теорема о соответствии подгрупп при гомоморфизме.

4.2.1. Теорема. *Если задан естественный гомоморфизм* $\varphi: G \to G/H$, *то возникает отображение* $\psi: L(G, H) \to L(G/H, 1)$, *сопоставляющее подгруппам из* $L(G, H)$ *их образы относительно* φ. *Это* ψ *является взаимно однозначным отображением* на. *Если* A, B — *подгруппы из* $L(G, H)$, *то они сопряжены в* G *тогда и только тогда, когда их образы* A^ψ, B^ψ *сопряжены в* G/H. *В частности, A нормальна в G тогда и только тогда, когда A^ψ нормальна в G/H. Если $A \leqslant B$, то $|B : A| = |B^\psi : A^\psi|$.*

Доказательство. Отображение ψ переводит разные подгруппы A, B из $L(G, H)$ в разные: если $a \in A$, $a \notin B$, то $a^\varphi \in A^\varphi$, $a^\varphi \notin B^\varphi$. Действительно, если $a^\varphi \in$

$\in B^\varphi$, то $a^\varphi = b^\varphi$, $b \in B$, откуда $b^{-1}a \in H \leqslant B$, $a \in B$, вопреки допущению. Далее, ψ — отображение *на*, так как прообразом данной подгруппы $\bar{A}$ из G/H относительно ψ будет полный прообраз $\bar{A}$ относительно φ. Столь же непосредственно проверяется, что

$$B = A^x \Leftrightarrow B^\varphi = (A^\varphi)^{x^\varphi}.$$

Наконец, если $A \leqslant B$, то между левыми смежными классами B по A и левыми смежными классами B^ψ по A^ψ существует взаимно однозначное соответствие, так как

$$x^{-1}y \in A \Leftrightarrow (xH)^{-1}(yH) \in A/H.$$

Теорема доказана.

Оказывается, естественными гомоморфизмами исчерпываются по существу все гомоморфизмы группы, точнее, любой гомоморфизм можно получить, выполнив сначала естественный гомоморфизм, а затем изоморфизм. Сейчас мы увидим также, что «гомоморфизмы с одним и тем же ядром помнят о группе одно и то же: их воспоминания изоморфны».

4.2.2. Т е о р е м а. *Если* φ — *гомоморфизм группы* G *с ядром* H, *то* $G^\varphi \simeq G/H$. *Более того, гомоморфизм* φ *равносилен последовательному выполнению естественного гомоморфизма* ε: $G \to G/H$, *а затем некоторого изоморфизма* τ: $G/H \to G^\varphi$.

Д о к а з а т е л ь с т в о. Установим отображение τ: $G/H \to G^\varphi$, полагая

$$(xH)^\tau = x^\varphi \text{ для } x \in G.$$

Это действительно отображение, так как из $xH = yH$ следует $x^\varphi = y^\varphi$. Отображение τ переводит разные элементы в разные, так как из $x^\varphi = y^\varphi$ следует $x^{-1}y \in H$. Далее, τ — отображение *на*, что очевидно. Наконец, τ сохраняет умножение, так как

$$(XH \cdot yH)^\tau = (xyH)^\tau = (xy)^\varphi = x^\varphi y^\varphi = (xH)^\tau (yH)^\tau.$$

Следовательно, τ — изоморфизм G/H на G^φ. Теперь ясно, что $\varphi = \varepsilon\tau$. Теорема доказана.

Для иллюстрации применим эту теорему к примерам 4.1.1. Вычисляя ядра указанных там гомоморфизмов, по-

лучаем следующие формулы:

$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n, \tag{1}$$

$$\mathbb{Q}_p/\mathbb{Z} \simeq \mathbb{C}_{p^\infty}, \tag{2}$$

$$\boldsymbol{S}_p/\boldsymbol{A}_n \simeq \mathbb{Z}^* \simeq \mathbb{Z}_2, \tag{3}$$

$$\boldsymbol{GL}_n(K)/\boldsymbol{SL}_n(K) \simeq K^*, \tag{4}$$

$$\boldsymbol{T}_n(K)/\boldsymbol{UT}_n(K) \simeq \boldsymbol{D}_n(K) \simeq \underbrace{K^* \times \ldots \times K^*}_{n \text{ раз}}, \tag{5}$$

$$\boldsymbol{UT}_n^m(K)/\boldsymbol{UT}_n^{m+1}(K) \simeq \underbrace{K \oplus \ldots \oplus K}_{n-m \text{ раз}}. \tag{6}$$

С помощью теоремы 4.2.2 продолжим изучение отображения ψ: $L(G, H) \to L(G/H, 1)$ из теоремы 4.2.1 и покажем, что нормальные подгруппы, соответствующие друг другу, определяют изоморфные фактор-группы.

4.2.3. Теорема. *Если* $H \trianglelefteqslant G$, $A \trianglelefteqslant G$ *и* $H \leqslant A$, *то*

$$(G/H)/(A/H) \simeq G/A.$$

Доказательство. Установим отображение φ: $G/H \to G/A$, полагая

$$(xH)^\varphi = xA \text{ для } x \in G.$$

Это действительно отображение, так как из $xH = yH$ следует $x^{-1}y \in H \leqslant A$, $xA = yA$. Далее, φ — отображение *на*, что очевидно. Наконец, φ сохраняет умножение, так как

$$(xH \cdot yH)^\varphi = (xyH)^\varphi = xyA = xA \cdot yA.$$

Таким образом, φ — гомоморфизм G/H на G/A. Очевидно, $\operatorname{Ker}\varphi = A/H$, поэтому $A/H \trianglelefteqslant G/H$, а изоморфизм вытекает из теоремы 4.2.2.

4.2.4. Теорема. *Если* $A \trianglelefteqslant B \leqslant G$, $H \trianglelefteqslant G$, *то*

$$BH/AH \simeq B/A\,(B \cap H).$$

В частности,

$$BH/H \simeq B/B \cap H.$$

Доказательство. Очевидно, что $AH \trianglelefteqslant BH$ и сужение на подгруппу B естественного гомоморфизма $BH \to BH/AH$ имеет ядро $B \cap AH$ и образ BH/AH. По теореме 4.2.2, примененной к этому сужению, $BH/AH \simeq B/B \cap AH$. Остается учесть очевидное равенство $B \cap AH = A\,(B \cap H)$. Теорема доказана.

4.2.5. Упражнение. Если $G = A \times B$, то $G/A \simeq B$.

4.2.6. Упражнение. Пусть H — подгруппа группы $\mathbb{C}^*$, состоящая из всех комплексных чисел с модулем 1, $\mathbb{R}^{**}$ — мультипликативная группа положительных действительных чисел. Тогда $\mathbb{C}^*/H \simeq \mathbb{R}^{**}$.

Несомненно, понятия группы, подгруппы, нормальной подгруппы, гомоморфизма и фактор-группы читатель знал из общего курса алгебры, но в книге под названием «Основы теории групп» уместно было напомнить их. Аналогичные понятия подкольца, идеала, кольцевого гомоморфизма и фактор-кольца напоминать, видимо, излишне. Интересная связь между теми и другими понятиями возникает при рассмотрении групп матриц над кольцами.

4.2.7. Упражнение. Пусть K — ассоциативное кольцо с единицей, G — группа матриц степени n над K. Если $\mathfrak{a}$ — идеал в K, то

$$G_{\mathfrak{a}} = \{e + a \mid e + a \in G,\ a_{ij} \in \mathfrak{a}\}$$

— нормальная подгруппа в G. Она называется *главной конгруэнц-подгруппой* по модулю $\mathfrak{a}$, а ее надгруппы — *конгруэнц-подгруппами* группы G. Всякий кольцевой гомоморфизм $\varphi\colon K \to K'$ индуцирует групповой гомоморфизм $\varphi_G\colon G \to G'$ по правилу

$$(g_{ij})^{\varphi_G} = (g_{ij}^{\varphi}),\ g \in G.$$

Его ядро $\operatorname{Ker}\varphi_G = G_{\operatorname{Ker}\varphi}$. Например, гомоморфизм $\mathbb{Z} \to \mathbb{Z}_m$ индуцирует гомоморфизм $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}_m)$, ядро которого ($m$-я главная конгруэнц-подгруппа) обозначается $\Gamma_n(m)$. Каждое $\Gamma_n(m)$ имеет конечный индекс в $SL_n(\mathbb{Z})$. Вообще, кольцевой гомоморфизм $K \to K/\mathfrak{a}$ индуцирует групповые гомоморфизмы $GL_n(K) \to GL_n(K/\mathfrak{a})$, $SL_n(K) \to SL_n(K/\mathfrak{a})$ и т. д.; их ядра — главные конгруэнц-подгруппы по модулю $\mathfrak{a}$ — обозначаются соответственно $GL_n(K, \mathfrak{a})$, $SL_n(K, \mathfrak{a})$ и т. д. В частности, $\Gamma_n(m) = SL_n(\mathbb{Z}, m\mathbb{Z})$.

В связи с последним упражнением возникает важная *конгруэнц-проблема* для матричной группы G: всякая ли подгруппа конечного индекса в G содержит G_I по некоторому идеалу I конечного индекса? Один из самых ранних примеров положительного решения конгруэнц-проблемы будет изложен на стр. 207. Отметим еще, что Меннике

(Mennicke J. L.— Ann. Math., 1965, 81, № 1, p. 31—37) и независимо Басс, Лазар и Серр (Bass H., Lazard M., Serre J.-P.— Bull. Amer. Math. Soc., 1964, 70, № 3, p. 385—392) положительно решили конгруэнц-проблему для группы $\boldsymbol{SL}_n(\mathbb{Z})$, $n \geqslant 3$ (для $n = 2$ давно было известно отрицательное решение). Работа Меннике доступна студенту второго курса.

4.2.8. Упражнение. Пусть p — простое число, m, n — натуральные числа, $m \geqslant 2$. Рассмотрим в группе $\boldsymbol{GL}_n(\mathbb{Z}_{p^m})$ главные конгруэнц-подгруппы

$$P_k = \boldsymbol{GL}_n(\mathbb{Z}_{p^m},\ p^k\mathbb{Z}_{p^m}),$$

т. е.

$$P_k = \{e + p^k a \mid a \in \boldsymbol{M}_n(\mathbb{Z}_{p^m})\}, \qquad k = 1, 2, \ldots$$

Доказать, что отображение φ_k: $P_k \to P_{m-1}$, определяемое правилом

$$e + p^k a \mapsto e + p^{m-1}a, \qquad a \in \boldsymbol{M}_n(\mathbb{Z}_{p^m}),$$

является гомоморфизмом *на* с ядром P_{k+1}. Этот гомоморфизм совпадает с возведением матриц в p^{m-k-1}-ю степень, за исключением случая, когда $p = 2$, $k = 1$.

4.3. Поддекартовы произведения. Напомним, что прямое произведение

$$G = \prod_{i \in I} G_i \tag{7}$$

состоит из функций f: $I \to \bigcup\limits_{i \in I} G_i$ с условиями:

1) $f(i) \in G_i$ для всех $i \in I$,
2) $|\operatorname{supp}(f)| < \infty$.

Легко проверить, что подмножество

$$G_i' = \{f \mid f \in G,\ f(j) = e \text{ при } j \neq i\}$$

является нормальной подгруппой в G, причем она изоморфна множителю G_i в силу отображения $f \mapsto f(i)$. Часто G_i' отождествляют с G_i в силу этого изоморфизма. При таком отождествлении $G_i \trianglelefteqslant G$, группа G порождается подгруппами G_i и каждый элемент g из G допускает запись

$$g = g_{i_1} \cdots g_{i_m},\ g_i \in G_i, \tag{8}$$

где все значки $i_1, \ldots, i_m$ различны, а неединичные множители однозначно определяются элементом g.

Это замечание позволяет дать внутреннее определение прямого произведения — в отличие от внешнего определения гл. 1.

Пусть группа G порождается своими нормальными подгруппами G_i, причем каждый элемент g из G допускает запись (8), где все значки $i_1, \ldots, i_m$ различны, а неединичные множители однозначно определяются элементом g. Тогда говорят, что *группа G разлагается в прямое произведение подгрупп G_i*. Очевидно, группа G тогда и только тогда разлагается в прямое произведение своих подгрупп G_i, когда она изоморфна прямому произведению абстрактных групп G_i. Поэтому для группы G, разложимой в прямое произведение подгрупп G_i, используется та же запись (7), что и для прямого произведения абстрактных групп G_i. При аддитивной записи операции говорят о разложении в прямую сумму и пишут

$$G = G_1 \oplus \ldots \oplus G_m, \qquad G = \sum_{i \in I} G_i.$$

4.3.1. Примеры. I. Аддитивная группа поля $\mathbb{C}$ разлагается в прямую сумму подгруппы действительных и подгруппы чисто мнимых чисел: $\mathbb{C} = \mathbb{R} \oplus i\mathbb{R}$.

II. Очевидно,

$$\mathbb{Q}^* = (-1) \times \prod_p (p).$$

III. Четверная группа Клейна разлагается в прямое произведение двух подгрупп второго порядка:

$$\{1,\ (12)(34),\ (13)(24),\ (14)(23)\} = ((12)(34)) \times ((13)(24)).$$

IV. Очевидно,

$$D_n(K) = G_1 \times \ldots \times G_n,$$

где G_i — подгруппа из $D_n(K)$, у матриц которой на всех диагональных местах, кроме i-го, стоит 1.

4.3.2. Упражнение. Группа G тогда и только тогда разлагается в прямое произведение своих нормальных подгрупп G_i, когда она порождается ими и из любого соотношения $g_{i_1} \ldots g_{i_m} = e$, где $g_i \in G_i$ и все значки различны, вытекают соотношения $g_{i_1} = \ldots = g_{i_m} = e$.

4.3.3. Упражнение. Группа G тогда и только тогда разлагается в прямое произведение нормальных подгрупп G_i, когда она порождается ими и

$$G_i \cap \text{гр}\,(G_j \mid j \neq i) = 1 \text{ для всех } i.$$

4.3.4. Упражнение. Циклическая группа порядка mn, где m и n взаимно просты, разлагается в прямое произведение подгрупп порядков m, n.

4.3.5. Упражнение. Пусть p — простое число. Циклическая группа порядка p^n неразложима в прямое произведение собственных подгрупп.

4.3.6. Упражнение. Аддитивная группа поля $\mathbb{Q}$ неразложима в прямую сумму собственных подгрупп.

Подгруппа A прямого произведения (7) называется *подпрямым произведением* групп G_i, если проекция A на каждый множитель G_i совпадает с G_i. Подчеркнем, что подпрямое произведение не определяется множителями однозначно. Очевидно, каждая подгруппа прямого произведения есть подпрямое произведение своих проекций. Это не всегда будет прямое произведение — контрпримером служит диагональ D прямого квадрата $G \times G$, состоящая из пар $\langle g, g\rangle$, $g \in G$.

4.3.7. Упражнение. Пусть $G = G_1 \times G_2$, A — подгруппа из G, A_i — ее проекция на множитель G_i, $i = 1, 2$. Доказать, что A разлагается в прямое произведение $A_1 \times A_2$ тогда и только тогда, когда $A_i = G_i \cap A$, $i = 1, 2$.

4.3.8. Упражнение. Пусть $G = G_1 \times G_2$, где G_1, G_2 — конечные группы взаимно простых порядков. Всякая подгруппа $A \leqslant G$ разлагается в прямое произведение своих проекций на множители G_1, G_2.

Если G — подпрямое произведение конечных групп, то очевидно, что любое конечное множество элементов из G содержится в конечной нормальной подгруппе. Последнее свойство принято называть *локальной нормальностью*. Как показывает пример группы $\mathbb{C}_{p^\infty}$, класс локально нормальных групп шире класса подпрямых произведений конечных групп. Вместе с тем имеются тесные связи между этими классами (Hall P.— J. London Math. Soc., 1959, **34**, p. 289—304; Горчаков Ю. М.— Матем. сб., 1965, **67**, с. 244—254). С теорией локально нормальных групп и

вообще, групп с конечными классами сопряженных элементов можно познакомиться по книге Ю. М. Горчакова [8].

По аналогии с подпрямыми произведениями определяются поддекартовы произведения: подгруппа A декартова произведения

$$G = \overline{\prod_{i \in I}} G_i$$

называется *поддекартовым произведением* групп G_i, если проекция A на каждый множитель G_i совпадает с G_i. Очевидно, любое подпрямое произведение групп G_i будет и поддекартовым произведением этих групп.

4.3.9. Теорема (Ремак). *Пусть в группе G задано семейство нормальных подгрупп H_i, $i \in I$, и H — их пересечение. Тогда фактор-группа G/H изоморфна некоторому поддекартову произведению фактор-групп G/H_i.*

Доказательство. Рассмотрим отображение

$$\varphi\colon G \to \overline{\prod_{i \in I}} (G/H_i),$$

сопоставляющее каждому g из G функцию f, где $f(i) = gH_i$. Легко проверить, что φ — гомоморфизм, а H — его ядро. Теперь остается воспользоваться теоремой о гомоморфизмах 4.2.2.

4.3.10. Примеры. I. Группа $\mathbb{Q}/\mathbb{Z}$ изоморфна поддекартовой сумме групп $\mathbb{Q}/\mathbb{Q}_p$ по всем простым p.

II. Группа $\mathbb{C}^*$ изоморфна подпрямому произведению групп $\mathbb{C}^*/\mathbb{C}_{p^\infty}$ по любым двум различным простым числам p.

III. Пусть множество M разбито на непересекающиеся части M_i, $i \in I$. Пусть $G \leqslant S(M)$, причем каждый элемент из G отображает каждое M_i на себя. Тогда G изоморфна поддекартову произведению подгрупп из $S(M_i)$, $i \in I$.

IV. Группа $GL_n(\mathbb{Z})$ изоморфна подгруппе декартова произведения конечных групп $GL_n(\mathbb{Z}_m)$, $m = 1, 2, \ldots$.

4.3.11. Упражнение. Пересечение нормальных подгрупп, определяющих абелевы фактор-группы, само определяет абелеву фактор-группу.

4.4. Матрёшки. Пусть G — группа. Система вложенных друг в друга подгрупп группы G, содержащая единич-

ную подгруппу и всю G, называется *матрёшкой* группы G (другие термины: башня, ряд, цепь). До § 22 мы будем иметь дело исключительно с конечными матрёшками (кроме двух случаев в § 7 и § 13, когда встретятся «трансфинитно возрастающие матрёшки»), а потому термин «матрёшка» будет всегда обозначать конечную матрёшку — вплоть до § 22. Матрёшка

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G \tag{9}$$

называется *нормальной*, если каждая подгруппа G_i нормальна в G. Например, любая матрёшка подгруппы абелевой группы нормальна. Матрёшка (9) называется *субнормальной*, если выполнено более слабое условие: каждый предыдущий член — нормальная подгруппа следующего члена, т. е. $G_i \trianglelefteqslant G_{i+1}$ для $i = 0, 1, 2, \ldots, n-1$. Члены субнормальных матрёшек называются *субнормальными подгруппами* (если подгруппа H субнормальна в G, то пишут $H \lhd\lhd G$. Факторгруппы G_{i+1}/G_i называются *секциями* матрёшки (9). Вообще, *секцией* группы G называется всякая факторгруппа B/A, где A, B — подгруппы из G, причем $A \trianglelefteqslant B$. Иногда матрёшки записываются не по возрастанию от 1 до G, а по убыванию от G до 1. Найдя в группе субнормальную матрёшку, секции которой хорошо изучены, мы тем самым продвигаемся и в изучении самой группы.

Говорят, что группа G является *расширением* группы A посредством группы B, если в G существует такая нормальная подгруппа H, что $H \simeq A$, $G/H \simeq B$. В этом смысле секции субнормальной матрёшки — это те строительные блоки, из которых путем последовательных расширений можно собрать всю группу. Подчеркнем, однако, что результат не определяется только использованными секциями, а зависит еще от способа их сборки — например, расширение $\mathbb{Z}_2$ посредством $\mathbb{Z}_2$ может быть группой $\mathbb{Z}_2 \times \mathbb{Z}_2$ и группой $\mathbb{Z}_4$. Группы, собранные из циклических секций, называют полициклическими. Точнее, субнормальная матрёшка с циклическими секциями называется *полициклической*, а группа с такой матрёшкой — *полициклической группой*.

4.4.1. Примеры. I. Секции матрёшки $1 < (2) < \mathbb{Z} < \mathbb{Q}_p$ изоморфны соответственно группам $\mathbb{Z}$, $\mathbb{Z}_2$, $\mathbb{C}_{p^\infty}$

II. Все секции матрёшки $1 < C_p < C_{p^2} < \ldots < C_{p^n}$ — циклические порядка p.

III. Группа A_4 обладает полициклической матрёшкой

$$1 < \{1, (12)(34)\} < \{1, (12)(34), (13)(24), (14)(23)\} < A_4 \quad (10)$$

с секциями порядков 2, 2, 3. Эта матрёшка не является нормальной, поскольку подгруппа ((12)(34)) не нормальна в A_4, хотя и субнормальна.

IV. Группа $T_n(K)$ обладает нормальной матрёшкой

$$T_n(K) \geqslant UT_n^1(K) \geqslant UT_n^2(K) \geqslant \ldots \geqslant UT_n^n(K) = 1 \quad (11)$$

с секциями $S_0, S_1, \ldots, S_{n-1}$, где

$$S_0 \simeq K^* \times \ldots \times K^* \quad (n \text{ раз}),$$
$$S_m \simeq K \oplus \ldots \oplus K \quad (n - m \text{ раз}) \text{ при } m \geqslant 1.$$

(Суб)нормальная матрёшка группы индуцирует (суб)нормальные матрёшки в подгруппах и фактор-группах:

4.4.2. Т е о р е м а. *Пусть G — группа с (суб)нормальной матрёшкой* (9). *Если $H \leqslant G$, то, пересекая матрёшку* (9) *с H, мы получим (суб)нормальную матрёшку в H:*

$$1 = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_n = H, \quad H_i = G_i \cap H,$$

причем секция H_{i+1}/H_i будет изоморфна подгруппе секции G_{i+1}/G_i. Если $H \trianglelefteqslant G$, то, беря образы членов матрёшки (9) *при естественном гомоморфизме $G \to G/H$, мы получим (суб)нормальную матрёшку в G/H:*

$$1 = \overline{G}_0 \leqslant \overline{G}_1 \leqslant \ldots \leqslant \overline{G}_n = G/H, \quad \overline{G}_i = G_iH/H,$$

причем секция $\overline{G}_{i+1}/\overline{G}_i$ будет гомоморфным образом секции G_{i+1}/G_i.

Д о к а з а т е л ь с т в о. Соотношения $H_i \trianglelefteqslant H_{i+1}$, $\overline{G}_i \trianglelefteqslant \overline{G}_{i+1}$, а в случае нормальных матрёшек соотношения $H_i \trianglelefteqslant H$, $\overline{G}_i \trianglelefteqslant \overline{G}$, проверяются непосредственно. Далее, используя теоремы о гомоморфизмах, получаем:

$$H_{i+1}/H_i = H_{i+1}/H_{i+1} \cap G_i \simeq H_{i+1}G_i/G_i \leqslant G_{i+1}/G_i,$$
$$\overline{G}_{i+1}/\overline{G}_i \simeq G_{i+1}H/G_iH \simeq G_{i+1}/G_i(G_{i+1} \cap H) \simeq (G_{i+1}/G_i)/(\ldots).$$

Теорема доказана.

4.4.3. У п р а ж н е н и е. Подгруппы и фактор-группы полициклической группы — полициклические. Рас-

ширение полициклической группы посредством полициклической группы — снова полициклическая группа. Произведение двух полициклических нормальных подгрупп произвольной группы — полициклическая подгруппа.

Две субнормальные матрёшки данной группы называются *изоморфными*, если они имеют одинаковое число секций и между их секциями существует такое взаимно однозначное соответствие, при котором соответственные секции изоморфны. Например, в группе $\mathbb{C}_{12}$ матрёшки

$$1 < \mathbb{C}_2 < \mathbb{C}_4 < \mathbb{C}_{12}$$

и

$$1 < \mathbb{C}_3 < \mathbb{C}_6 < \mathbb{C}_{12}$$

изоморфны. Если одна матрёшка содержит все члены другой, то первая называется *уплотнением* второй.

4.4.4. Теорема (Шрайер). *Во всякой группе всякие две (суб)нормальные матрёшки обладают изоморфными (суб)нормальными уплотнениями.*

Доказательство. Пусть в группе G заданы две (суб)нормальные матрёшки

$$1 = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_m = G, \tag{12}$$

$$1 = B_0 \leqslant B_1 \leqslant \ldots \leqslant B_n = G. \tag{13}$$

Мы уплотним каждый промежуток $A_i \leqslant A_{i+1}$ первой матрёшки вставкой, приготовленной при помощи второй матрёшки, и наоборот. Вставка в промежуток $A_i \leqslant A_{i+1}$ изготовляется так: пересекаем матрёшку (13) с A_{i+1}, а затем почленно умножаем на A_i; получилась цепочка подгрупп с началом A_i и концом A_{i+1} — вставка готова. Она имеет вид

$$A_i = C_{i0} \leqslant C_{i1} \leqslant \ldots \leqslant C_{in} = A_{i+1},$$
$$C_{ij} = (A_{i+1} \cap B_j)A_i.$$

Аналогично изготовляются вставки для второй матрёшки:

$$B_j = D_{j0} \leqslant D_{j1} \leqslant \ldots \leqslant D_{jm} = B_{j+1},$$
$$D_{ji} = (B_{j+1} \cap A_i)B_j.$$

Очевидно, если члены матрёшек (12), (13) были нормальны в G, то и все члены вставок такие же. Остается проверить, что

$$C_{i,j+1}/C_{ij} \simeq D_{j,i+1}/D_{ji}.$$

Но по теореме 4.2.4

$$C_{i,j+1}/C_{ij} = (A_{i+1} \cap B_{j+1})A_i/(A_{i+1} \cap B_j)A_i \simeq$$
$$\simeq (A_{i+1} \cap B_{j+1})/(A_{i+1} \cap B_j)(A_i \cap B_{j+1}),$$
$$D_{j,i+1}/D_{ji} = (B_{j+1} \cap A_{i+1})B_j/(B_{j+1} \cap A_i)B_j \simeq$$
$$\simeq (B_{j+1} \cap A_{i+1})/(B_{j+1} \cap A_i)(B_j \cap A_{i+1}).$$

Теорема доказана.

Из этой теоремы вытекает, в частности, что *во всякой группе всякие две (суб)нормальные матрёшки без повторяющихся членов, не уплотняемые без повторения членов, изоморфны* (теорема Жордана — Гёльдера).

4.4.5. У п р а ж н е н и е. Пусть G — полициклическая группа. Число бесконечных секций в любой ее полициклической матрёшке одно и то же. Оно называется *полициклической размерностью* группы G. По этому числу удобно вести индукцию при изучении полициклических групп.

Отметим, что теоремы 4.4.2 и 4.4.4 без каких-либо изменений в доказательствах переносятся на с ч ё т н ы е матрёшки вида

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \ldots \trianglelefteq G_n \trianglelefteq \ldots, \qquad G = \bigcup_{n=1}^{\infty} G_n,$$

а также на некоторые более сложные типы «бесконечных субнормальных матрёшек», но, как уже упоминалось выше, мы отложим эту тему до § 22.

В заключение пункта отметим тесно связанное с гомоморфизмами понятие аппроксимируемости. В наиболее общей форме это понятие определяется следующим образом (Каргаполов М. И., Мерзляков Ю. И. Бесконечные группы.— В сб.: Итоги науки. Алгебра. Топология. Геометрия. 1966.— М., 1968, с. 75; мы говорим о группах, хотя можно было бы говорить о произвольных алгебраических системах — см. п. 27.1 Дополнения).

Пусть G — группа, ρ — отношение (или, иначе, предикат) между элементами и множествами элементов, определенное на G и всех ее гомоморфных образах (например, бинарное отношение равенства элементов, бинарное отношение «элемент x входит в подгруппу y», бинарное отношение сопряженности элементов и т. п.). Пусть K — класс групп. Будем говорить, что группа G *аппроксимируется*

группами из K относительно ρ, если для всяких элементов и множеств элементов из G, не находящихся в отношении ρ, существует такой гомоморфизм группы G на группу из класса K, при котором образы этих элементов тоже не находятся в отношении ρ. В литературе чаще всего встречается аппроксимируемость относительно равенства элементов, в этом случае упоминание об отношении обычно опускают и говорят просто об аппроксимируемости. Как вытекает из теоремы Ремака 4.3.9, группа G тогда и только тогда аппроксимируется группами класса K, когда она вкладывается в декартово произведение групп из K.

Аппроксимируемость конечными группами называют также *финитной аппроксимируемостью*. Финитную аппроксимируемость относительно предиката ρ удобно обозначать ФАρ; в частности, если ρ пробегает предикаты равенства, сопряженности, вхождения в подгруппу, вхождения в конечно порожденную подгруппу, вхождения в данную подгруппу H и т. п., то получаются свойства (и классы) ФАР, ФАС, ФАВ, ФАВ$_\omega$, ФАВ-H и т. п. На важную роль этих свойств указал А. И. Мальцев (Уч. зап. Ивановского пед. ин-та, 1958, **18**, с. 49—60): из их наличия в группе вытекает разрешимость соответствующей алгоритмической проблемы.

§ 5. Эндоморфизмы. Автоморфизмы

5.1. Определения. Гомоморфное отображение группы в себя называется ее *эндоморфизмом*, а изоморфное отображение группы на себя называется ее *автоморфизмом*. Эндоморфный образ подобен удостоверению личности в кармане этой личности. Множества всех эндоморфизмов и автоморфизмов данной группы G обозначаются соответственно через End G и Aut G. На этих множествах определяют умножение, считая произведением двух эндоморфизмов их последовательное выполнение. Легко проверить, что тогда End G становится полугруппой, а Aut G даже группой, причем

$$\mathrm{Aut}\, G \leqslant \mathcal{S}(G).$$

Если группа G абелева, то на End G определяют еще

сложение, полагая

$$x^{\varphi+\psi} = x^{\varphi}x^{\psi} \text{ для } \varphi,\ \psi \in \operatorname{End} G,\ x \in G.$$

Непосредственно проверяется, что тогда End G становится кольцом. В общем случае кольца не получается, и End играет в теории групп меньшую роль, чем Aut.

В гл. 1 мы уже отмечали, что сопряжение группы G некоторым элементом a из G является изоморфизмом, так как оно взаимно однозначно и

$$(xy)^a = x^a y^a \text{ для } x,\ y \in G.$$

Этот автоморфизм $\hat{a}$ называется *внутренним автоморфизмом* группы G, производимым элементом a. Непосредственно проверяется, что

$$(x^a)^b = x^{ab},\ (x^a)^{a^{-1}} = x, \quad x^{\varphi^{-1}\hat{a}\varphi} = x^{\widehat{a^{\varphi}}},$$
$$a,\ b,\ x \in G,\ \varphi \in \operatorname{Aut} G,$$

поэтому

$$\hat{a}\hat{b} = \widehat{ab},\ \hat{a}^{-1} = \widehat{a^{-1}},\ \varphi^{-1}\hat{a}\varphi = \widehat{a^{\varphi}}. \tag{1}$$

Отсюда вытекает, в частности, что множество Int G всех внутренних автоморфизмов группы G является нормальной подгруппой группы Aut G,

$$\operatorname{Int} G \trianglelefteq \operatorname{Aut} G. \tag{2}$$

Автоморфизмы, не являющиеся внутренними, называют *внешними*, а группу

$$\operatorname{Out} G = \operatorname{Aut} G/\operatorname{Int} G \tag{3}$$

называют *группой внешних автоморфизмов*. Очевидно, для абелевой группы Out совпадает с Aut.

Первое из соотношений (1) показывает, что отображение $G \to \operatorname{Int} G$, сопоставляющее каждому g из G внутренний автоморфизм $\hat{g}$, является гомоморфным. Ядро этого гомоморфизма состоит из элементов g с условием

$$x^g = x,\ x \in G,$$

т. е. совпадает с центром Z (G) группы G. Применяя теорему о гомоморфизмах, получаем формулу

$$\operatorname{Int} G \simeq G/\mathrm{Z}(G). \tag{4}$$

В качестве иллюстрации опишем кольца End G и группы Aut G для некоторых групп G из примеров I—IV гл. 1. При этом мы используем очевидную формулу

$$(\mathrm{End}\ G)^* = \mathrm{Aut}\ G.$$

5.1.1. Примеры. I. Имеем:

$$\mathrm{End}\ \mathbb{Z} \simeq \mathbb{Z}, \quad \mathrm{Aut}\ \mathbb{Z} \simeq \mathbb{Z}^* \simeq \mathbb{Z}_2, \tag{5}$$

$$\mathrm{End}\ \mathbb{Z}_m \simeq \mathbb{Z}_m, \quad \mathrm{Aut}\ \mathbb{Z}_m \simeq \mathbb{Z}_m^*, \tag{6}$$

$$\mathrm{End}\ \mathbb{Q} \simeq \mathbb{Q}, \quad \mathrm{Aut}\ \mathbb{Q} \simeq \mathbb{Q}^*. \tag{7}$$

Действительно, изоморфизмы для End даются соответственно следующими формулами (ввиду аддитивной записи групповой операции мы пишем эндоморфизм φ не как показатель степени, а как множитель):

$$\varphi \mapsto 1\varphi, \quad \varphi \mapsto (1(\mathrm{mod}\ m))\varphi, \quad \varphi \mapsto 1\varphi.$$

Рассмотрим подробно только последний случай. Гомоморфность отображения $\varphi \mapsto 1\varphi$ проверяется непосредственно. Покажем, что ядро тривиально, т. е. из $1\varphi = 0$ следует $\varphi = 0$. Пусть r, s — целые числа, $s \neq 0$. Так как

$$0 = 1\varphi = \left(s \cdot \frac{1}{s}\right)\varphi = s\left(\frac{1}{s}\right)\varphi,$$

то

$$\left(\frac{1}{s}\right)\varphi = 0, \quad \left(\frac{r}{s}\right)\varphi = 0, \quad r\varphi = 0.$$

Наконец, для всякого $\alpha \in \mathbb{Q}$ найдется прообраз $\varphi \in \mathrm{End}\ \mathbb{Q}$, а именно, эндоморфизм $x \mapsto x\alpha$ группы $\mathbb{Q}$.

II. Опишем кольцо End $\mathbb{C}_{p^\infty}$. Пусть ε_n — первообразный корень из 1 степени p^n в поле комплексных чисел, причем $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ Очевидно, эндоморфизмы группы $\mathbb{C}_{p^\infty}$ полностью определяются своим действием на $\varepsilon_1, \varepsilon_2, \ldots$ Пусть $\varphi \in \mathrm{End}\ \mathbb{C}_{p^\infty}$, тогда

$$\varepsilon_n^\varphi = \varepsilon_n^{k_n}, \quad k_n \in \mathbb{Z}_{p^n}, \quad n = 1, 2, \ldots$$

Так как $(\varepsilon_{n+1}^\varphi)^p = \varepsilon_n^\varphi$, то k_n — образ k_{n+1} при гомоморфизме $\mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$ (по правилу: $x \pmod{p^{n+1}} \mapsto x \pmod{p^n}$ для $x \in \mathbb{Z}$). Таким образом, каждому φ из End $\mathbb{C}_{p^\infty}$ отвечает последовательность $(k_1, k_2, \ldots)$, $k_n \in \mathbb{Z}_{p^n}$, с условием, что k_n — образ k_{n+1} при канониче-

ском гомоморфизме $\mathbb{Z}_{p^{n+1}} \to \mathbb{Z}_{p^n}$. Непосредственно проверяется, что множество $\mathbb{Z}_{p^\infty}$ всех таких последовательностей является кольцом относительно покомпонентного сложения и покомпонентного умножения, а возникшее у нас отображение $\mathrm{End}\, \mathbb{C}_{p^\infty} \to \mathbb{Z}_{p^\infty}$ является изоморфизмом *на*. Это дает искомое описание кольца $\mathrm{End}\, \mathbb{C}_{p^\infty}$. Кольцо $\mathbb{Z}_{p^\infty}$ называется *кольцом целых p-адических чисел*, его элементы естественным образом записываются в виде

$$\ldots a_n \ldots a_1 a_0 = \sum_{n=0}^{\infty} a_n p^n, \quad 0 \leqslant a_n < p,$$

и естественно складываются и умножаются: «вычет пишем, число периодов в уме». Приведем для иллюстрации образцы действий над целыми 5-адическими числами:

$$\begin{array}{r} \ldots 20134 \\ +\ \ldots 12203 \\ \hline \ldots 32342 \end{array} \qquad \begin{array}{r} \ldots 20134 \\ \times\ \ldots 12203 \\ \hline \ldots 11012 \\ \ldots 0000 \\ \ldots 323 \\ +\ \ldots 23 \\ \ldots 4 \\ \ldots \\ \hline \ldots 11312 \end{array} \qquad \begin{array}{r} \ldots 20134 \\ -\ \ldots 12203 \\ \hline \ldots 02431 \end{array}$$

Отметим попутно, что множество $\mathbb{Q}_{p^\infty}$ «дробных» p-адических чисел вида

$$\ldots a_n \ldots a_1 a_0,\ a_{-1} \ldots a_{-s} = \sum_{n=-s}^{\infty} a_n p^n, \quad 0 \leqslant a_n < p,$$

оказывается уже полем относительно аналогичных операций и называется *полем p-адических чисел*. Читатель сам сформулирует правило деления углом для p-адических чисел (только при делении и нужна простота p). Итак,

$$\mathrm{End}\, \mathbb{C}_{p^\infty} \simeq \mathbb{Z}_{p^\infty}, \ \mathrm{Aut}\, \mathbb{C}_{p^\infty} \simeq \mathbb{Z}_{p^\infty}^*. \tag{8}$$

Легко сообразить, что $\mathbb{Z}_{p^\infty}^*$ состоит из тех целых p-адических чисел, у которых «свободный член» a_0 отличен от нуля.

III. Справедлива формула

$$\operatorname{Aut} \boldsymbol{S}_n \simeq \boldsymbol{S}_n \quad \text{при } n \neq 2,\ 6. \tag{9}$$

Мы докажем ее в конце параграфа. При $n = 2, 6$ эта формула неверна — см. там же.

IV. Описанию автоморфизмов классических матричных групп посвящена обширная литература — см., например, [1, 9]. Приведем без доказательства типичный результат. Пусть $n \geqslant 3$, K — поле характеристики $\neq 2$. Тогда для каждого автоморфизма φ из $\operatorname{Aut} \boldsymbol{GL}_n(K)$ либо

$$x^{\varphi} = x^{\psi} \cdot g^{-1} x^{\sigma} g, \qquad x \in \boldsymbol{GL}_n(K), \tag{10}$$

либо

$$x^{\varphi} = x^{\psi} \cdot g^{-1} \hat{x}^{\sigma} g, \qquad x \in \boldsymbol{GL}_n(K), \tag{11}$$

при подходящих $\sigma \in \operatorname{Aut} K$, $\psi\colon \boldsymbol{GL}_n(K) \to K^*$ и подходящем элементе $g \in \boldsymbol{GL}_n(K)$. Здесь $\hat{}$ обозначает взятие обратной матрицы к транспонированной. Для многих матричных групп, особенно над кольцами, группы автоморфизмов плохо изучены или совсем не изучены.

5.1.2. Упражнение. Если $|G| > 2$, то $\operatorname{Aut} G \neq 1$.

Указание: рассмотреть случаи, когда 1) G неабелева, 2) G абелева и содержит элементы порядка > 2, 3) G удовлетворяет тождественному соотношению $x^2 = e$.

5.1.3. Упражнение:

$$\operatorname{End}(\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}) \simeq \boldsymbol{M}_n(\mathbb{Z}),$$
$$\operatorname{Aut}(\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}) \simeq \boldsymbol{GL}_n(\mathbb{Z}),$$
$$\operatorname{End}(\mathbb{Z}_m \oplus \ldots \oplus \mathbb{Z}_m) \simeq \boldsymbol{M}_n(\mathbb{Z}_m),$$
$$\operatorname{Aut}(\mathbb{Z}_m \oplus \ldots \oplus \mathbb{Z}_m) \simeq \boldsymbol{GL}_n(\mathbb{Z}_m),$$
$$\operatorname{End}(\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}) \simeq \boldsymbol{M}_n(\mathbb{Q}),$$
$$\operatorname{Aut}(\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}) \simeq \boldsymbol{GL}_n(\mathbb{Q})$$

(в левых частях n слагаемых).

5.1.4. Упражнение:

$$\operatorname{End}(\mathbb{C}_{p^\infty} \times \ldots \times \mathbb{C}_{p^\infty}) \simeq \boldsymbol{M}_n(\mathbb{Z}_{p^\infty}),$$
$$\operatorname{Aut}(\mathbb{C}_{p^\infty} \times \ldots \times \mathbb{C}_{p^\infty}) \simeq \boldsymbol{GL}_n(\mathbb{Z}_{p^\infty})$$

(в левых частях n множителей).

5.1.5. Упражнение. Все конгруэнц-подгруппы

$$\boldsymbol{GL}_n(\mathbb{Z}_{p^\infty},\ p^k \mathbb{Z}_{p^\infty}), \qquad k = 1, 2, \ldots,$$

группы $GL_n(\mathbb{Z}_{p^\infty})$ не имеют кручения, за исключением случая $p = 2$, $k = 1$.

Указание: рассмотреть формулу бинома

$$(e + p^k a)^m = e + \binom{m}{1} p^k a + \binom{m}{2} p^{2k} a^2 + \ldots + p^{mk} a^m.$$

5.1.6. Упражнение. Пусть A, B — абелевы группы. Множество $\mathrm{Hom}(A, B)$ всех гомоморфизмов из A в B является кольцом относительно поточечного сложения по правилу

$$a(\varphi + \psi) = a\varphi + a\psi, \quad a \in A,$$

и суперпозиции в качестве умножения:

$$a(\varphi\psi) = (a\varphi)\psi, \quad a \in A.$$

5.1.7. Упражнение. Учитывая, что порядки элементов группы не меняются при ее автоморфизмах, перечислить непосредственно автоморфизмы группы S_3 и убедиться, что все они внутренние.

5.2. Допустимые подгруппы. Язык автоморфизмов позволяет дать еще одно определение нормальных подгрупп: подгруппа H группы G тогда и только тогда нормальна, когда она выдерживает все внутренние автоморфизмы группы G, т. е.

$$H^\varphi \leqslant H \text{ для всех } \varphi \in \mathrm{Int}\, G.$$

Заменяя в этом условии $\mathrm{Int}\, G$ на произвольное множество Φ из $\mathrm{End}\, G$, приходят к более общему понятию: подгруппу H группы G называют *допустимой* относительно Φ (короче, Φ-*допустимой*) и пишут $H \overset{\Phi}{\leqslant} G$, если

$$H^\varphi \leqslant H \text{ для всех } \varphi \in \Phi.$$

Очевидно, единичная подгруппа и вся группа допустимы относительно любого Φ. Если группа не содержит других Φ-допустимых нормальных подгрупп, она называется Φ-*простой*. При $\varphi \in \Phi$ подмножества M, M^φ называются Φ-*сопряженными*. Отношение Φ-сопряженности используется только при $\Phi \leqslant \mathrm{Aut}\, G$, когда оно является эквивалентностью, в общей ситуации оно бесполезно. В наи-

более употребительных случаях, когда Ф совпадает с End G, Aut G, Int G, приставку Ф читают «эндоморфно», «автоморфно», «внутренне» и пишут

$$H \overset{e}{\leqslant} G,\ H \overset{a}{\leqslant} G,\ H \overset{i}{\leqslant} G.$$

Знак $\overset{i}{\leqslant}$ употребляют обычно в стилизованной форме $\trianglelefteqslant$, как мы и поступаем с самого начала. Отметим, что некоторые авторы дают Ф-понятиям особые названия согласно следующей таблице

	сопряженные	допустимые	простые
внутренне	сопряженные	нормальные	простые
автоморфно	равнотипные	характеристические	элементарные
эндоморфно	—	вполне характеристические	—

Мы пощадим читателя и будем использовать из этой таблицы только первую строчку, которая новых слов не содержит. Оставшиеся четыре названия — от пяти разных корней — можно не запоминать.

5.2.1. Упражнение. Пересечение и порождение любого множества Ф-допустимых подгрупп есть Ф-допустимая подгруппа.

5.2.2. Упражнение. Отношения $\overset{\bullet}{\leqslant}$, $\overset{a}{\leqslant}$ транзитивны (в отличие от отношения $\trianglelefteqslant$), т. е.

$$A \overset{e}{\leqslant} B,\ B \overset{e}{\leqslant} C \Rightarrow A \overset{e}{\leqslant} C,$$
$$A \overset{a}{\leqslant} B,\ B \overset{a}{\leqslant} C \Rightarrow A \overset{a}{\leqslant} C.$$

5.2.3. Упражнение. Автоморфно допустимая подгруппа нормальной подгруппы нормальна во всей группе, т. е.

$$A \overset{a}{\leqslant} B,\ B \trianglelefteqslant C \Rightarrow A \trianglelefteqslant C.$$

Очевидными примерами эндоморфно допустимых подгрупп произвольной группы G служат ее последовательные коммутанты, *n-я степень* $G^n = \text{гр}\ (x^n \mid x \in G)$ и *n-й слой*

$G_n = \text{гр}\,(x \mid x \in G,\ x^n = 1)$. Центр группы G всегда автоморфно допустим, так как из $ab = ba$, $a, b \in G$, $\varphi \in \in \operatorname{Aut} G$ следует $a^\varphi b^\varphi = b^\varphi a^\varphi$, причем при пробегании элементом a группы G элемент a^φ тоже пробегает всю группу G. Подчеркнем, что даже в конечной группе центр может не быть эндоморфно допустимым — см. ниже III.

Укажем примеры допустимых подгрупп в конкретных группах.

5.2.4. Примеры. I. В группах $\mathbb{Z}$, $\mathbb{Z}_n$ все подгруппы эндоморфно допустимы. Группа $\mathbb{Q}$ автоморфно проста (и тем более эндоморфно проста), так как любые два ее ненулевых элемента автоморфно сопряжены — см. описание $\operatorname{Aut}\mathbb{Q}$ выше.

II. Очевидно, что

$$\mathbb{C}_p \overset{e}{\leqslant} \mathbb{C}_{p^2} \overset{e}{\leqslant} \ldots,\ \mathbb{C}_{p^n} \overset{e}{\leqslant} \mathbb{C}_{p^\infty}.$$

III. Так как коммутант группы эндоморфно допустим в ней, то $A_n \overset{e}{\leqslant} S_n$. Пусть $n \geqslant 3$. Так как группа S_n не имеет центра, то в конечной группе $\mathbb{C}_2 \times S_n$ центром служит подгруппа $\mathbb{C}_2$. Она не является эндоморфно допустимой, так как не выдерживает эндоморфизма $(-1)^m x \mapsto \mapsto (12)^m$, $m = 0, 1$, $x \in S_n$.

IV. Пусть K — поле. Так как взаимный коммутант Ф-допустимых подгрупп есть Ф-допустимая подгруппа, то

$$SL_n(K) \overset{e}{\leqslant} GL_n(K),$$

$$T_n(K) \overset{e}{\geqslant} UT_n^i(K), \quad i = 1, 2, \ldots$$

5.2.5. Упражнение. Максимальные примарные подгруппы абелевой группы эндоморфно допустимы.

5.2.6. Упражнение. Подгруппа Фраттини произвольной группы автоморфно допустима. Поэтому в конечной простой группе она равна 1.

5.2.7. Упражнение. Группа $\mathbb{Q} \oplus \ldots \oplus \mathbb{Q}$ автоморфно проста.

5.2.8. Упражнение. Периодическая абелева группа тогда и только тогда автоморфно проста, когда она является *элементарной абелевой группой*, т. е. абелевой группой простого периода или, что равносильно, разла-

гается в прямую сумму некоторого множества изоморфных копий группы $\mathbb{Z}_p$ для некоторого простого числа p.

Иногда рассматривают более общую ситуацию: G — группа, V — произвольное множество с заданным отображением $V \to \operatorname{End} G$. Тогда V называется *множеством операторов* группы G и для $\Phi \subseteq V$ очевидным образом определяются все Ф-понятия. При $\Phi = V$ приставку Ф читают «операторно».

5.3. Совершенные группы. Группа называется *совершенной*, если она без центра и все ее автоморфизмы внутренние. Если группа G совершенна, то $Z(G) = 1$, $\operatorname{Out} G = 1$ и по (3), (4)'

$$\operatorname{Aut} G \simeq G,$$

т. е. изучение группы автоморфизмов заменяется изучением самой группы. Этим свойством совершенных групп и вызвано роскошное название, данное им на заре теории групп. В действительности совершенные группы не играют какой-либо особой роли в теории групп (точно так же, как совершенные числа в теории чисел). Цель этого пункта — указать классическую серию совершенных групп — симметрические группы.

5.3.1. Т е о р е м а (Гёльдер). *При $n \neq 2, 6$ симметрическая группа $\boldsymbol{S}_n$ совершенна.*

Д о к а з а т е л ь с т в о. а) Из § 3 мы уже знаем, что при $n \geqslant 3$ группа $\boldsymbol{S}_n$ имеет тривиальный центр. Остается доказать, что при $n \neq 6$ каждый автоморфизм γ группы $\boldsymbol{S}_n$ внутренний. Пусть B_k — множество всех произведений k независимых транспозиций из $\boldsymbol{S}_n$, $1 \leqslant k \leqslant \frac{n}{2}$. Согласно 2.5.7.III две подстановки из $\boldsymbol{S}_n$ сопряжены в $\boldsymbol{S}_n$ тогда и только тогда, когда в разложении на независимые циклы они имеют одинаковое число циклов каждой длины. В частности, $B_1 \cup B_2 \cup \ldots$ — разбиение множества всех элементов порядка 2 из $\boldsymbol{S}_n$ на классы сопряженных элементов и каждое B_k переходит при внутренних автоморфизмах группы $\boldsymbol{S}_n$ в себя. Это подсказывает нам следующий путь: сначала докажем, что γ переводит B_1 в себя, а уже затем, что γ — внутренний автоморфизм.

б) Автоморфизм γ переводит B_1 в себя. Действительно, всякий автоморфизм группы сохраняет порядки элементов, а классы сопряженных элементов переводит в классы

сопряженных элементов, поэтому $B_1^\gamma = B_k$ при некотором k. Мы получим равенство $B_1^\gamma = B_1$ из самых грубых соображений: проверим, что $|B_k| \neq |B_1|$, если $k \neq 1$, $n \neq 6$.

Действительно, S_n содержит $\binom{n}{2}$ транспозиций, поэтому имеется $\prod_{i=0}^{k-1}\binom{n-2i}{2}$ множеств из k независимых транспозиций. Так как порядок множителей в произведении независимых транспозиций несуществен, то

$$|B_k'| = \frac{1}{k!}\prod_{i=0}^{k-1}\binom{n-2i}{2} = \frac{1}{k!2^k}\,n(n-1)\ldots(n-2k+1).$$

Теперь равенство $|B_1| = |B_k|$ сводится к следующему:

$$(n-2)(n-3)\ldots(n-2k+1) = k!2^{k-1}. \qquad (12)$$

Докажем, что при $n \neq 6$, $k \neq 1$ это невозможно. В самом деле, так как правая часть (12) положительна, то должно быть $n \geqslant 2k$. Отсюда левая часть удовлетворяет неравенству:

$$\text{л. ч. } (12) \geqslant (2k-2)!$$

Индукцией легко получаем, что

$$(2k-2)! > k!2^{k-1} \text{ при } k \geqslant 4.$$

Остается рассмотреть случаи $k = 2, 3$. При $k = 2$ легко проверяется, что равенство (12) невозможно ни для каких n. Пусть $k = 3$. Так как $n \geqslant 2k$, $n \neq 6$, то $n > 6$ и

$$\text{л. ч. } (12) \geqslant 5\cdot4\cdot3\cdot2 > 3!2^2 = \text{пр. ч. } (12).$$

Итак, равенство (12) невозможно, если $n \neq 6$, $k \neq 1$.

в) Автоморфизм γ внутренний. В самом деле, пусть $T(i)$ — множество всех транспозиций символа i с другими символами. Покажем, что $T(i)^\gamma = T(j)$ при некотором j. Так как всякие две транспозиции из $T(i)$ не перестановочны, то их образы относительно γ также должны содержать общий перемещаемый символ. При этом тройка (ia), (ib), (ic) не может перейти в тройку (ju), (jv), (uv), так как произведение первых трех элементов имеет порядок 4, а произведение вторых трех — порядок 2. Следовательно, $T(i)^\gamma \subseteq T(j)$. Применив к $T(j)$ обратный автоморфизм γ^{-1}, видим, что $T(i)^\gamma = T(j)$. Тем самым

по автоморфизму γ мы построили такую подстановку π, что $T(i)^\gamma = T(i\pi)$ для всех $i = 1, 2, \ldots, n$. Так как

$$(kl)^\gamma = (T(k) \cap T(l))^\gamma = T(k\pi) \cap T(l\pi) = \\ = (k\pi,\quad l\pi) = \pi^{-1}(kl)\pi,$$

то γ совпадает на всех транспозициях, а потому и вообще на всех подстановках с сопряжением подстановкой π. Теорема доказана.

Группы S_2, S_6 не являются совершенными, так как первая абелева, а вторая обладает внешним автоморфизмом порядка 2. Построение этого автоморфизма указано, например, в заметке: Miller D. W.— Amer. Math. Monthly, 1958, **65**, № 4, p. 252—254.

5.3.2. Упражнение. Совершенная нормальная подгруппа всегда выделяется прямым множителем группы. Наводящий вопрос: что должно быть другим множителем?

§ 6. Расширения посредством автоморфизмов

Опишем две важные в теории групп конструкции, основанные на автоморфизмах.

6.1. Голоморф. Эта конструкция возникает в связи вот с каким вопросом: нельзя ли произвольную группу G вложить изоморфно в такую группу G^*, чтобы каждый автоморфизм группы G оказался сужением внутреннего автоморфизма группы G^*? Пусть $\Phi = \mathrm{Aut}\, G$. Оказывается, в качестве G^* можно взять множество пар φg, $\varphi \in \Phi$, $g \in G$, умножаемых по правилу:

$$\varphi g \cdot \varphi' g' = \varphi\varphi' g^{\varphi'} g' \qquad (1)$$

(мы пишем пары без скобок и запятых). Действительно, аксиомы группы проверяются непосредственно. Так же непосредственно проверяется, что отображения

$$\Phi \to G^*,\ G \to G^* \qquad (2)$$

по правилам $\varphi \mapsto \varphi 1$, $g \mapsto 1g$ являются изоморфными вложениями. Мы отождествим Φ и G с подгруппами из G^* в силу этих вложений. Из правила умножения (1) сразу вытекает, что

$$\varphi^{-1} g \varphi = g^\varphi \text{ для } \varphi \in \Phi,\ g \in G. \qquad (3)$$

Теперь ясно, что

$$G^* = \Phi G,\ G \trianglelefteqslant G^*,\ \Phi \cap G = 1 \qquad (4)$$

и ввиду (3) каждый автоморфизм $\varphi \in \Phi$ является сужением некоторого внутреннего автоморфизма группы G^*. Задача решена. Построенная группа ΦG называется *голоморфом* группы G и обозначается $\mathrm{Hol}\ G$.

Если вместо $\Phi = \mathrm{Aut}\ G$ взять $\Phi \leqslant \mathrm{Aut}\ G$, то группа ΦG по-прежнему будет обладать свойствами (3), (4). В этом случае ΦG называется *расширением группы G посредством группы автоморфизмов* Φ. Ввиду (4) это согласуется с общим понятием расширения из п. 4.4.

Можно еще дальше обобщить ситуацию и взять произвольную группу Φ с отмеченным гомоморфизмом $\Phi \to \mathrm{Aut}\ G$. Считая, что элементы из Φ действуют на G как соответствующие им автоморфизмы, мы тем же правилом (1) превращаем ΦG в группу со свойствами (3), (4). Теперь группа ΦG называется *расширением группы G посредством группы операторов* Φ.

Отметим, что все обсуждавшиеся сейчас расширения расщепляемы в следующем смысле: расширение G группы A посредством группы B называется *расщепляемым*, если в G существуют такие подгруппы H, K, что

$$G = HK,\ A \simeq H \trianglelefteqslant G,\ H \cap K = 1.$$

Очевидно, что тогда $K \simeq G/A$. Говорят также, что G — *полупрямое произведение* групп A и B, и пишут $G = A \leftthreetimes B$ или $G = B \rightthreetimes A$.

Укажем голоморфы некоторых конкретных групп.

6.1.1. Примеры. I. Пусть K — любое из колец $\mathbb{Z}$, $\mathbb{Z}_n$, $\mathbb{Q}$. Согласно 5.1.1.I автоморфизмы аддитивной группы K исчерпываются умножениями на элементы из K^*, поэтому

$$\mathrm{Hol}\ K \simeq \left\{ \begin{pmatrix} 1 & \beta \\ 0 & \alpha \end{pmatrix} \middle| \alpha \in K^*,\ \beta \in K \right\}.$$

II. Похожее по форме описание можно дать для $\mathrm{Hol}\ \mathbb{C}_{p^\infty}$. Именно, частичную последовательность $(s_1, s_2, \ldots)$ назовем *p-нитью*, если в ней несколько первых мест пусты, а на остальных стоят элементы $s_n \in \mathbb{Z}_{p^n}$, причем $ps_n = s_{n+1}$ (в понятном смысле) и ее нельзя доопределить на пустых местах с сохранением этого свойства. Условимся

складывать p-нити покомпонентно на тех местах, где оба слагаемых определены, с последующим доопределением суммы на пустых местах, пока оно возможно. Непосредственно проверяется, что p-нити с таким сложением составляют группу. Она изоморфна группе $\mathbb{C}_{p^\infty}$. Действительно, пусть ε_n — первообразный корень из 1 степени p^n в поле комплексных чисел, причем $\varepsilon_{n+1}^p = \varepsilon_n$, $n = 1, 2, \ldots$ Каждое число x из $\mathbb{C}_{p^\infty}$ лежит в некоторой группе $\mathbb{C}_{p^n}$, поэтому $x = \varepsilon_n^{s_n}$, $s_n \in \mathbb{Z}_{p^n}$, начиная с некоторого n. Так как $\varepsilon_{n+1}^{s_{n+1}} = \varepsilon_n^{s_n} = \varepsilon_{n+1}^{ps_n}$, то частичная последовательность показателей s_n будет p-нитью. Легко видеть, что отображение $x \mapsto (s_1, s_2, \ldots)$ является изоморфизмом группы $\mathbb{C}_{p^\infty}$ на группу p-нитей, причем автоморфизмы из $\operatorname{Aut}\mathbb{C}_{p^\infty}$, представленные согласно 5.1.1.II целыми p-адическими числами, действуют на p-нити как покомпонентные умножения. Поэтому

$$\operatorname{Hol}\mathbb{C}_{p^\infty} \simeq \left\{\begin{pmatrix}1 & \beta\\ 0 & \alpha\end{pmatrix} \middle| \alpha \in \mathbb{Z}_{p^\infty}^*,\ \beta \text{ есть } p\text{-нить}\right\}.$$

Отличие от предыдущего примера здесь в том, что коэффициенты матриц берутся из разных множеств и не видно кольца, в котором бы оба они лежали.

III. Мы знаем, что при $n \neq 2, 6$ группа $\boldsymbol{S}_n$ совершенна. В частности, $\operatorname{Aut}\boldsymbol{S}_n \simeq \boldsymbol{S}_n$. Так как $\boldsymbol{S}_n$ нормальна в своем голоморфе, то она выделяется в нем прямым множителем (упражнение 5.3.2). Поэтому

$$\operatorname{Hol}\boldsymbol{S}_n \simeq \boldsymbol{S}_n \times \boldsymbol{S}_n \quad \text{при } n \neq 2,\ 6.$$

Ясно, что и для любой другой совершенной группы G справедлива формула $\operatorname{Hol} G \simeq G \times G$.

IV. Для голоморфов групп $\boldsymbol{GL}$, $\boldsymbol{SL}$, $\boldsymbol{T}$ и пр. трудно рассчитывать на описание, которое было бы проще определения, поскольку уже группы автоморфизмов в этом случае довольно сложно устроены.

6.1.2. Упражнение. Пусть K — любое из колец $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Q}$. Доказать формулу (в суммах n слагаемых):

$$\operatorname{Hol}(K \oplus \ldots \oplus K) \simeq$$
$$\simeq \left\{\begin{pmatrix}1 & \beta\\ 0 & \alpha\end{pmatrix} \middle| \alpha \in \boldsymbol{GL}_n(K),\ \beta \in K \oplus \ldots \oplus K\right\}.$$

6.1.3. Упражнение. Найти все классы сопряженных элементов группы Hol $\mathbb{Z}$.

6.1.4. Упражнение. Указать в Hol $\mathbb{Z}$ такой убывающий ряд нормальных подгрупп

$$\mathrm{Hol}\,\mathbb{Z} = H_0 \geqslant H_1 \geqslant \ldots,$$

что $\bigcap H_i = 1$ и каждая секция H_i/H_{i+1} лежит в центре фактор-группы H_0/H_{i+1}, $i = 0, 1, 2, \ldots$

6.1.5. Упражнение. Является ли Hol $\mathbb{Z}$ совершенной группой?

6.1.6. Упражнение. Пусть G — расширение конечной элементарной абелевой p-группы A при помощи конечной элементарной абелевой q-группы B. Если $p \neq q$ и B — нециклическая группа, то в G существуют элементы порядка pq.

Решение. Будем рассматривать группу $A \simeq \mathbb{Z}_p \oplus \ldots \oplus \mathbb{Z}_p$ как векторное пространство над полем k из p элементов. Пусть B^* — множество линейных преобразований этого пространства, индуцированных сопряжениями посредством элементов из B. Легко видеть, что дело сводится к отысканию неединичных элементов $a \in A$, $b \in B$ с условием $a^b = a$ (тогда ab будет искомым элементом порядка pq) или, другими словами, к отысканию в B^* неединичного элемента θ, обладающего в пространстве A ненулевой неподвижной точкой. По условию, B^* содержит два таких преобразования φ, ψ порядка q, что $\mathrm{гр}\,(\varphi) \neq \mathrm{гр}\,(\psi)$. Из основного курса алгебры известно, что перестановочные линейные преобразования обладают общим собственным вектором над алгебраическим замыканием $\bar{k}$ поля k; пусть a — такой вектор для φ, ψ, причем

$$a\varphi = \mu a, \quad a\psi = \nu a, \quad \mu, \nu \in \bar{k}.$$

Если $\mu = 1$ или $\nu = 1$, то можно взять $\theta = \varphi$ или $\theta = \psi$ соответственно. Пусть $\mu \neq 1$, $\nu \neq 1$. Так как μ, ν порождают в мультипликативной группе поля $\bar{k}$ одну и ту же циклическую подгруппу порядка q, то $\mu = \nu^m$ при подходящем натуральном показателе m. Тогда $\theta = \varphi\psi^{-m}$ — искомое преобразование, так как $\theta \neq 1$ и $a\theta = a$.

6.2. Сплетения. Пусть A, B — группы. Обозначим через Fun (B, A), fun (B, A) декартово произведение и

прямое произведение изоморфных копий группы A, индексированных элементами группы B. Таким образом, $\mathbf{Fun}\,(B, A)$ — это группа всех функций $B \to A$ с обычным умножением, а $\mathrm{fun}\,(B, A)$ — подгруппа функций с конечными носителями. Для $f \in \mathbf{Fun}\,(B, A)$, $b \in B$ определим функцию f^b, полагая

$$f^b(x) = f(bx), \quad x \in B. \tag{5}$$

Непосредственно проверяется, что отображение

$$\hat{b}: \mathbf{Fun}\,(B, A) \to \mathbf{Fun}\,(B, A) \tag{6}$$

по правилу $f \mapsto f^b$ есть автоморфизм группы $\mathbf{Fun}\,(B, A)$, отображающий $\mathrm{fun}\,(B, A)$ на себя, а отображения

$$B \to \mathrm{Aut}\,(\mathbf{Fun}\,(B, A)), \quad B \to \mathrm{Aut}\,(\mathrm{fun}\,(B, A)), \tag{7}$$

сопоставляющие каждому b из B автоморфизм $\hat{b}$ и его сужение на $\mathrm{fun}\,(B, A)$, являются при $A \neq 1$ изоморфными вложениями. Расширения групп $\mathbf{Fun}\,(B, A)$, $\mathrm{fun}\,(B, A)$ посредством групп операторов (7) называются *декартовым сплетением* и *прямым сплетением группы* A с *группой* B и обозначаются $A \,\bar{\wr}\, B$ и $A \wr B$ соответственно. Таким образом, декартово сплетение $A \,\bar{\wr}\, B$ — это множество $B \cdot \mathbf{Fun}\,(B, A)$ с умножением

$$bf \cdot b'f' = bb'f^{b'}f', \text{ где } f^b(x) = f(bx), \tag{8}$$

а прямое сплетение $A \wr B$ — его подгруппа $B \cdot \mathrm{fun}\,(B, A)$. Мы видим, что при построении сплетений группы A с группой B сами группы A, B играют разные роли: A *пассивна*, а B *активна*. Впредь мы так и будем называть эти группы.

Подгруппы $\mathbf{Fun}\,(B, A)$, $\mathrm{fun}\,(B, A)$ называются *фундаментами* или *базами* соответствующих сплетений. Очевидно, декартово сплетение $A \,\bar{\wr}\, B$ и прямое сплетение $A \wr B$ тогда и только тогда совпадают, когда A тривиальна или B конечна. Подгруппа

$$\mathrm{Diag}\,(B, A) = \{f \mid f \in \mathbf{Fun}\,(B, A),\ f(x) = \mathrm{const} \text{ для } x \in B\},$$

т. е. диагональ базы $\mathbf{Fun}\,(B, A)$, называется также *диагональю декартова сплетения* $A \,\bar{\wr}\, B$. Наконец, для каж-

дого $a \in A$ определим функцию $\dot{a}$ из $\mathrm{Fun}(B, A)$, полагая

$$\dot{a}(x) = \begin{cases} a & \text{при } x = e, \\ e & \text{при } x \neq e. \end{cases}$$

Непосредственно проверяется, что отображение $A \to \mathrm{Fun}(B, A)$ по правилу $a \mapsto \dot{a}$ является изоморфным вложением. Подгруппа $\dot{A}$, на которую при этом вложении отображается группа A, называется *первой копией*, а сопряженная с ней подгруппа $\dot{A}^b$, $b \in B$, называется b-*й копией* пассивной группы. Таким образом, пассивная группа A участвует в сплетениях $A \bar{\imath} B$, $A \imath B$ своими копиями $\dot{A}^b$, а активная группа B сама содержится в этих сплетениях и, действуя сопряжениями на копии пассивной группы, «сплетает» их — переставляет между собой. Очевидно,

$$\mathrm{fun}(B, A) = \prod_{b \in B} \dot{A}^b.$$

6.2.1. Упражнение. Если $A' \leqslant A$, $B' \leqslant B$, то сплетение $A' \imath B'$ изоморфно подгруппе сплетения $A \imath B$ (порожденной образом подгруппы A' при каноническом вложении в первую копию пассивной группы и подгруппой B').

6.2.2. Упражнение. Нетривиальная нормальная подгруппа прямого сплетения имеет нетривиальное пересечение с базой (при условии, конечно, что пассивная группа нетривиальна).

6.2.3. Упражнение. Пусть группа A нетривиальна. Тогда

$$Z(A \bar{\imath} B) = \mathrm{Diag}(B, Z(A)),$$

$$Z(A \imath B) = 1, \text{ если } B \text{ бесконечна.}$$

6.2.4. Упражнение. Коммутант сплетения $A \imath B$ совпадает с произведением $[B, B] \cdot H$, где

$$H = \left\{ f \in \mathrm{fun}(B, A) \mid \prod_{\in B} f(b) \equiv e \pmod{[A, A]} \right\}.$$

6.2.5. Упражнение. Каждый элемент коммутанта сплетения $\mathbb{Z} \imath \mathbb{Z}$ есть коммутатор.

6.2.6. Упражнение. Сплетение $\mathbb{Z}\, r\, \mathbb{Z}$ изоморфно подгруппе, порожденной в $GL_n(\mathbb{R})$ матрицами

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

где ζ — трансцендентное действительное число.

6.2.7. Упражнение. Операции $\bar{r}$, r неассоциативны в классе групп (даже в классе конечных групп).

Важную связь сплетений с произвольными расширениями дает следующая

6.2.8. Теорема. *Любое расширение группы A посредством группы B изоморфно вкладывается в декартово сплетение $A\ \bar{r}\ B$* (вложение Фробениуса).

Доказательство. Пусть $A \trianglelefteq G$, $G/A = B$, s: $B \to G$ — функция, выбирающая представителей в смежных классах. Пусть $W = A\ \bar{r}\ B$. Определим отображение φ_s: $G \to W$, полагая $g^{\varphi_s} = \bar{g} f_g$, $g \in G$, где $\bar{g}$ — смежный класс Ag, f_g — элемент базы сплетения W, задаваемый формулой

$$f_g(b) = ((gb)^s)^{-1} g b^s, \quad b \in B.$$

Непосредственно проверяется, что φ_s — изоморфное вложение. Оно называется *вложением Фробениуса*.

6.2.9. Упражнение. В тех же обозначениях

$$G^{\varphi_s} \cdot \mathrm{Fun}\ (B, A) = W, \quad G^{\varphi_s} \cap \mathrm{Fun}\ (B, A) = A^{\varphi_s}.$$

6.2.10. Упражнение. Если s' — другая выбирающая функция, то подгруппы G^{φ_s}, $G^{\varphi_{s'}}$ сопряжены в W.

Отметим, что декартово сплетение $A\ \bar{r}\ B$ называют также полным сплетением и обозначают $A\ \mathrm{Wr}\ B$, а прямое сплетение $A\ r\ B$ называют также дискретным сплетением и обозначают $A\ \mathrm{wr}\ B$. Пассивную и активную группы называют иногда нижней и верхней. В § 12 мы слегка обобщим изложенное здесь понятие сплетения в связи с рассмотрением мономиальных представлений — исторически самой ранней разновидности сплетений. Там же будет указано вложение произвольной группы G, содержащей заданную подгруппу H заданного индекса m, в мономиальную группу матриц степени m над H — начальный вариант доказанной здесь теоремы.

Глава 3

АБЕЛЕВЫ ГРУППЫ

Для абелевых групп более удобна и общепринята аддитивная запись операции, и мы будем в этой главе пользоваться ею.

§ 7. Свободные абелевы группы. Размерность

7.1. Свободные абелевы группы. Пусть $\mathfrak{L}$ — класс групп. Говорят, что группа $F = (x_i \mid i \in I)$ из $\mathfrak{L}$ есть *свободная группа в классе* $\mathfrak{L}$ *со свободным порождающим множеством* $\{x_i \mid i \in I\}$, если для любой группы $G \in \mathfrak{L}$ с порождающим множеством $\{a_i \mid i \in I\}$ отображение $x_i \mapsto a_i$ продолжается до гомоморфизма $F \to G$. Мощность множества I называется *степенью* (*свободы*) свободной группы F. Само множество $\{x_i \mid i \in I\}$ будем называть также *базой* F. Можно показать, что не всякий класс групп обладает свободными группами. Однако в классе абелевых групп свободные группы существуют и имеют очень ясное описание.

7.1.1. Лемма. *Пусть фактор-группа G/N абелевой группы G разлагается в прямую сумму бесконечных циклических групп*:

$$G/N = \sum_{i \in I} (A_i/N), \qquad A_i = \text{гр}\,(a_i, N)\,.$$

Тогда G есть прямая сумма подгрупп N и $A = \text{гр}\ (a_i \mid i \in I)$.

Доказательство. Во-первых, замечаем, что $G = \text{гр}\ (N, A)$. Далее, предположим, что $A \cap N \neq 0$. В пересечении $A \cap N$ возьмем ненулевой элемент a, который можно записать в виде

$$a = \sum n_k a_{i_k}.$$

Отсюда в фактор-группе G/N получаем равенство

$$N = \sum n_k a_{i_k} + N,$$

что в силу определения прямой суммы влечет $n_k a_{i_k} + N = N$. Так как A_{i_k} / N является бесконечной циклической группой, то из равенства $n_k a_{i_k} + N = N$ следует $n_k = 0$. Таким образом, элемент $a = \sum n_k a_{i_k}$ равен нулю, что противоречит допущению.

7.1.2. Т е о р е м а. *Прямые суммы бесконечных циклических групп и только они являются свободными группами в классе абелевых групп.*

Д о к а з а т е л ь с т в о. Рассмотрим прямую сумму $G = \sum\limits_{i \in I} (x_i)$ бесконечных циклических групп (x_i) и произвольную абелеву группу A с множеством порождающих элементов a_i, $i \in I$. Отображение $\sum n_k x_{i_k} \mapsto \sum n_k a_{i_k}$, продолжающее отображение $x_i \mapsto a_i$ множества $\{x_i \mid i \in I\}$ на множество $\{a_i \mid i \in I\}$, как легко видеть, будет гомоморфизмом $G \to A$. Но это означает, что G есть свободная абелева группа, т. е. свободная группа в классе абелевых групп. Степень ее свободы равна числу прямых слагаемых.

Пусть теперь F — свободная абелева группа и $\{x_i \mid i \in I\}$ — множество ее свободных порождающих. По определению свободной группы существует гомоморфизм τ группы F на прямую сумму $A = \sum\limits_{i \in I} (a_i)$ бесконечных циклических групп (a_i), продолжающий отображение $x_i \mapsto a_i$. С другой стороны, по доказанному выше, существует гомоморфизм $\sigma\colon A \to F$, продолжающий отображение $a_i \mapsto x_i$. Так как $\tau\sigma$ оставляет на месте все порождающие элементы группы F, то $\tau\sigma = 1$ и $F \simeq A$. Теорема доказана.

Оказывается, подгруппы свободной абелевой группы сами являются свободными абелевыми группами. В доказательстве этого факта мы воспользуемся понятием *трансфинитно возрастающей матрёшки*

$$0 = N_0 < N_1 < \ldots < N_\alpha < \ldots < N_\gamma = G \qquad (1)$$

абелевой группы G, т. е. вполне упорядоченного по возрастанию ряда подгрупп, занумерованных трансфинитными числами. При этом предполагается, что для предельного трансфинитного числа α подгруппа N_α совпадает с объединением всех подгрупп N_β, $\beta < \alpha$.

Если $A \leqslant G$, то в системе подгрупп

$$0 = A_0 \leqslant A_1 \leqslant \ldots \leqslant A_\alpha \leqslant \ldots \leqslant A_\gamma = A, \qquad (2)$$

где $A_\alpha = A \cap N_\alpha$, возможны совпадения. Заново занумеровав трансфинитными числами различные члены системы (2), получаем возрастающую матрёшку

$$0 = A'_0 < A'_1 < \ldots < A'_\rho < \ldots < A'_\tau = A \qquad (3)$$

подгруппы A, о которой говорят, что она получена пересечением матрёшки (1) с подгруппой A.

Для доказательства теоремы о подгруппах нам потребуется следующий признак свободы коммутативной группы.

7.1.3. Теорема. *Абелева группа G свободна тогда и только тогда, когда она обладает трансфинитно возрастающей матрёшкой, каждая секция которой изоморфна бесконечной циклической группе $\mathbb{Z}$.*

Доказательство. Пусть в абелевой группе G имеется возрастающая матрёшка (1) с бесконечными циклическими секциями. Для всякого $\alpha < \gamma$ в разности $N_{\alpha+1} \setminus N_\alpha$ выберем такой элемент $a_{\alpha+1}$, что $N_{\alpha+1} = (a_{\alpha+1} + N_\alpha)$, и покажем разложимость G в прямую сумму $\sum_{\alpha<\gamma} (a_{\alpha+1})$ бесконечных циклических подгрупп $(a_{\alpha+1})$. Доказательство будем вести индукцией по длине γ матрёшки (1). При $\gamma = 1$ утверждение очевидно; сделаем допущение о справедливости этого утверждения для всякого $\alpha < \gamma$.

В группе G выбираем произвольный элемент $g \neq 0$ и считаем $g \in N_\beta$, $g \notin \sum_{\sigma<\beta} N_\sigma = N_{\beta-1}$. В силу $N_\beta = (a_\beta, N_{\beta-1})$ и леммы 7.1.1 элемент g однозначно представляется в виде $g = g_1 + na_\beta$, $g_1 \in N_{\beta-1}$. По индуктивному предположению, так как $\beta - 1 < \gamma$, элемент g_1 однозначно записывается через $a_{\beta i}$:

$$g_1 = n_1 a_{\beta_1} + \ldots + n_s a_{\beta_s}, \quad \beta_i < \beta,$$

что влечет однозначность записи

$$g = n_1 a_{\beta_1} + \ldots + n_s a_{\beta_s} + na_\beta.$$

Итак, доказана разложимость группы G в прямую сумму бесконечных циклических подгрупп, что по теореме 7.1.2 равносильно свободе G.

Пусть теперь G — свободная абелева группа и $G = \sum_{\alpha<\gamma} (g_\alpha)$ — разложение G в прямую сумму бесконечных циклических подгрупп. Положив $N_0 = 0$, $N_{\alpha+1} = (g_\alpha, N_\alpha)$ и $N_\alpha = \sum_{\beta<\alpha} N_\beta$ для предельного трансфинитного числа α, получаем трансфинитно возрастающую матрёшку с бесконечными циклическими секциями. Тем самым доказана и необходимость условия. Теорема доказана.

В п. 4.4 было установлено, что секции субнормальной матрёшки подгруппы $A \leqslant G$, полученной пересечением A с членами субнормальной матрёшки группы G, изоморфны подгруппам секций матрёшки группы G. Точно так же доказывается это утверждение для трансфинитно возрастающих матрёшек (1) и (3). Поэтому непосредственно из теоремы 7.1.3 вытекает теорема о подгруппах свободной абелевой группы:

7.1.4. Т е о р е м а. *Всякая ненулевая подгруппа свободной абелевой группы является свободной абелевой группой.*

7.1.5. У п р а ж н е н и е. Пусть n — целое положительное число, $\mathfrak{A}_n$ — класс всех абелевых групп, на которых выполняется тождество $nx = 0$. Доказать, что прямые суммы групп $\mathbb{Z}_n$ и только они будут свободными группами в классе $\mathfrak{A}_n$. Для каких классов $\mathfrak{A}_n$ справедлива теорема о свободе подгрупп свободной группы?

7.2. Размерность абелевой группы. Выше мы определили степень свободной абелевой группы как мощность системы свободных порождающих. Это понятие по определению имеет смысл только для свободных абелевых групп. Теперь мы введем понятие размерности для произвольных абелевых групп. Оно аналогично понятию размерности векторного пространства и, как легко сообразить, для свободных абелевых групп размерность будет совпадать с их степенью свободы.

Конечное множество элементов $g_1, \ldots, g_k$ абелевой группы G называется *линейно зависимым*, если найдутся такие целые числа $n_1, \ldots, n_k$, не все равные нулю, что $\sum n_i g_i = 0$. Произвольная система элементов группы G называется *линейно зависимой*, если линейно зависима некоторая конечная подсистема этой системы. Легко показать, что в абелевой группе G, содержащей хотя бы

один элемент бесконечного порядка, существуют максимальные линейно независимые системы элементов и все такие системы имеют одинаковые мощности. Мощность максимальной линейно независимой системы элементов абелевой группы G называется *размерностью* или, более точно, *$\mathbb{Z}$-размерностью* этой группы и обозначается $\dim G$ или, более точно, $\dim_{\mathbb{Z}} G$.

Периодическая группа, очевидно, не содержит линейно независимых систем, поэтому ее размерность естественно считать равной нулю.

7.2.1. Т е о р е м а. *Ненулевая абелева группа без кручения имеет размерность* 1 *тогда и только тогда, когда она изоморфна подгруппе аддитивной группы рациональных чисел* $\mathbb{Q}$.

Д о к а з а т е л ь с т в о. Пусть $G \leqslant \mathbb{Q}$, $G \neq 0$ и g_1, g_2 — отличные от нуля элементы группы G. Тогда существуют такие целые числа $n_1, n_2 \neq 0$, что $n_1 g_1 = n_2 g_2$. Таким образом, любые два ненулевых элемента из G составляют линейно зависимую систему и, следовательно, $\dim G = 1$.

Пусть теперь размерность абелевой группы G без кручения равна 1. Зафиксируем некоторый отличный от нуля элемент $g_0 \in G$. Тогда для произвольного элемента $g \in G$ найдутся такие целые n, m (причем, если $g \neq 0$, то n, $m \neq 0$), что $ng = mg_0$. Ввиду произвольности выбора $g \in G$ мы получили некоторое отображение φ: $g \mapsto \frac{m}{n}$ группы G в группу $\mathbb{Q}$.

Отображение φ однозначно. В самом деле, пусть еще $n_1 g = m_1 g_0$. Вычитая почленно из равенства $ng = mg_0$, умноженного на m_1, равенство $n_1 g = m_1 g_0$, умноженное на m, получаем $(nm_1 - n_1 m)\, g = 0$. Если $g \neq 0$, то $nm_1 - n_1 m = 0$ и, значит, $\frac{m}{n} = \frac{m_1}{n_1}$. При $g = 0$ числа m, m_1 обязаны равняться нулю, поэтому $\frac{m}{n} = \frac{m_1}{n_1} = 0$.

Пусть теперь $kg_1 = lg_0$ и $\frac{l}{k} = \frac{m}{n}$. Тогда из равенств $ng = mg_0$, $kg_1 = lg_0$ получаем $mk\,(g - g_1) = 0$ и, так как G без кручения, $g = g_1$. Тем самым доказана взаимная однозначность отображения φ.

Так как из равенств $ng = mg_0$, $sg' = tg_0$, $g, g' \in G$, следует, что $ns\,(g + g') = (sm + nd)\, g_0$, то отображение

φ удовлетворяет соотношению $(g + g')\varphi = g\varphi + g'\varphi$. Теорема доказана.

7.2.2. Упражнение. Пусть G — абелева группа и $A \leqslant G$. Тогда $\dim G = \dim A + \dim G/A$.

7.2.3. *Пусть G — конечномерная абелева группа без кручения и φ — ее изоморфизм в себя. Тогда индекс $|G : G\varphi|$ конечен.*

Доказательство. Зафиксируем в G какую-нибудь максимальную линейно независимую систему элементов $a_1, \ldots, a_n$. Отображению φ естественным образом можно сопоставить матрицу $(\alpha_{ij}(\varphi))$ над полем $\mathbb{Q}$, полагая

$$a_i\varphi = \sum_j \alpha_{ij}(\varphi)\, a_j.$$

Погрузив G с отмеченной в ней базой $a_1, \ldots, a_n$ в векторное пространство $\mathbb{Q}^n$, мы можем продолжить φ до линейного преобразования этого пространства. Умножим характеристический многочлен этого преобразования на общий знаменатель его коэффициентов; пусть f —получившийся при этом многочлен над $\mathbb{Z}$. По основному свойству характеристического многочлена $f(\varphi) = 0$, а так как $\det \varphi \neq 0$, то $f(0) = m \neq 0$. Тогда $mG \leqslant G\varphi$. Так как $|G : mG| \leqslant m^{\dim G} < \infty$, то и $|G : G\varphi| < \infty$. Предложение доказано.

Следует предостеречь читателя, что далеко не все привычные теоремы линейной алгебры сохраняются для абелевых групп и их размерностей. Например, в связи с хорошо известной возможностью разложения любого векторного пространства в прямую сумму одномерных подпространств естественно спросить: всякая ли абелева группа без кручения разлагается в прямую сумму одномерных групп? Ответ отрицателен:

7.2.4. Пример (Л. С. Понтрягин). Существует двумерная абелева група G без кручения, не разложимая в прямую сумму $A \oplus B$, где A, B — одномерные слагаемые. Группу G мы определим как подгруппу аддитивной группы H всех линейных форм $ax + by$ с рациональными коэффициентами a, b; очевидно, $H \simeq \mathbb{Q} \oplus \mathbb{Q}$, так что $\dim H = 2$. Именно, пусть

$$G = \text{гр}\,(x_0, x_1, x_2, \ldots, y),$$

где

$$x_0 = x, \quad x_i = \frac{x_{i-1} + y}{2^{2i-1}}, \quad i = 1, 2, \ldots \tag{4}$$

Очевидные вычисления показывают, что

$$x_i = \frac{x + (1 + 2 + 2^4 + \ldots + 2^{(i-1)^2})\, y}{2^{i^2}}, \quad i = 1, 2, \ldots \tag{5}$$

Так как каждое x_{i-1} целочисленно выражается через x_i и y (см. (4)), то каждый элемент $g \in G$ целочисленно выражается через x_i и y при достаточно большом i. Отсюда и из (5) легко следует, что если $cy \in G$, $c \in \mathbb{Q}$, то $c \in \mathbb{Z}$,— запомним это.

Для доказательства неразложимости группы G в прямую сумму $A \oplus B$ достаточно убедиться, что никакой ненулевой элемент $g \in G$ не является безгранично делимым в G, т. е. для каждого $g \neq 0$ найдется такое натуральное число $n(g)$, что для каждого $n \geqslant n(g)$ уравнение $n\xi = g$ не имеет в G решений. В самом деле, если бы было $G = A \oplus B$, то A и B были бы одномерными (учесть 7.2.2 и то, что H не имеет кручения). Поскольку ни A, ни B не содержат ненулевых элементов, допускающих безграничное деление, то по теореме 7.2.1 $A \simeq B \simeq \mathbb{Z}$, откуда $G \simeq \mathbb{Z} \oplus \mathbb{Z}$, что очевидным образом неверно.

Итак, осталось доказать, что G не содержит ненулевых элементов, допускающих безграничное деление. Пусть, напротив, такой элемент g существует. Так как всякое его целочисленное кратное тоже безгранично делимо, то можно считать, что

$$g = ax + by, \quad \text{где } a, b \in \mathbb{Z}.$$

Из (5) видно, что коэффициентами линейных форм, лежащих в G, могут быть далеко не любые рациональные числа, а только 2-ичные дроби, поэтому безграничная делимость в группе G равносильна безграничной делимости пополам. Таким образом, для каждого $i = 1, 2, \ldots$ в G существует элемент

$$u_i = \frac{1}{2^{i^2}}\, g = \frac{ax + by}{2^{i^2}}.$$

Ввиду (5) $u_i - ax_i = c_i y$, где

$$c_i = \frac{1}{2^{i^2}}[b - a(1 + 2 + 2^4 + \ldots + 2^{(i-1)^2})].$$

По замечанию из первого абзаца c_i — целое число. «Уплотнив» сумму в круглых скобках до геометрической прогрессии со знаменателем 2, получим оценку

$$1 + 2 + 2^4 + \ldots + 2^{(i-1)^2} < 2^{(i-1)^2+1},$$

откуда

$$|c_i| < \frac{|a|}{2^{2(i-1)}} + \frac{|b|}{2^{i^2}}.$$

Так как c_i — целые числа, то, начиная с некоторого i, все они равны нулю. Но тогда для этих i

$$b - a(1 + 2 + 2^4 + \ldots + 2^{(i-1)^2}) = 0,$$

что явно невозможно.

§ 8. Конечно порожденные абелевы группы

В этом параграфе мы в первую очередь уточним теорему о подгруппах свободной абелевой группы конечной степени и, основываясь на этом уточнении, докажем основную теорему о конечно порожденных абелевых группах.

8.1.1. Теорема. *Пусть F_n — свободная абелева группа конечной степени n, A — ее отличная от нуля подгруппа. Тогда A свободна и группы F_n, A обладают соответственно базами $f_1, \ldots, f_n$ и $a_1, \ldots, a_k$ такими, что $k \leqslant n$, $a_i = m_i f_i$, $1 \leqslant i \leqslant k$, и m_{i+1} делится на m_i, $1 \leqslant i \leqslant k-1$.*

Доказательство. Пусть

$$F_n = (f_1') \oplus \ldots \oplus (f_n'),$$
$$A = (a_1') \oplus \ldots \oplus (a_k')$$

и

$$a_i' = \sum_j m_{ij} f_j', \qquad m_{ij} \in \mathbb{Z}.$$

Возникает матрица $M = (m_{ij})$. Будем называть *элементарными* следующие преобразования строк и столбцов целочисленной матрицы: а) перестановка двух строк, б) прибавление к одной строке целочисленного кратного другой строки, в) умножение строки на -1 и аналогич-

ные преобразования столбцов. Пользуясь тем, что для любых целых чисел a, b, отличных от нуля, найдутся такие целые числа x, y, что $ax + by =$ н. о. д. (a, b), обычными рассуждениями линейной алгебры — более точно, теории λ-матриц — можно привести матрицу M элементарными преобразованиями строк и столбцов к виду

$$\begin{pmatrix} m_1 & & & & \\ & m_2 & & & \\ & & \ddots & & \\ & & & m_k & 0 \ldots 0 \end{pmatrix}, \text{ где } m_i \mid m_{i+1}.$$

Остается заметить, что элементарные преобразования строк соответствуют переходу к другой базе подгруппы A, а элементарные преобразования столбцов — к другой базе группы F_n. Теорема доказана.

8.1.2. Т е о р е м а. *Всякая конечно порожденная абелева группа G разлагается в прямую сумму циклических подгрупп. Более точно, G разлагается в прямую сумму бесконечных циклических и примарных циклических групп, причем количество бесконечных циклических слагаемых и набор порядков примарных циклических слагаемых в любом таком разложении одни и те же, т. е. являются инвариантами группы G.*

Д о к а з а т е л ь с т в о. По условию, группа G изоморфна некоторой фактор-группе F_n/A свободной абелевой группы F_n конечной степени n. Согласно теореме 8.1.1 в группах F_n и A существуют такие базы $f_1, \ldots, f_n$ и $a_1, \ldots, a_k$, что $a_i = m_i f_i$, $1 \leqslant i \leqslant k$. Покажем, что F_n/A — прямая сумма циклических подгрупп $(f_i + A)$.

Прежде всего, ясно, что F_n/A порождается этими подгруппами. Далее, пусть нуль фактор-группы F_n/A имеет запись

$$A = l_1 f_1 + \ldots + l_n f_n + A.$$

Тогда $l_1 f_1 + \ldots + l_n f_n = a \in A$. С другой стороны, выражая элемент a через базу $a_1, \ldots, a_k$ подгруппы A и учитывая равенства $a_i = m_i f_i$, приходим к соотношениям

$$l_1 f_1 + \ldots + l_n f_n = s_1 a_1 + \ldots + s_k a_k = \\ = s_1 m_1 f_1 + \ldots + s_k m_k f_k.$$

Ввиду однозначности записи элементов через свободные порождающие f_i получаем $l_i = s_i m_i$, $1 \leqslant i \leqslant k$, $l_j = 0$,

$k < j \leqslant n$. Но это означает, что каждый из элементов $l_i f_i$ принадлежит A. Тем самым доказана однозначность представления нуля в виде суммы элементов подгрупп $(f_i + A)$ и, значит, разложимость группы G в прямую сумму циклических подгрупп. Наконец, каждую конечную циклическую подгруппу можно разложить в прямую сумму примарных циклических слагаемых ввиду 1.2.12.

Докажем теперь инвариантность чисел, о которых говорится в формулировке теоремы. Зафиксируем какое-нибудь разложение группы G в прямую сумму бесконечных циклических и примарных циклических слагаемых и обозначим через G_∞ и G_p прямые суммы бесконечных циклических и циклических p-слагаемых этого разложения соответственно, где p — простое число. Понятно, что G_p — максимальная p-подгруппа, а $T = \sum_p G_p$ — максимальная периодическая подгруппа группы G, так что подгруппа $G_\infty \simeq G/T$ и все G_p не зависят от выбранного разложения. Так как число бесконечных циклических слагаемых равно $\dim G_\infty$, то оно — инвариант группы G. Далее, число циклических слагаемых в разложении группы G_p совпадает с таким же числом для ее нижнего слоя $G_p^* = \{g \in G_p \mid pg = 0\}$ и, значит, с размерностью векторного пространства G_p^* над полем из p элементов, а потому — тоже инвариант. Наконец, пусть

$$G_p \simeq \mathbb{Z}_{p^{m_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_s}}$$

и, для определенности, $m_1 \geqslant \ldots \geqslant m_s$. Индукцией по $m_1 + \ldots + m_s$ мы докажем, что числа m_i не зависят от выбора разложения. В самом деле,

$$G_p/G_p^* \simeq \mathbb{Z}_{p^{m_1-1}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_s-1}},$$

поэтому, по индуктивному предположению, те из чисел m_i, которые $\geqslant 2$,— инварианты разложения. Так как количество остальных m_i — это разность между s и количеством чисел $m_i \geqslant 2$, то оно — также инвариант группы. Теорема доказана.

8.1.3. Упражнение. Пусть F — свободная абелева группа конечной степени n с базой

$$f_1, \ldots, f_n. \tag{3}$$

Элементарным преобразованием базы (3) назовем переход от (3) к базе одного из следующих типов:

а) $f_1, \ldots, f_j, \ldots, f_i, \ldots, f_n$, $i < j$,

б) $f_1, \ldots, f_i + mf_j, \ldots, f_j, \ldots, f_n$, $i \neq j$,

в) $f_1, \ldots, -f_i, \ldots, f_n$.

Показать, что с помощью конечной цепочки элементарных преобразований можно перейти от базы (3) к наперед заданной базе группы F.

8.1.4. Упражнение. Пересечение подгрупп конечного индекса конечно порожденной абелевой группы равно нулю.

8.1.5. Упражнение. Совокупность всех элементов конечного порядка конечно порожденной абелевой группы — конечная подгруппа.

8.1.6. Упражнение. Показать на примере, что теорема 8.1.1 не распространяется на случай свободных абелевых групп бесконечной степени.

Решение. Пусть $G = (a_1) \oplus (a_2) \oplus \ldots$ — счетная прямая сумма бесконечных циклических групп,

$$H = \text{гр}\,(b_1, b_2, \ldots), \text{ где } b_n = na_n - a_{n-1}.$$

Если бы в G и H существовали согласованные базы, то фактор-группа $G/H \simeq \mathbb{Q}$ тоже разлагалась бы в прямую сумму циклических групп, что неверно.

8.1.7. Упражнение. Все подгруппы конечно порожденной абелевой группы конечно порождены.

8.1.8. Упражнение. Если A, B — конечно порожденные абелевы группы, то аддитивная группа кольца $\text{Hom}\,(A, B)$ (см. определение в 5.1.6) также конечно порождена.

§ 9. Полные абелевы группы

Группа G называется *полной* или *делимой*, если для всякого целого числа $n > 0$ и любого элемента $g \in G$ уравнение $nx = g$ имеет в группе G хотя бы одно решение.

9.1.1. Примеры. I. Очевидно, аддитивная группа $\mathbb{Q}$ рациональных чисел полна.

II. Докажем полноту квазициклической группы $\mathbb{C}_{p^\infty}$. Как мы знаем, группа $\mathbb{C}_{p^\infty}$ изоморфна (в аддитивной записи) объединению возрастающей цепочки конечных

циклических групп

$$(a_1) < (a_2) < \ldots < (a_n) < \ldots,$$

причем $pa_1 = 0$, $pa_{n+1} = a_n$, $n = 1, 2, \ldots$. Рассмотрим уравнение $sx = g$. Элемент g содержится в одной из подгрупп последовательности, например, в (a_n), т. е. $g = la_n$. Если $s = p^k m$, $(m, p) = 1$, то найдутся такие d_1, d_2, что $1 = p^n d_1 + md_2$. Отсюда с помощью равенств $g = la_n$, $p^n a_n = 0$ получаем $g = (p^n d_1 + md_2)\, g = md_2 la_n$. Последнее равенство с учетом соотношения $p^k a_{n+k} = a_n$ влечет равенство $g = mp^k (d_2 l a_{n+k})$. Таким образом, элемент $d_2 l a_{n+k}$ удовлетворяет уравнению $sx = g$.

Важность рассмотренных примеров определяется тем, что прямыми суммами групп $\mathbb{Q}$ и $\mathbb{C}_{p^\infty}$ исчерпываются все полные абелевы группы — см. ниже теорему 9.1.6.

9.1.2. У п р а ж н е н и е. Доказать полноту гомоморфных образов, прямых и декартовых сумм полных абелевых групп.

9.1.3. Т е о р е м а. *Произвольная абелева группа изоморфна подгруппе некоторой полной абелевой группы.*

Д о к а з а т е л ь с т в о. Пусть F — такая свободная абелева группа со свободными порождающими x_i, $i \in I$, что $G \simeq F/N$. Обозначим через F^* прямую сумму $\sum\limits_{i \in I} Q_i$ групп Q_i, изоморфных аддитивной группе рациональных чисел $\mathbb{Q}$, и в каждом слагаемом Q_i отметим какой-нибудь ненулевой элемент b_i. Очевидно, отображение $x_i \mapsto b_i$ продолжается до изоморфного отображения τ группы F в группу F^*. На основании изоморфизма τ группу F можно считать подгруппой в F^*. Согласно 9.1.2 фактор-группа F^*/N полна и, кроме того, содержит подгруппу F/N, изоморфную группе G.

9.1.4. Т е о р е м а. *Полная подгруппа A абелевой группы G выделяется в G прямым слагаемым.*

Д о к а з а т е л ь с т в о. Обозначим через B максимальную подгруппу группы G, пересекающуюся по нулю с подгруппой A (существование подгруппы B легко доказать методом трансфинитной индукции или с помощью леммы Цорна), и докажем равенство $G = A \oplus B$.

Предположим, что $G \neq A \oplus B$, и выберем элемент $g \in G$, не содержащийся в сумме $A \oplus B$. Циклическая подгруппа (g) имеет ненулевое пересечение с $A \oplus B$, так

как в противном случае сумма $A + B + (g)$ оказалась бы прямой и подгруппа $B \oplus (g)$, строго содержащая B, пересекалась с A по нулю, что противоречит выбору B. Таким образом, $g \notin A \oplus B$, но некоторое кратное ng этого элемента уже содержится в $A \oplus B$, причем n можно считать наименьшим положительным числом с условием $ng \in A \oplus B$. Можно даже считать n простым числом: если бы это было не так, то вместо g мы стали бы рассматривать элемент $\frac{n}{p} g$, где p — простой делитель n.

Ввиду выбора g найдутся такие элементы $a \in A$, $b \in B$, что $ng = a + b$. Так как подгруппа A полная, то в ней существует элемент a_1 с условием $na_1 = a$. Подставив в предыдущее равенство вместо a элемент na_1, получим $ng_1 = b$, где $g_1 = g - a_1$. Вместе с g элемент g_1 также не принадлежит подгруппе $A \oplus B$.

На основании выбора подгруппы B пересечение $A \cap (g_1, B)$ отлично от нуля. Это означает, что некоторый ненулевой элемент $a' \in A$ можно представить в виде суммы $a' = kg_1 + b'$, $b' \in B$, $0 < k < n$. Так как $(k, n) = 1$, то существуют такие l, s, что $lk + sn = 1$ и, следовательно, $g_1 = lkg_1 + sng_1$. Так как ng_1, $kg_1 = a' - b' \in A \oplus B$, то $g_1 \in A \oplus B$. Полученное противоречие доказывает теорему.

9.1.5. Упражнение. Сумма любого множества полных подгрупп абелевой группы является полной подгруппой.

9.1.6. Теорема. *Ненулевая полная абелева группа G разлагается в прямую сумму подгрупп, изоморфных аддитивной группе $\mathbb{Q}$ рациональных чисел или квазициклическим группам $\mathbb{C}_{p^\infty}$, быть может, по различным простым числам p.*

Доказательство. Нужное нам разложение группы G будем строить трансфинитной индукцией.

В группе G выберем произвольный элемент $g \neq 0$. Разберем две возможности относительно g.

1) Элемент g имеет бесконечный порядок. Ввиду полноты группы G существует такая последовательность элементов

$$g = g_1, g_2, \ldots, g_n, \ldots,$$

что $(n + 1) g_{n+1} = g_n$, $n = 1, 2, \ldots$ Легко проверяется,

что подгруппа, порожденная $g_1, g_2, \ldots$, изоморфна аддитивной группе рациональных чисел $\mathbb{Q}$.

2) Элемент g имеет конечный порядок n. Тогда элемент $a_1 = \frac{n}{p} g$, где p — простой делитель n, имеет простой порядок p. Снова ввиду полноты G существует последовательность элементов $a_1, a_2, \ldots, pa_{n+1} = a_n$, порождающая теперь группу, изоморфную $\mathbb{C}_{p^\infty}$.

Итак, в любом случае в группе G существует подгруппа A_1, изоморфная $\mathbb{Q}$ или $\mathbb{C}_{p^\infty}$.

Пусть построена последовательность полных подгрупп $A_1 < A_2 < \ldots < A_\beta < \ldots, \beta < \alpha$, такая, что при предельном трансфинитном числе β $A_\beta = \sum_{\delta<\beta} A_\delta$, а при непредельном β подгруппа A_β разлагается в прямую сумму $A_{\beta-1}$ и подгруппы $C_{\beta-1}$, изоморфной $\mathbb{Q}$ или некоторой $\mathbb{C}_{p^\infty}$.

Если α — предельное число, то положим $A_\alpha = \sum_{\beta<\alpha} A_\beta$. Если α — непредельное число, то подгруппа $A_{\alpha-1}$ полна. При $A_{\alpha-1} \neq G$ по теореме 9.1.4 существует прямое разложение $G = A_{\alpha-1} \oplus C$. Аналогично построению A_1 в полной группе C выбираем подгруппу $C_{\alpha-1}$, изоморфную $\mathbb{Q}$ или $\mathbb{C}_{p^\infty}$, и полагаем $A_\alpha = A_{\alpha-1} \oplus C_{\alpha-1}$.

Процесс индуктивного построения A_α оборвется на первом номере γ, для которого $A_\gamma = G$.

Построив A_α, $\alpha \leqslant \gamma$, остается заметить, что G разлагается в прямую сумму подгрупп $A_1 = C_0, C_1, \ldots, C_\alpha, \ldots$ Теорема доказана.

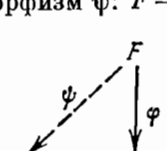
9.1.7. Упражнение. В абелевой группе без кручения пересечение любого множества полных подгрупп есть полная подгруппа.

9.1.8. Упражнение. Минимальная полная группа G^*, содержащая данную группу G, называется *пополнением* G. Другими словами, пополнение G^* группы G есть такая полная группа, содержащая G, что всякая полная группа A с условием $G \leqslant A \leqslant G^*$ совпадает с G^*. Доказать существование абелевых пополнений без кручения абелевой группы G без кручения. Между двумя такими пополнениями G существует изоморфизм, продолжающий произвольный наперед заданный автоморфизм G.

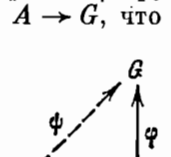
9.1.9. Упражнение. Показать на примере, что пересечение полных подгрупп периодической группы не обязано быть полным.

9.1.10. Упражнение. Группа, не содержащая ненулевых полных подгрупп, называется *редуцированной*. Произвольная абелева группа разлагается в прямую сумму полной и редуцированной подгрупп.

9.1.11. Упражнение. В теории модулей важную роль играют понятия проективного и инъективного модулей. Эти понятия для абелевых групп (модулей над кольцом целых чисел) можно определить так. Абелева группа F называется *проективной* (*проективным $\mathbb{Z}$-модулем*), если для любого гомоморфизма $\tau\colon A \to B$ группы A на B и любого гомоморфизма $\varphi\colon F \to B$ группы F в B существует такой гомоморфизм $\psi\colon F \to A$, что диаграмма



коммутативна, т. е. $\varphi = \psi\tau$. Абелева группа G называется *инъективной*, если для любого изоморфизма τ группы B в A и любого гомоморфизма φ группы B в G существует такой гомоморфизм $\psi\colon A \to G$, что диаграмма



коммутативна, т. е. $\varphi = \tau\psi$. Доказать, что 1) абелева группа проективна тогда и только тогда, когда она свободна, 2) абелева группа инъективна тогда и только тогда, когда она полна.

§ 10. Периодические абелевы группы

В произвольной абелевой группе G совокупность T всех элементов конечного порядка образует подгруппу, которую иногда называют *периодической частью* группы G.

Фактор-группа G/T уже не имеет кручения. Этот факт в какой-то мере сводит изучение произвольных абелевых групп к исследованию периодических групп и групп без кручения. Следует заметить, что вообще периодическая часть не выделяется прямым слагаемым.

10.1.1. Пример. Пусть

$$\bar{G} = \overline{\sum_p} \mathbb{Z}_p, \quad G = \sum_p \mathbb{Z}_p$$

(суммирование по всем простым p). Очевидно, G — периодическая часть в $\bar{G}$. Покажем, что $\bar{G}/G$ — полная группа и G не выделяется в $\bar{G}$ прямым слагаемым.

Докажем сначала полноту фактор-группы $\bar{G}/G$. Пусть $f \in \bar{G}$, n — целое положительное число. Поскольку при $p > n$ в группе $\mathbb{Z}_p$ существует элемент g_p с условием $ng_p = f(p)$, то $ng = f'$, где

$$g(p) = \begin{cases} 0 & \text{при } p \leqslant n, \\ g_p & \text{при } p > n, \end{cases} \quad f'(p) = \begin{cases} 0 & \text{при } p \leqslant n, \\ f(p) & \text{при } p > n. \end{cases}$$

Но $fG = f'G$, поэтому уравнение $nx = fG$ имеет решение в $\bar{G}/G$.

Теперь допустим, что $\bar{G}$ разлагается в прямую сумму $\bar{G} = G \oplus H$. Из предыдущего ввиду $H \simeq \bar{G}/G$ следует полнота подгруппы H. Таким образом, в подгруппе H при произвольном n должно иметь решение уравнение $nx = h$, $h \in H$. Но если, например, $h(p) \neq 0$, то это уравнение не может иметь решений при $n = p$. Полученное противоречие доказывает наше утверждение относительно $\bar{G}$.

В периодической абелевой группе G совокупность G_p всех p-элементов, т. е. элементов, порядки которых есть степени фиксированного простого числа p, образует подгруппу. Очевидно, G_p — максимальная p-подгруппа в G; она называется также *примарной компонентой* группы G.

10.1.2. Упражнение. Периодическая абелева группа разлагается в прямую сумму своих примарных компонент.

Ввиду 10.1.2 при изучении периодических абелевых групп — по крайней мере в постановке и решении вопроса о разложимости — достаточно рассматривать p-группы. Поэтому в настоящем параграфе мы ограничимся формулировкой и доказательством некоторых предложе-

ний относительно p-групп, хотя соответствующие обобщения на периодические группы можно было бы легко установить.

В связи с теоремой о разложимости конечно порожденной абелевой группы в прямую сумму циклических подгрупп естественно возникает вопрос о существовании такого разложения в произвольной абелевой p-группе без полных подгрупп. В общем случае вопрос решается отрицательно, однако имеются полезные признаки, при выполнении которых абелева p-группа разлагается в прямую сумму циклических подгрупп.

10.1.3. Пример. Пусть $G = \sum_n (a_n)$ — прямая сумма циклических подгрупп (a_n) порядков $|a_n| = p^n$, $n = 1, 2, \ldots$, и $b_n = p^{n-1}a_n$. Положим $N = \text{гр}\,(c_1, \ldots, c_n, \ldots)$, где $c_n = b_n - b_{n+1}$, докажем, что группа $\bar{G} = G/N$ не содержит нетривиальных полных подгрупп и не разлагается в прямую сумму циклических подгрупп.

В самом деле, фактор-группа $\bar{G}/\bar{N}_1$, где $\bar{N}_1 = N_1/N$, $N_1 = (b_1, N)$, по конечной подгруппе $\bar{N}_1$ разлагается в прямую сумму циклических подгрупп $(\bar{a}_n, \bar{N}_1)/\bar{N}_1$, $\bar{a}_n = a_n + N$. Легко показать, что такие группы не имеют отличных от нуля полных подгрупп.

Так как $b_i + N = b_{i+1} + N$, то $p^{n-1}\bar{a}_n = a_1$ и, значит, в группе $\bar{G}$ для произвольного числа n и фиксированного элемента $\bar{a}_1$ решается уравнение $p^n x = \bar{a}_1$. Однако прямые суммы циклических p-групп таким свойством, очевидно, не обладают. Поэтому $\bar{G}$ не может разлагаться в прямую сумму циклических подгрупп.

10.1.4. Упражнение. Абелева группа простого периода p разлагается в прямую сумму циклических подгрупп.

Указание: воспользоваться трансфинитной индукцией или рассмотреть абелеву группу периода p как линейное пространство над полем $GF(p)$ и применить теорему линейной алгебры о разложимости пространства в прямую сумму одномерных подпространств.

10.1.5. Первая теорема Прюфера. *Абелева p-группа конечного периода разлагается в прямую сумму циклических подгрупп.*

Доказательство будем вести индукцией по периоду группы. Ввиду 10.1.4 сразу предполагаем, что

теорема истинна для групп периода $<p^n$, и рассматриваем абелеву группу G периода p^n.

Так как подгруппа pG имеет период p^{n-1}, то по индуктивному предположению она разлагается в прямую сумму циклических подгрупп: $pG = \sum_{i \in I} (a_i)$. Обозначим через x_i решение уравнения $px = a_i$ — которое, разумеется, существует в группе G — и положим $H = (x_i \mid i \in I)$. Заметим, что $H = \sum_{i \in I} (x_i)$ (доказать!). Пусть, далее, B — максимальная подгруппа, пересекающая H по нулю, и пусть $G \neq H + B$. Возьмем элемент $g \in G$, не содержащийся в $H + B$. Из построения подгруппы H видно, что уравнение $px = pg$ имеет в H хотя бы одно решение, например, h. Элемент $g_1 = g - h$ не принадлежит сумме $H + B$ и $pg_1 = 0$. По выбору подгруппы B пересечение $H \cap (g_1, B)$ не равно нулю. Это означает, что некоторый ненулевой элемент $h_1 \in H$ можно представить в виде $h_1 = kg_1 + b_1$, $b_1 \in B_1$, $0 < k < p$. Отсюда, если $sk \equiv 1 \pmod{p}$, то $g_1 = skg_1 = sh_1 - sb_1 \in \in H + B$, что противоречит предположению относительно элемента g_1. Таким образом, $G = H \oplus B$.

Так как подгруппа H по построению, а подгруппа B ввиду 10.1.4 разлагаются в прямые суммы циклических подгрупп, то аналогичным разложением обладает и группа G. Теорема доказана.

Говорят, что элемент $g \neq 0$ абелевой p-группы G имеет в G *конечную высоту* h, если уравнение $p^n x = g$ разрешимо только при $n \leqslant h$. Если уравнение $p^n x = g$ имеет решение при любом n, то высота g считается по определению бесконечной.

В терминах высоты мы сформулируем и докажем еще один достаточный признак разложения абелевой p-группы в прямую сумму циклических подгрупп. Но прежде чем формулировать признак, введем полезное понятие сервантной подгруппы.

Подгруппа A группы G называется *сервантной*, если для произвольного числа n и всякого элемента $a \in A$ из разрешимости уравнения $nx = a$ в группе G следует разрешимость этого уравнения в подгруппе A.

10.1.6. Упражнение. В прямой сумме абелевых групп каждое из слагаемых сервантно.

10.1.7. Упражнение. Периодическая часть абелевой группы G сервантна в G.

10.1.8. Упражнение. Подгруппа A абелевой p-группы G сервантна тогда и только тогда, когда разрешимость произвольного уравнения типа $p^n x = a$, $a \in A$, в группе G влечет разрешимость этого уравнения в A.

10.1.9. Упражнение. В абелевой группе G с условием $nG = 0$ подгруппа A сервантна тогда и только тогда, когда для всякого делителя m числа n и любого $a \in A$ разрешимость уравнения $mx = a$ в G влечет разрешимость этого уравнения в подгруппе A.

10.1.10. Упражнение. Пусть сервантная подгруппа A абелевой группы G определяет циклическую фактор-группу $G/A = (g + A)$. Тогда в смежном классе $g + A$ существует такой элемент g_1, что $| g_1 | = | G/A |$.

10.1.11. Упражнение. Если фактор-группа абелевой группы G по сервантной подгруппе A разлагается в прямую сумму циклических подгрупп, то A выделяется в G прямым слагаемым.

Указание: использовать упражнение 10.1.10.

10.1.12. Теорема (Прюфер — Л. Я. Куликов). *Если сервантная подгруппа A абелевой группы G имеет конечный период, то она выделяется в G прямым слагаемым.*

Доказательство. Согласно условию $nA = 0$ для некоторого числа $n \neq 0$. Отсюда и из сервантности A следует $A \cap nG = 0$.

Докажем сервантность подгруппы B/nG, где $B = A + nG$, в фактор-группе G/nG. Для этого предположим, что уравнение $mx = a + nG$, $a \in A$, имеет в G/nG решение $g + nG$. Ввиду 10.1.9 число m можно считать делителем n, $n = mm_1$.

Из соотношения $m(g + nG) = a + nG$ вытекает равенство $mg = a + ng_1$ и, значит, $a = m(g - m_1 g_1)$. Отсюда и из сервантности A следует существование в A такого элемента a_1, что $a = ma_1$. Но тогда элемент $a_1 + nG$ удовлетворяет уравнению $mx = a + nG$.

Так как B/nG сервантна в G/nG, а фактор-группа группы G/nG по B/nG по первой теореме Прюфера разлагается в прямую сумму циклических подгрупп, то согласно 10.1.11 подгруппа B/nG выделяется прямым слагае-

мым, $G/nG = B/nG \oplus C/nG$. Отсюда $G = A \oplus C$, что и требовалось доказать.

10.1.13. Следствие. *Если периодическая часть T абелевой группы G имеет конечный период, то T служит для G прямым слагаемым.*

10.1.14. Вторая теорема Прюфера. *Счетная абелева p-группа G без элементов бесконечной высоты разлагается в прямую сумму циклических подгрупп.*

Доказательство. Ввиду счетности G нижний слой $A = \{g \in G \mid pg = 0\}$ также счетен, и поэтому существует такая последовательность подгрупп

$$0 = A_0 < A_1 < \ldots < A_n < \ldots,$$

что $\bigcup\limits_n A_n = A$ и $|A_{n+1} : A_n| = p$.

Пусть $A_1 = (a_1)$ и b_1 — решение уравнения $p^{h_1}x = a_1$, где h_1 — высота элемента a_1. Как легко заметить, подгруппа (b_1) сервантна в G и, следовательно, G разлагается в прямую сумму $G = (b_1) \oplus B_1$. Очевидно, $A_2 = A_1 + (A_2 \cap B_1)$ и высота h_2 ненулевого элемента $a_2 \in A_2 \cap B_1$ в G совпадает с высотой этого элемента в подгруппе B_1.

Обозначим через $b_2 \in B_1$ решение уравнения $p^{h_2}x = a_2$. Как и прежде, существует прямое разложение $B_1 = (b_2) \oplus B_2$, причем $G = (b_1) \oplus (b_2) \oplus B_2$.

Продолжая аналогично процесс построения подгрупп (b_n) и B_n, получим прямую сумму $C = (b_1) \oplus (b_2) \oplus \ldots$ и последовательность подгрупп $B_1 > B_2 > \ldots$, такие, что $G = (b_1) \oplus \ldots \oplus (b_n) \oplus B_n$ и $B_2 \cap A_n = 0$.

Докажем, что $G = C$. Пусть $g \in G$, $|g| = p^m$. Выберем n, для которого $p^{m-1}g \in A_n$. Пусть $g = c + b$, $c \in (b_1) + \ldots + (b_n)$, $b \in B_n$. Так как $p^{m-1}b \in A_n \cap B_n = 0$, то $|b| < |g|$ и, значит, можно считать уже доказанным, что $b \in C$. Но тогда и $g \in C$. Теорема доказана.

Отказаться от условия счетности во второй теореме Прюфера нельзя, как показывает следующий

10.1.15. Пример. Пусть p — простое число, $G = \sum\limits_n \mathbb{Z}_{p^n}$, T — периодическая часть группы G. Очевидно, T является p-группой без элементов бесконечной высоты и имеет мощность континуума. Докажем, что T не разлагается в прямую сумму циклических подгрупп. Пусть,

напротив, $T = \sum_{i \in I} (a_i)$. Ввиду несчетности T найдется такое бесконечное подмножество $I_1 \subseteq I$, что порядки элементов подгруппы $A = \sum_{i \in I_1} (a_i)$ ограничены в совокупности — скажем, числом p^k. Так как A в группе T выделяется прямым слагаемым, то высоты ненулевых элементов подгруппы A в группе T не превосходят k. Пусть b_n — порождающий элемент группы $\mathbb{Z}_{p^n}$. Для любого $f \in A$

$$f(n) \in (p^{n-k} b_n) \text{ при } n \geqslant k.$$

Так как компоненты функций f в прямом слагаемом $\mathbb{Z}_{p^n}$ принимают только конечное множество значений, а подгруппа A бесконечна, то в A найдутся такие различные элементы f_1, f_2, что $f_1(n) = f_2(n)$ при $1 \leqslant n \leqslant 2k$. Их разность $f = f_1 - f_2$ отлична от нуля, лежит в A и имеет в T высоту, большую k. Но это противоречит построению A.

Отметим, что весьма нетривиальные аналоги теорем Прюфера для локально нормальных групп установили Ю. М. Горчаков и Ф. Холл (см. [8]).

Изучим в заключение, как устроены периодические абелевы группы конечного ранга. Учитывая упражнение 2.3.4, достаточно рассмотреть только примарные группы, а для них полное описание дает следующая

10.1.16. Т е о р е м а. *Примарная абелева группа тогда и только тогда имеет конечный ранг r, когда она разлагается в прямую сумму r квазициклических и конечных циклических групп.*

Д о к а з а т е л ь с т в о. Так как циклические и квазициклические группы имеют ранг 1, то утверждение «тогда» очевидно (с учетом 4.1.7). Обратно, пусть G — абелева p-группа конечного ранга r. Ввиду 9.1.10 достаточно рассмотреть следующие два случая.

1. Группа G полна. Тогда по теореме 9.1.16 она должна быть прямой суммой квазициклических групп. Понятно, что число слагаемых не может быть больше r.

2. Группа G редуцирована. Покажем, что G счетна и не содержит элементов бесконечной высоты, тогда останется сослаться на вторую теорему Прюфера 10.1.14. Прежде всего для каждого $k = 1, 2, \ldots$ группа G со-

держит лишь конечное число элементов, удовлетворяющих уравнению $p^k x = 0$ (учесть первую теорему Прюфера и конечность ранга группы), поэтому G счетна. Далее, допустим, что G содержит ненулевой элемент a бесконечной высоты; пусть p^m — его порядок. Возьмем в G для каждого $k = 1, 2, \ldots$ по элементу x_k с условием $p^k x_k = a$. Так как элементы $p^{k-1}x_k$, $k = 1, 2, \ldots$, имеют один и тот же порядок p^{m+1}, то, по предыдущему, среди них найдется бесконечная подпоследовательность совпадающих друг с другом; обозначим этот элемент a_1. Очевидно, $pa_1 = a$ и, по построению, a_1 тоже имеет бесконечную высоту. Продолжая построение по индукции, получим элементы $a = a_0, a_1, a_2, \ldots$ с условием $pa_{i+1} = a_i$, $i = 0, 1, 2, \ldots$ Ясно, что порожденная ими подгруппа полна,— противоречие с редуцированностью группы G.

Глава 4

КОНЕЧНЫЕ ГРУППЫ

§ 11. Силовские подгруппы

Изучая абелевы группы, мы видели, что их строение во многом определяется строением максимальных p-подгрупп. В теории конечных групп максимальные p-подгруппы также играют существенную роль. В этом параграфе мы докажем следующую теорему Силова о конечных группах: для каждой степени p^α, делящей порядок группы, существует подгруппа порядка p^α, причем если $p^{\alpha+1}$ делит порядок группы, то всякая подгруппа порядка p^α содержится в некоторой подгруппе порядка $p^{\alpha+1}$; все максимальные p-подгруппы попарно сопряжены в группе, а их число сравнимо с 1 по модулю p. Эта теорема, доказанная норвежским математиком Л. Силовом в 1872 году, явилась краеугольным камнем теории конечных групп. Она неоднократно обобщалась в разных направлениях как в нашей стране (С. А. Чунихин и др.), так и за рубежом (Ф. Холл и др.). В связи с этой теоремой и в честь ее автора максимальные p-подгруппы конечных (а часто и бесконечных) групп называются *силовскими p-подгруппами*.

Из теоремы Силова вытекает, в частности, что силовские p-подгруппы конечной группы — это в точности подгруппы порядка p^r, где p^r — максимальная степень p, делящая порядок группы. Отметим, что если число m делит порядок конечной группы G, но не является степенью простого числа, то в G может и не быть подгрупп порядка m — например, в знакопеременной группе A_4 порядка 12 нет подгрупп порядка 6, см. упражнение 11.2.2.

11.1. Теорема Силова. В доказательстве этой теоремы нам понадобится понятие действия. Говорят, что *группа G действует на множестве M*, если для каждых элементов $m \in M$, $g \in G$ определен элемент $mg \in M$, причем $(mg_1)\,g_2 = m\,(g_1g_2)$ и $me = m$ для всех $m \in M$, $g_1, g_2 \in G$; здесь e — единица группы G. Множество $mG = \{mg \mid g \in$

$\in G\}$ называется *орбитой* элемента m. Очевидно, орбиты любых двух элементов из M либо совпадают, либо не пересекаются, так что множество M разбивается на непересекающиеся орбиты.

11.1.1. Теорема (Силов). *Пусть G — конечная группа, p — простое число. Существование. Для каждой степени p^α, делящей порядок G, в G существует подгруппа порядка p^α. Вложение. Если $p^{\alpha+1}$ делит порядок G, то каждая подгруппа порядка p^α из G вложена в некоторую подгруппу порядка $p^{\alpha+1}$ из G. В частности, силовские p-подгруппы из G — это в точности подгруппы порядка p^r, где p^r — максимальная степень p, делящая порядок G. Сопряженность. Все силовские p-подгруппы из G сопряжены в G. Количество. Количество силовских p-подгрупп из G сравнимо с 1 по модулю p и делит порядок G.*

Доказательство. Существование. Пусть $|G| = p^r l$, $(p, l) = 1$. Пусть $\mathfrak{M}$ — множество всех подмножеств мощности p^α из G. Очевидно,

$$|\mathfrak{M}| = \binom{p^r l}{p^\alpha} = p^{r-\alpha} l \prod_{j=1}^{p^\alpha - 1} \frac{p^r l - j}{j},$$

поэтому наибольшая степень p, делящая $|\mathfrak{M}|$, — это $p^{r-\alpha}$. Если $M \in \mathfrak{M}$, $g \in G$, то, очевидно, $Mg = \{mg \mid m \in M\} \in \mathfrak{M}$, так что G действует на $\mathfrak{M}$ правыми сдвигами. Пусть $\{M_1, \ldots, M_s\}$ — та орбита, мощность s которой не делится на $p^{r-\alpha+1}$. Пусть, далее,

$$G_i = \{g \mid g \in G,\ M_1 g = M_i\},\ 1 \leqslant i \leqslant s.$$

Непосредственно проверяется, что G_1 — подгруппа в G, а G_i — правые смежные классы G по G_1. Покажем, что подгруппа G_1 имеет требуемый порядок p^α. Обозначим пока $|G_1| = t$, тогда по теореме Лагранжа 2.4.5 $st = |G| = p^r l$. Так как наибольшая степень p, делящая s, — это $p^{r-\alpha}$, то t делится на p^α, в частности, $t \geqslant p^\alpha$. С другой стороны, если $x \in M_1$, то, очевидно, $xG_1 \subseteq M_1$, поэтому $|G_1| \leqslant |M_1|$ или $t \leqslant p^\alpha$. Окончательно $t = p^\alpha$.

Вложение. Пусть $p^{\alpha+1}$ делит $|G|$, P — подгруппа порядка p^α из G, $\mathfrak{C}$ — класс подгрупп, сопряженных

с P элементами из G. Мы знаем, что

$$| \mathfrak{C} | = | G : N_G(P) |.$$

Если $| \mathfrak{C} |$ не делится на p, то $| N_G(P) |$ делится на $p^{\alpha+1}$, а потому по первой части теоремы в $N_G(P)/P$ существует подгруппа P^*/P порядка p. Тогда P^* — требуемая подгруппа P. Пусть теперь $| \mathfrak{C} |$ делится на p. Группа P действует на $\mathfrak{C}$ сопряжениями, причем мощности орбит делят $| P |$, а потому имеют вид p^{α_i}, $\alpha_i \geqslant 0$. Так как имеется по крайней мере одна одноэлементная орбита $\{P\}$ и $| \mathfrak{C} |$ делится на p, то непременно найдется и другая одноэлементная орбита $\{Q\}$. Но это означает, что P нормализует Q, поэтому PQ есть p-подгруппа (учесть, что $PQ/Q \simeq P/P \cap Q$ и расширение p-подгруппы посредством p-подгруппы есть p-подгруппа). Применяя к PQ тот внутренний автоморфизм группы G, который переводит Q в P, мы получим p-подгруппу $P'P$, содержащую P в качестве собственной нормальной подгруппы. Снова по первой части теоремы в $P'P/P$ найдется подгруппа P^*/P порядка p, тогда P^* — требуемая подгруппа.

Из доказанного утверждения вытекает, что силовские p-подгруппы конечной группы — это в точности подгруппы порядка p^r, где p^r — максимальная степень p, делящая порядок группы.

Сопряженность. Теперь пусть P — подгруппа порядка p^r из G (в частности, это силовская p-подгруппа), а $\mathfrak{C}$ имеет прежний смысл. Надо доказать, что любая силовская p-подгруппа Q из G лежит в $\mathfrak{C}$. Но Q действует на $\mathfrak{C}$ сопряжениями, причем орбиты имеют снова мощности p^{α_i}, $\alpha_i \geqslant 0$. Так как теперь $| \mathfrak{C} |$ заведомо не делится на p, то имеется некоторая одноэлементная орбита $\{P'\}$, т. е. Q нормализует P'. Тогда $P'Q$ есть p-подгруппа, и ввиду максимальности P', Q имеем $Q = P'Q = P' \in \mathfrak{C}$.

Количество. В обозначениях предыдущего пункта достаточно проверить, что $\{Q\}$ — единственная одноэлементная орбита. Но если $\{Q'\}$ — другая такая орбита, то QQ' является p-подгруппой, отличной от Q, что невозможно. Теорема доказана.

Отметим, что иногда говорят не об одной, а о трех теоремах Силова: утверждения о существовании и вложении называются первой теоремой, о сопряженности —

второй, а о количестве силовских p-подгрупп — третьей теоремой Силова.

11.1.2. Упражнение. Группа порядка 196 содержит нормальную силовскую p-подгруппу.

11.1.3. Упражнение. Силовские p-подгруппы бесконечной группы не всегда сопряжены в группе, т. е. предположение конечности в теореме Силова существенно.

Указание: рассмотреть прямую степень группы S_3.

11.1.4. Упражнение. Пусть P — силовская p-подгруппа конечной группы G, H — подгруппа, содержащая нормализатор $N_G(P)$. Тогда $N_G(H) = H$.

11.2. Применение к группам порядка pq. Теорема Силова часто дает весьма существенную информацию о данной конечной группе, а группы не очень большие — в том или ином смысле — позволяет описать полностью. В качестве иллюстрации дадим здесь описание групп порядка pq.

Пусть p, q — простые числа, $p < q$. Какой должна быть группа G порядка pq? Силовские p- и q-подгруппы из G, будучи подгруппами простого порядка, являются циклическими. Пусть (a), (b) — соответственно силовские p- и q-подгруппа. По теореме Силова число силовских q-подгрупп в G имеет вид $1 + kq$ и делит pq, поэтому силовская q-подгруппа (b) единственна. В частности, она нормальна в G. Число силовских p-подгрупп имеет вид $1 + kp$ и делит q, поэтому возможны два случая:

а) Силовская p-подгруппа (a) единственна. Тогда она нормальна и, значит, $[a, b] \in (a) \cap (b) = 1$. Так как $(ab)^{pq} = a^{pq}b^{pq} = 1$, то $G = (ab)$. Таким образом, в этом случае $G \simeq \mathbb{Z}_{pq}$.

б) Имеется q силовских p-подгрупп. Конечно, это возможно лишь при условии $q \equiv 1 \pmod{p}$. Пусть $a^{-1}ba = b^r$. Если $r = 1$, то снова $G = (ab)$, т. е. $G \simeq \mathbb{Z}_{pq}$. Пусть $r \neq 1$. Индукцией по x получаем $a^{-x}ba^x = b^{r^x}$, откуда

$$a^{-x}b^ya^x = b^{r^xy}$$

для всех целых x, y. При $x = p$, $y = 1$ это дает $r^p \equiv 1 \pmod{q}$, кроме того, получаем формулу умножения

$$a^xb^y \cdot a^zb^t = a^{x+z}b^{y^{r^z}+t}. \tag{1}$$

Обратно, легко проверить, что если $q \equiv 1 \pmod{p}$, $r^p \equiv$

$\equiv 1 \pmod q$, $r \not\equiv 1 \pmod q$, то эта формула умножения определяет неабелеву группу порядка pq. Наконец, решения сравнения $r^p \equiv 1 \pmod q$ составляют циклическую группу порядка p, поэтому те из них, которые $\not\equiv 1 \pmod q$, имеют вид $r, r^2, \ldots, r^{p-1}$, где r — одно из них. Все эти решения определяют одну и ту же группу, так как замена порождающего a на a^j приводит к замене r на r^j.

Таким образом, с помощью теоремы Силова мы описали все возможные типы групп порядка pq; их оказалось два — абелев и неабелев, причем второй существует только при условии $q \equiv 1 \pmod p$.

11.2.1. Упражнение. Существуют только две неизоморфные группы из 6 элементов — циклическая $\mathbb{Z}_6$ и симметрическая S_3.

11.2.2. Упражнение. Знакопеременная группа A_4 не содержит подгрупп порядка 6, хотя число 6 делит ее порядок 12. Таким образом, теорему Лагранжа 2.4.5 нельзя обратить — факт, упоминавшийся в начале параграфа.

Решение. Если бы подгруппа из 6 элементов содержалась в A_4, то она была бы изоморфна $\mathbb{Z}_6$ или S_3 (упражнение 11.2.1). Но никакая подстановка на 4 символах не может быть порядка 6, поэтому первый случай невозможен. Невозможен и второй, так как в S_3 существуют неперестановочные элементы порядка 2, а в A_4 их нет. В самом деле, A_4 содержит три элемента порядка 2: (12) (34), (13) (24), (14) (23), и все они попарно перестановочны.

11.3. Примеры силовских подгрупп. Обратимся к группам I—IV гл. 1.

11.3.1. Примеры. I. Аддитивная группа кольца вычетов $\mathbb{Z}_n$ разлагается в прямое произведение своих силовских p-подгрупп, которые являются циклическими подгруппами порядков $p_1^{m_1}, \ldots, p_s^{m_s}$, если n имеет каноническое разложение $n = p_1^{m_1} \ldots p_s^{m_s}$.

II. Силовская p-подгруппа мультипликативной группы $\mathbb{C}^*$ — это квазициклическая группа $\mathbb{C}_{p^\infty}$.

III. Опишем силовские p-подгруппы симметрических групп. Как мы знаем, $|S_n| = n!$ Каков максимальный показатель $e(n)$, при котором $p^{e(n)}$ делит $n!$? В последовательности $1, 2, \ldots, n$ кратными p будут числа $p, 2p, \ldots$

..., kp, где $k = \left[\frac{n}{p}\right]$, поэтому $e(n) = \left[\frac{n}{p}\right] + e(k)$. Так как $\left[\frac{k}{p}\right] = \left[\frac{n}{p^2}\right]$, то $e(n) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \ldots$ Удобно разложить n по основанию p:

$$n = a_0 + a_1 p + \ldots + a_s p^s, \quad 0 \leqslant a_i < p, \tag{2}$$

тогда

$$e(n) = a_1 + a_2(1 + p) + a_3(1 + p + p^2) + \ldots \\ \ldots + a_s(1 + p + \ldots + p^{s-1}). \tag{3}$$

Рассмотрим сначала группы S_n, когда n — степень p. Пусть в S_{p^m} уже найдена силовская p-подгруппа, т. е. подгруппа H_m порядка $p^{1+\ldots+p^{m-1}}$; построим по ней в $S_{p^{m+1}}$ подгруппу H_{m+1} порядка $p^{1+\ldots+p^m}$. Для этого разобьем переставляемые символы $1, 2, \ldots, p^{m+1}$ на последовательные отрезки длины p^m. Если

$$c = \prod_{j=1}^{p^m} (j, p^m + j, 2p^m + j, \ldots, (p-1)p^m + j)$$

и x — подстановка на символах i-го отрезка, то легко сообразить, что $c^{-1}xc$ — подстановка на символах $(i+1)$-го отрезка (сложение по модулю p). Отсюда видно, что подгруппа, порожденная подгруппами $c^{-r}H_m c^r$, $0 \leqslant r < p$, является их прямым произведением и, стало быть, подгруппа H_{m+1}, порожденная подгруппой H_m и элементом c, изоморфна сплетению $H_m \wr (c)$. Подгруппа H_{m+1} — искомая, так как

$$|H_{m+1}| = |H_m|^p \cdot |c| = p^{1+\ldots+p^m}.$$

Одновременно мы видим, что силовская p-подгруппа в S_{p^m} изоморфна последовательному сплетению $(\ldots(\mathbb{Z}_p \wr \mathbb{Z}_p) \wr \ldots \ldots) \wr \mathbb{Z}_p$ циклической группы $\mathbb{Z}_p$ с самой собою m раз.

Теперь пусть n произвольно. Разобьем символы $1, \ldots \ldots, n$ на a_0 одноэлементных, a_1 p-элементных и т. д. отрезков (см. (2)). На каждом из этих отрезков рассмотрим симметрическую группу — она будет некоторой степени p^m, а в ней возьмем силовскую p-подгруппу, построенную как выше. Так как эти подгруппы действуют на непересекающихся множествах, то их порождение P_n является

их прямым произведением, а потому имеет порядок

$$|P_n| = \prod_{m=1}^{s} (p^{1+p+\ldots+p^{m-1}})^{a_m} = p^{e(n)}$$

(см. (3)). Следовательно, P_n — силовская p-подгруппа в S_n. Из построения видно, что она изоморфна прямому произведению нескольких последовательных сплетений типа $(\ldots(\mathbb{Z}_p \wr \mathbb{Z}_p) \wr \ldots) \wr \mathbb{Z}_p$.

IV. Рассмотрим, наконец, общие линейные группы над конечными полями. Пусть p — простое число, m, n — целые числа $\geqslant 1$ и $q = p^m$. Покажем, что $UT_n(q)$ — силовская p-подгруппа группы $GL_n(q)$. Подсчитаем порядки этих групп.

Какие n-ки над полем $GF(q)$ могут быть первой строкой невырожденной матрицы? Очевидно, любые, кроме нулевой, т. е. $q^n - 1$ штук. Если первая строка выбрана, то в качестве второй строки можно взять любую, не пропорциональную первой; таких строк $q^n - q$. Если две первые строки уже выбраны, то в качестве третьей можно взять любую строку, не зависящую линейно от первых двух; это дает $q^n - q^2$ возможностей. И так далее. Значит,

$$|GL_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i). \tag{4}$$

Так как угловые элементы матриц из $UT_n(q)$ пробегают независимо друг от друга всё поле, а всего угловых мест $\binom{n}{2}$, то $|UT_n(q)| = q^{\binom{n}{2}}$. Из сравнения порядков мы видим, что $UT_n(q)$ — силовская p-подгруппа в $GL_n(q)$.

11.3.2. Упражнение. Выписать подстановки, составляющие силовскую 2-подгруппу группы S_4.

11.3.3. Упражнение. Пусть p — простое число, m, n — натуральные числа, $P_n(\mathbb{Z}_{p^m})$ — совокупность тех матриц из $GL_n(\mathbb{Z}_{p^m})$, коэффициенты которых, стоящие под главной диагональю, кратны p, а на диагонали — сравнимы с 1 по модулю p. Проверить, что $P_n(\mathbb{Z}_{p^m})$ — силовская p-подгруппа в $GL_n(\mathbb{Z}_{p^m})$.

Указание: с помощью гомоморфизма $GL_n(\mathbb{Z}_{p^m}) \to GL_n(\mathbb{Z}_p)$ вывести формулу

$$|GL_n(\mathbb{Z}_{p^m})| = \prod_{i=0}^{n-1} (p^{mn} - p^{mn-n+i}). \qquad (5)$$

В заключение отметим в виде упражнений несколько общих замечаний.

11.3.4. Упражнение. Пусть φ — гомоморфизм конечной группы G. Если P — силовская p-подгруппа из G, то P^φ — силовская p-подгруппа из G^φ. Обратно, всякая силовская p-подгруппа из G^φ является образом некоторой силовской p-подгруппы из G. Это замечание бывает полезно в индуктивных доказательствах.

11.3.5. Упражнение. Произведение двух элементов порядка p может иметь как конечный порядок, не делящийся на p, так и бесконечный порядок. Таким образом, элементы порядков p^α при данном p не всегда составляют подгруппу.

11.3.6. Упражнение. Пусть G — конечная группа и $A \leqslant G$. Если индекс $|G : A|$ меньше некоторого простого делителя p порядка группы G, то пересечение $\bigcap A^g$, $g \in G$, содержит силовские p-подгруппы группы G и, в частности, отлично от единицы.

§ 12. Группы подстановок

Рассмотрим более подробно группы подстановок — важный и исторически первый пример групп. Они были введены в науку Эваристом Галуа для изучения условий разрешимости алгебраических уравнений в радикалах — с каждым алгебраическим уравнением он связал некоторую группу подстановок корней, полицикличность которой оказалась необходимым и достаточным условием разрешимости уравнения в радикалах. В 1870 году появился фундаментальный трактат Жордана о группах подстановок, содержащий ясное и подробное изложение идей Галуа, а также многочисленные свойства подстановок. Лишь к началу XX в. современное абстрактное понятие группы освободилось от этих пелёнок, а группы подстановок постепенно заняли их нынешнее скромное положение в общей теории. Вообще, группы подстановок есте-

ственно возникают всюду, где изучается симметрия «конечно определенных» объектов — например, с каждым кристаллом можно связать группу его вращений, записываемых подстановками вершин. Детальнее с группами подстановок можно познакомиться по книге [46].

12.1. Регулярное представление. Оказывается, подстановки дают исчерпывающий пример конечных групп.

12.1.1. Теорема (Кэли). *Всякая конечная группа изоморфна некоторой группе подстановок.*

Доказательство. Пусть G — конечная группа, которую мы хотим изобразить подстановками. Подстановками чего, какого множества?— вот первый вопрос, который возникает. Возьмем в качестве этого множества саму G, поскольку ничем другим мы не располагаем. Пусть g — элемент из G. Какую подстановку $\hat{g}$ ему сопоставить? Ее первая строка уже выбрана — это элементы из G, как-нибудь занумерованные. Умножим их справа на g и запишем полученные элементы во вторую строчку. Из групповых аксиом следует, что элементы второй строчки попарно различны, так что $\hat{g}$ — действительно подстановка. Остается проверить, что отображение $\hat{}$ является изоморфизмом. Но, во-первых, это гомоморфизм, т. е.

$$\widehat{ab} = \hat{a}\hat{b} \text{ для всех } a, b \in G.$$

Действительно, на каждый элемент $x \in G$ обе части равенства действуют одинаково:

$$x\widehat{ab} = x(ab) = (xa)\,b = (x\hat{a})\,\hat{b} = x(\hat{a}\hat{b}).$$

Во-вторых, ядро отображения $\hat{}$ тривиально: если $\hat{g} = 1$, то подстановка $\hat{g}$ переводит символ 1, с одной стороны, в g, а с другой — оставляет на месте, поэтому $g = 1$. Теорема доказана.

12.1.2. Упражнение. Всякая конечная группа вкладывается в знакопеременную группу.

Если в доказательстве теоремы Кэли не предполагать, что группа G конечна, то с помощью того же представления правыми сдвигами — оно называется *регулярным представлением* группы G — получается

12.1.3. Обобщенная теорема Кэли. *Всякая группа изоморфна группе взаимно однозначных отображений — «бесконечных подстановок» — некоторого множества на себя.*

Представление абстрактных групп подстановками бывает полезно в самых различных вопросах, и не только в теории конечных групп.

12.1.4. Пример. О теоремах вложения. Часто возникает потребность вложить данную группу G в некоторую бо́льшую группу G^* с тем или иным интересным свойством,— например, с одним из следующих свойств:

а) G^* — простая группа,

б) в G^* из каждого элемента извлекаются корни произвольной степени, т. е. уравнение $x^n = g$ разрешимо в G^* для любого g из G^* и любого натурального n,

в) любые два элемента из G^*, имеющие одинаковый — конечный или бесконечный — порядок, сопряжены в G^*.

Читатель без труда увеличит этот список, руководствуясь своим собственным пониманием интересного.

В двух совместных работах авторов и В. Н. Ремесленникова (ДАН СССР, 1960, **134**, № 3, с. 518—520; Уч. зап. Пермского ун-та, 1960, **17**, № 2, с. 9—11) был предложен путь доказательства теорем вложения, состоящий в том, что группа, предварительно представленная подстановками, вкладывается в группу подстановок, в некоторой мере уже обладающую требуемым свойством (простотой, корнями, сопрягающими элементами и т. п.), после чего дело завершает индукция, иногда трансфинитная. Такой путь удобен тем, что конкретное представление абстрактной группы подстановками конкретизирует — и тем самым облегчает — вычисления. В качестве иллюстрации укажем вложение произвольной группы G в группу G^* со свойством в). Для этого определим по индукции цепочку групп $G = G_0 \leqslant G_1 \leqslant \ldots$. Именно, если G_n уже построена, то возьмем в качестве G_{n+1} группу преобразований множества G_n, а вложение $G_n \leqslant G_{n+1}$ определим как регулярное представление группы G_n. Объединение G^* групп G_n и будет искомым. В самом деле, если a, b — два элемента одинакового порядка $r \leqslant \infty$ из G^*, то они лежат в некоторой G_n, а потому в G_{n+1} изображаются произведениями независимых циклов длины r. Согласно 2.5.7 элементы a, b сопряжены в G_{n+1}, а потому и в G^*.

Аналогично, если мы хотим вложить G в группу G^* со свойством б), то достаточно научиться вкладывать G в такую группу, в которой уравнение $x^n = g$ для данных

n, $g \in G$ было бы разрешимо. Один способ такого вложения указан — на языке подстановок — в упомянутых выше работах, что и решает задачу.

Наконец, задача а) тоже решается положительно, как мы увидим в следующем параграфе.

Возникает вопрос — нельзя ли произвольную группу вложить в такую группу G^*, которая обладала бы свойствами а), б) и т. п. одновременно? Разумеется, ответ будет утвердительный, если можно построить G^* с каждым из этих свойств в отдельности и если эти свойства переносятся на объединения возрастающих цепочек групп — для доказательства достаточно периодически повторить вложения типов а), б), в), . . . счетное число раз и перейти к объединению.

Отметим, что другие методы доказательства теорем вложения — в частности, для отмеченных выше свойств а), б), в) — указали также Ф. Холл (Hall P. — J. London Math. Soc., 1959, **34**, p. 305—319) и Б. Нойман (Neumann B. H.— J. London Math. Soc., 1943, 18, p. 4—11); метод первого основан на сплетениях, а второго — на свободных произведениях с объединенной подгруппой.

12.2. Представления подстановками смежных классов. Обобщим теперь теорему Кэли в другом направлении. Пусть H — подгруппа конечного индекса группы G, не обязательно конечной. Каждому элементу g из G сопоставим подстановку $\hat{g}$ множества правых смежных классов G по H, определяемую по аналогии с п. 12.1. Именно, если $x_1, \ldots, x_m$ — правые представители G по H, то полагаем

$$\hat{g} = \begin{pmatrix} Hx_1 & \ldots & Hx_m \\ Hx_1g & \ldots & Hx_mg \end{pmatrix}.$$

12.2.1. Теорема. *Отображение* $\hat{}$, *задаваемое последней формулой, является гомоморфным представлением группы G. Ядром этого представления служит нормальная подгруппа N из G, максимальная среди содержащихся в H.*

Доказательство. То, что $\hat{}$ — представление, легко проверяется непосредственно, как и раньше. Пусть K — ядро этого представления. Покажем, что $K \leqslant N$. Пусть $g \in K$, т. е. $\hat{g} = 1$. Это означает, что $Hxg = Hx$

для всех $x \in G$. Отсюда $H^x g = H^x$ и, следовательно,

$$g \in \bigcap_{x \in G} H^x.$$

Ясно, что правая часть этого включения — нормальная подгруппа из G, содержащаяся в H. Ясно также, что любая другая такая же подгруппа содержится в каждом H^x, поэтому

$$N = \bigcap_{x \in G} H^x.$$

Таким образом, $g \in N$ и $K \leqslant N$. Обратно, $N \leqslant K$. Действительно, пусть $g \in N$. Тогда $Hxg = Hxgx^{-1}x = Hx$, откуда $\hat{g} = 1$ и $N \leqslant K$. Теорема доказана.

Из нее и теоремы Лагранжа 2.4.5 сразу вытекает

12.2.2. Т е о р е м а. *Всякая подгруппа конечного индекса m содержит нормальную подгруппу конечного индекса, делящегося на m и делящего $m!$.*

Более слабое утверждение уже отмечалось в первой главе (см. 2.5.13). Теорема 12.2.1 и вытекающая из нее теорема 12.2.2 позволяют устанавливать отсутствие подгрупп того или иного порядка в данной группе — см. упражнение 13.1.3 в следующем параграфе.

12.2.3. У п р а ж н е н и е. Группа из 12 элементов не может быть простой.

Пусть R — кольцо, H — группа. *Групповым кольцом* группы H над R называется кольцо $R[H]$ формальных линейных комбинаций

$$r_1 h_1 + \ldots + r_n h_n, \qquad r_i \in R,\ h_i \in H,$$

которые складываются и умножаются по следующим правилам:

$$\sum r_i h_i + \sum s_i h_i = \sum (r_i + s_i) h_i,$$
$$\sum r_i h_i \cdot \sum s_j f_j = \sum r_i s_j h_i f_j$$

(аналогичный объект встречался нам на стр. 43).

Вернемся теперь к началу пункта и заметим, что представление $g \mapsto \hat{g}$ связывает с каждым g из G «перестановку представителей» $\pi(g)$ и «дополнительные множители» $h_i(g)$:

$$Hx_i g = Hx_{i\pi(g)}, \quad x_i g = h_i(g)\, x_{i\pi(g)}.$$

Непосредственно проверяется, что формула

$$g \mapsto \operatorname{diag}(h_1(g), \ldots, h_m(g)) \cdot \pi(g)$$

задает изоморфное вложение $G \to \boldsymbol{GL}_m(\mathbb{Z}[H])$, где $\mathbb{Z}[H]$ — целочисленное групповое кольцо группы H, а перестановка $\pi(g)$ записана матрицей из нулей и единиц. Это вложение называется *мономиальным представлением группы G над подгруппой H*. Мы видим, что любая группа, содержащая H в качестве подгруппы индекса m, вкладывается в группу всевозможных матриц степени m над $\mathbb{Z}[H]$, содержащих в каждой строке и каждом столбце точно один ненулевой элемент, лежащий в H (*мономиальная подгруппа* группы $\boldsymbol{GL}_m(\mathbb{Z}[H])$). Описанная конструкция особенно употребительна в теории линейных представлений конечных групп, где она дает представление группы, индуцированное представлением подгруппы.

Сказанное можно следующим образом перевести на язык сплетений.

Пусть A, B — группы, причем $B \leqslant \boldsymbol{S}(X)$, X — некоторое множество. Легко проверить, что множество $B \cdot \operatorname{Fun}(X, A)$ с умножением

$$bf \cdot b'f' = bb'f^{b'}f', \text{ где } f^b(x) = f(xb^{-1}),\ x \in X,$$

является группой. Она называется *сплетением группы A с группой подстановок B*. Наиболее важный случай этого понятия — сплетение, рассмотренное в гл. 2, оно называется *стандартным* и получается, если B представить подстановками самой себя по правилу $x \mapsto b^{-1}x$. Употребляя для сплетений прежнюю символику, мы видим, что мономиальная подгруппа из $\boldsymbol{GL}_m(\mathbb{Z}[H])$ — это в точности $H \wr \boldsymbol{S}_m$, а теорема 6.2.8 констатирует описанную выше ситуацию для стандартных сплетений.

12.3. Транзитивность. Примитивность. Здесь мы рассмотрим некоторые понятия, относящиеся к группам подстановок и существенно связанные с их действием на множестве передвигаемых символов. В действительности эти понятия относятся к произвольным группам, действующим на множестве, поэтому мы дадим определения в более общей ситуации, чем необходимо.

Если группа G действует на множестве M и существует всего одна орбита — само M,— то говорят, что G *транзитивна* (на M). Ясно, что это равносильно требованию,

что для любых двух элементов m, m' из M найдется элемент g из G с условием $mg = m'$. Обобщая это понятие, говорят, что группа G *r-кратно транзитивна*, если для любых двух r-ок $\{m_1, \ldots, m_r\}$ и $\{m'_1, \ldots, m'_r\}$ элементов из M найдется элемент g из G с условием $m_i g = m'_i$, $1 \leqslant i \leqslant r$. Разбиение множества M на непересекающиеся подмножества $\{M_\alpha\}$ называется *разбиением на блоки относительно* G, если для каждого M_α и каждого $g \in G$ найдется такое M_β, что $M_\alpha g = M_\beta$, иными словами, если элементы из G переставляют подмножества M_α (*блоки*) целиком. Конечно, всегда существуют тривиальные разбиения — на одноэлементные блоки и на единственный блок. Если нетривиальных разбиений M на блоки не существует, то говорят, что группа G *примитивна*. В частности, все эти понятия распространяются на группы подстановок конечного множества M, рассматриваемые с их естественным действием на M.

12.3.1. Упражнение. Условие $M_\alpha g = M_\beta$ в определении блочного разбиения равносильно более слабому по форме условию $M_\alpha g \subseteq M_\beta$.

12.3.2. Упражнение. Группы S_n, A_n соответственно n- и $(n-2)$-кратно транзитивны.

12.3.3. Упражнение. Всякая дважды транзитивная группа примитивна.

12.3.4. Упражнение. Всякая неединичная нормальная подгруппа N примитивной группы G транзитивна.

Указание: орбиты для N составляют полную систему блоков для G.

Пусть группы G, G' действуют соответственно на множествах M, M'. Естественно называть их *изоморфными* — как группы преобразований,— если можно установить взаимно однозначное отображение M на M' (скажем, φ) и изоморфизм G на G' (скажем, ψ), при которых соответствующие элементы групп переводят соответствующие элементы множеств снова в соответствующие элементы, т. е.

$$m^\varphi g^\psi = (mg)^\varphi \text{ для всех } m \in M,\ g \in G.$$

Изоморфные группы подстановок называют также *подобными*.

В предыдущем пункте с каждой подгруппой конечного индекса мы связали гомоморфное представление группы

подстановками множества смежных классов. Легко видеть, что это представление транзитивно. Оказывается, верно и обратное: всякое транзитивное представление данной группы подстановками подобно некоторому описанному ранее представлению подстановками правых смежных классов по некоторой подгруппе конечного индекса. Именно, справедлива

12.3.5. Т е о р е м а. *Пусть* π — *гомоморфизм группы* G *на транзитивную группу подстановок множества* M. *Будем считать, что* G *действует на* M *по правилу* $mg = mg^{\pi}$. *Пусть* $m_1 \in M$, H — *стабилизатор* m_1 *в* G, *т. е.*

$$H = \{g \mid g \in G,\ m_1 g = m_1\}.$$

Тогда H — *подгруппа конечного индекса в* G *и группа* G^{π} *подобна группе подстановок смежных классов* G *по* H, *описанной в предыдущем пункте.*

Д о к а з а т е л ь с т в о. Пусть $M = \{m_1, \ldots, m_s\}$. Обозначим

$$H_i = \{g \mid g \in G, m_1 g = m_i\},\ 1 \leqslant i \leqslant s.$$

В силу транзитивности G^{π} все H_i непусты. Непосредственно проверяется, что H_1 — подгруппа из G, а H_i — правые смежные классы G по H_1. Так как $H = H_1$, то H — подгруппа конечного индекса в G.

Пусть π' — описанное в предыдущем пункте представление G подстановками правых смежных классов G по H. Нам осталось доказать, что группы подстановок G^{π} и $G^{\pi'}$ подобны. Пусть φ — отображение M на правые смежные классы G по H, переводящее m_i в H_i, а ψ — отображение G^{π} на $G^{\pi'}$, переводящее g^{π} в $g^{\pi'}$. Легко проверить, что если $x^{\pi} = y^{\pi}$, то $x^{\pi'} = y^{\pi'}$, так что отображение ψ определено корректно. Теперь непосредственно проверяется, что φ, ψ — взаимно однозначные отображения *на* и

$$m_i^{\varphi}(g^{\pi})^{\psi} = (m_i g^{\pi})^{\varphi} \quad \text{для} \quad 1 \leqslant i \leqslant s,\ \ g \in G.$$

Теорема доказана.

Покажем, что изучение произвольных групп подстановок сводится в некоторой мере к изучению транзитивных групп, а изучение транзитивных групп — к изучению примитивных. Напомним, что подпрямым произведением групп G_i называется такая подгруппа их прямого про-

изведения, проекция которой на каждый множитель G_i совпадает с G_i.

12.3.6. Теорема. *Всякая группа подстановок на n символах является подпрямым произведением транзитивных групп подстановок на n_i символах с условием $\sum n_i = n$. Если G — транзитивная группа подстановок множества M и задано неизмельчаемое разбиение M на блоки мощности $\geqslant 2$, то стабилизатор блока M' в целом, т. е. множество*

$$H = \{g \mid g \in G,\ M'g = M'\},$$

является подгруппой группы G, примитивно действующей на M'.

Доказательство. Пусть G — группа подстановок множества M, M_i — соответствующие орбиты, G_i — группа подстановок множества M_i, индуцированная действием G на M_i. Очевидно, G будет подпрямым произведением групп G_i.

Теперь докажем второе утверждение. Очевидно, H — подгруппа. Пусть $x_1, \ldots, x_s$ — правые представители G по H. Тогда $M'x_1, \ldots, M'x_s$ — исходное разбиение M на блоки (использовать транзитивность G). Если бы H действовала на M' не примитивно, то существовало бы нетривиальное разбиение M' на блоки $M'_1, \ldots, M'_r$ относительно H. Но тогда исходное разбиение множества M относительно G можно было бы измельчить до разбиения $M'_i x_j$, $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Теорема доказана.

12.3.7. Теорема. *Пусть G — транзитивная группа подстановок множества M. Пусть M разбито на блоки, M_1 — какой-нибудь блок, m_1 — какая-нибудь точка из M_1. Пусть H — стабилизатор m_1, K — стабилизатор M_1 в целом, т. е.*

$$H = \{g \mid g \in G,\ m_1 g = m_1\},$$
$$K = \{g \mid g \in G,\ M_1 g = M_1\}.$$

Тогда H, K — подгруппы из G, причем $H \leqslant K \leqslant G$. Общее число блоков равно $|G : K|$ и каждый блок состоит из $|K : H|$ элементов.

Доказательство. Первое вытекает из определений. Далее, пусть $Hx_1, \ldots, Hx_s$ — правые смежные классы G по H, причем $x_1 = 1$. По теореме 12.3.5 можно

считать, что $M = \{Hx_1, \ldots Hx_s\}$, а G действует на M правыми сдвигами. Пусть $M_1 = \{Hx_1, \ldots, Hx_r\}$, $m_1 = H$. Ввиду транзитивности G всякий блок получается из M_1 правым сдвигом на элемент из G, поэтому все блоки равномощны, и, значит, достаточно убедиться, что $r = |K : H|$ или что

$$K = Hx_1 \cup \ldots \cup Hx_r.$$

Но, с одной стороны, каждое hx_i, $h \in H$, $1 \leqslant i \leqslant r$, переводит смежный класс H в некоторый смежный класс из M_1, поэтому и весь блок M_1 переводит в себя. Значит,

$$Hx_1 \cup \ldots \cup Hx_r \subseteq K.$$

С другой стороны, если $x \in K$, то $Hx = Hx_i$ для некоторого $1 \leqslant i \leqslant r$, откуда получается противоположное вложение.

§ 13. Простые конечные группы

Подобно тому как натуральные числа получаются из простых чисел посредством умножения, так и любую конечную группу можно построить из простых конечных групп посредством расширений. В самом деле, рассмотрим в конечной группе G субнормальную матрёшку без повторений

$$1 = G_0 < G_1 < \ldots < G_m = G,$$

т. е. матрёшку, в которой каждый предыдущий член — собственная нормальная подгруппа следующего члена. Если некоторая секция G_{i+1}/G_i не является простой группой, то, взяв в ней собственную нормальную подгруппу H/G_i, можно уплотнить матрёшку вставкой $G_i < H < G_{i+1}$, поэтому в неуплотняемой без повторений субнормальной матрёшке все секции просты. В этом смысле простые конечные группы — это те строительные блоки, из которых можно собрать произвольную конечную группу, хотя в отличие от чисел результат не определяется здесь только составляющими блоками, а зависит от способа сборки. Тривиальный пример простых групп — циклические группы простого порядка; очевидно, это единственные простые группы, являющиеся абелевыми. Классификация простых конечных групп — чрезвычайно важная и, по-

жалуй, в настоящее время главная проблема в теории конечных групп, хотя она не исчерпывает всего содержания этой теории. Наступление ведется в нескольких направлениях: одни развивают общие — «индустриальные» — методы, стремясь к тому, чтобы научиться единообразно получать все простые конечные группы,— сюда примыкают и тонкие работы по отождествлению групп, полученных разными способами,— другие, напротив, полагаясь на интуицию и старательское счастье, ищут отдельные примеры — ценность каждой новой простой группы сейчас необычайно высока,— третьи проводят классификацию при тех или иных дополнительных условиях,— например, при заданной силовской подгруппе, и т. д. В 60-е годы пала знаменитая проблема Бернсайда, полвека остававшаяся неприступной,— Файт и Томпсон [36] доказали, что любая нециклическая простая конечная группа содержит четное число элементов (впрочем, чаще эту теорему формулируют иначе — без упоминания простых групп: *любая нечетная группа*, т. е. конечная группа нечетного порядка, *полициклична*).

Настоящий параграф преследует скромную цель — указать две классические серии простых конечных групп — знакопеременные группы и проективные специальные линейные группы. Приводимые здесь доказательства кустарны и не дают представления об упоминавшихся индустриальных методах. Хороший обзор современного состояния этой области и таблицу известных простых конечных групп можно найти в статьях В. Д. Мазурова [18] и Ашбахера [35].

13.1. Знакопеременные группы. В этом пункте нам будет полезно замечание III из примера 2.5.7.

13.1.1. Т е о р е м а (Галуа). *При $n \neq 4$ знакопеременная группа A_n проста. Группа A_4 не проста.*

Д о к а з а т е л ь с т в о. а) Группы A_1, A_2, A_3 имеют порядки 1, 1, 3 соответственно, а потому просты. Группа A_4 не проста — ввиду 4.4.1.III она обладает полициклической матрёшкой с секциями порядков 2, 2, 3. Пусть теперь $n \geqslant 5$ и N — неединичная нормальная подгруппа группы A_n; надо доказать, что $N = A_n$. Так как A_n порождается тройными циклами (см. 2.2.2.III), то достаточно показать, что все они лежат в N. Мы сделаем это в несколько этапов.

б) Так как N содержит неединичную четную подстановку, то, разлагая ее в произведение независимых циклов, можно считать, что N содержит одну из следующих подстановок:

б.1) $a = (1234\ldots)\ldots$, т. е. в разложении подстановки a есть цикл длины $\geqslant 4$,

б.2) $a = (123)(45\ldots)\ldots$, т. е. имеется тройной цикл и еще какие-то циклы,

б.3) $a = (123)$,

б.4) $a = (12)(34)\ldots$, т. е. a — произведение независимых транспозиций.

в) Подгруппа N содержит хотя бы один тройной цикл. В самом деле, она содержит коммутатор $[a, b] = a^{-1}(b^{-1}ab)$ при любом $b \in A_n$. Взяв

$$b_1' = \begin{cases} (123) \text{ в случае б.1),} \\ (124) \text{ в случае б.2),} \\ (123) \text{ в случае б.4),} \end{cases}$$

после несложных вычислений получим

$$[a, b] = \begin{cases} (124) & \text{в случае б.1),} \\ (12534) & \text{в случае б.2),} \\ (13)(24) & \text{в случае б.4).} \end{cases}$$

Тем самым случай б.2) свелся к б.1), который в свою очередь свелся к б.3), а для него утверждение тривиально. Осталось разобрать случай б.4). Сопрягая четной подстановкой (12534) подстановку $[a, b]$, мы получим (24)(15) (см. замечание III в примере 2.5.7), а затем, умножив $[a, b]$ на эту подстановку, получим (135).

г) Подгруппа N содержит все тройные циклы. В самом деле, по предыдущему она содержит некоторый цикл $(i_1i_2i_3)$. Пусть $(j_1j_2j_3)$ — любой другой тройной цикл. Так как $n \geqslant 5$, то существует четная подстановка вида

$$\begin{pmatrix} i_1 & i_2 & i_3 & \ldots \\ j_1 & j_2 & j_3 & \ldots \end{pmatrix}.$$

Сопрягая ею $(i_1i_2i_3)$, получим $(j_1j_2j_3)$. Теорема доказана.

Заметим, что рассуждение а) — г) этого доказательства — типичный и в принципе универсальный путь доказательства простоты: взяв в нормальной подгруппе N элемент a, о котором мы знаем только, что он отличен

от единицы, и учитывая, что умножение и обращение, а также сопряжение и коммутирование произвольным элементом группы не выводят нас за пределы N, мы постепенно вытягиваем из N всё новые и новые элементы, пока не обнаружим там все порождающие элементы группы. Философ, снизошедший до теоремы Галуа, мог бы так резюмировать идею приведенного доказательства: ухватившись за данное звено, вытаскиваем всю цепь. К сожалению, эта руководящая идея оставляет в тени способ вытаскивания.

13.1.2. Упражнение. Если $\mathfrak{n}$ — произвольное кардинальное число, то *знакопеременной группой степени* $\mathfrak{n}$ называют группу $\boldsymbol{A}_{\mathfrak{n}}$ тех преобразований множества мощности $\mathfrak{n}$, каждое из которых действительно передвигает лишь конечное число символов и разлагается в произведение четного числа транспозиций. Повторяя доказательство теоремы Галуа, доказать простоту $\boldsymbol{A}_{\mathfrak{n}}$ при $\mathfrak{n} \neq 4$.

В связи с последним упражнением отметим следующее. Пусть, как это принято в теории множеств, ω_ν обозначает $(\nu + 1)$-е бесконечное кардинальное число. Пусть M — множество мощности ω_ν и $\boldsymbol{S}_\mu(M)$ — совокупность тех отображений из $\boldsymbol{S}(M)$, которые в действительности передвигают множество символов мощности $<\omega_\mu$. Ясно, что трансфинитно возрастающая матрёшка

$$1 < \boldsymbol{A}_{\omega_\nu} < \boldsymbol{S}_0(M) < \boldsymbol{S}_1(M) < \ldots$$
$$\ldots < \boldsymbol{S}_\nu(M) < \boldsymbol{S}(M) \quad (1)$$

состоит из нормальных подгрупп группы $\boldsymbol{S}(M)$. Оказывается, членами этой матрёшки исчерпываются вообще все нормальные подгруппы группы $\boldsymbol{S}(M)$ (Baer R.— Studia math., 1934, 5, p. 15—17). В частности, секция $\boldsymbol{S}(M)/\boldsymbol{S}_\nu(M)$ — простая группа. Отметим, наконец, что в свете этих фактов задача а) из 12.1.4 решается совсем просто. В самом деле, для конечных групп решение сразу следует из 12.1.2. Если же группа G имеет бесконечную мощность ω_ν, то, взятая в регулярном представлении, она попадает в $\boldsymbol{S}(G)$, где пересекается с $\boldsymbol{S}_\nu(G)$ по единице, а потому G изоморфно вкладывается в $\boldsymbol{S}(G)/\boldsymbol{S}_\nu(G)$.

13.1.3. Упражнение. В знакопеременной группе $\boldsymbol{A}_5$ порядка 60 нет подгрупп порядка 15, 20, 30.

Р е ш е н и е. Если бы A_5 содержала подгруппу порядка 15, т. е. индекса 4, то по теореме 12.2.2 она содержала бы нормальную подгруппу конечного индекса, делящегося на 4 и делящего 24. Это, однако, невозможно, так как согласно теореме 13.1.1 A_5 — простая группа. Остальные случаи разбираются аналогично.

13.2. Проективные специальные линейные группы. Пусть K — поле. Фактор-группа $PSL_n(K)$ специальной линейной группы $SL_n(K)$ по ее центру — подгруппе скалярных матриц — называется *проективной специальной линейной группой*. Эти группы — над конечными полями — были введены в числе других серий групп Жорданом (1870), который установил их простоту. Неточности в первоначальном доказательстве Жордана устранил Диксон.

13.2.1. У п р а ж н е н и е. Дробно-линейные функции

$$f(x) = \frac{ax+b}{cx+d}$$

с коэффициентами из поля K и определителем $ad - bc = 1$ составляют относительно суперпозиции группу, изоморфную группе $PSL_2(K)$.

13.2.2. У п р а ж н е н и е. Проверить формулы:

$$|SL_n(q)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i), \tag{2}$$

$$|PSL_n(q)| = \frac{1}{d(q-1)}\prod_{i=0}^{n-1}(q^n - q^i), \text{ где } d = (n, q-1). \tag{3}$$

У к а з а н и е: рассмотреть SL как ядро гомоморфизма det и воспользоваться формулой (4) из § 11, а также упражнением 3.1.6.

Для доказательства теоремы Жордана — Диксона, причем над любым — не обязательно конечным — полем, мы воспользуемся таким признаком простоты:

13.2.3. Л е м м а. *Примитивная группа G преобразований множества M проста, если выполнены следующие условия:*

1) *G совпадает со своим коммутантом G',*

2) *стабилизатор* S_m *некоторого элемента* m *из* M *содержит такую абелеву нормальную подгруппу* A_m, *что*

$$G = \text{гр}\,(A_m^g \mid g \in G). \qquad (4)$$

Доказательство. а) Пусть N — неединичная нормальная подгруппа группы G; надо доказать, что $G = N$. Заметим сначала, что $G = S_m N$. В самом деле, ввиду 12.3.4 N транзитивна, поэтому для всякого $g \in G$ найдется такое $h \in N$, что $mh = mg$. Следовательно, $gh^{-1} \in S_m$ и $g \in S_m N$.

б) Далее, $G = A_m N$. Действительно, в силу (4) каждый элемент g из G записывается в виде

$$g = a_1^{g_1} \ldots a_s^{g_s}, \quad a_i \in A_m, \quad g_i \in G,$$

а ввиду а) можно считать, что каждый g_i лежит в N. Так как A_m и N перестановочны, то $g \in A_m N$.

в) Наконец, $G = N$. В самом деле, ввиду 1), б) и коммутаторных соотношений из § 3,

$$G = [A_m N,\ A_m N] \leqslant N.$$

Лемма доказана.

13.2.4. Теорема (Жордан — Диксон). *Для всякого поля* K *группа* $\boldsymbol{PSL}_n(K)$ *проста, за исключением двух случаев*: $\boldsymbol{PSL}_2$ (2) *и* $\boldsymbol{PSL}_2$ (3).

Доказательство. Прежде всего, указанные две группы имеют порядки 6 и 12 (см. формулу (3)), а потому действительно не просты — см. упражнения 11.2.1 и 12.2.3. Переходя к общему случаю, рассмотрим естественное действие группы $G = \boldsymbol{PSL}_n(K)$ на множестве M всех прямых n-мерного векторного пространства над полем K с какой-нибудь фиксированной базой $e_1, \ldots, e_n$ и проверим, что для G, M выполнены все условия леммы 13.2.3.

Так как для любых двух пар различных прямых существует линейное преобразование, переводящее первую пару во вторую, то группа G дважды транзитивна, а потому примитивна (см. 12.3.3).

Далее, G совпадает со своим коммутантом — это сразу следует из формулы (8) примера 3.2.1 (именно здесь выпадают две исключительные группы).

Проверим, наконец, условие 2). Пусть m — прямая с направляющим вектором e_n. Ясно, что стабилизатор

S_m (точнее, его прообраз в группе $\boldsymbol{SL}_n(K)$) состоит из всевозможных матриц вида

$$\left(\begin{array}{c|c} * & \begin{matrix}*\\ \vdots\\ *\end{matrix} \\ \hline 0\ldots0 & * \end{array}\right).$$

Отображение группы S_m на пару диагональных клеток — гомоморфизм, ядро которого A_m состоит из всевозможных матриц того же вида с единичными клетками по диагонали. Очевидно, группа A_m абелева, и остается проверить только формулу (4). Так как группа $\boldsymbol{SL}_n(K)$ порождается своими трансвекциями $t_{ij}(\alpha)$ (см. 2.2.2.IV), то достаточно убедиться, что $t_{ij}(\alpha)$ сопряжена в $\boldsymbol{SL}_n(K)$ с некоторой $t_{1k}(\alpha)$. Но если $i = 1$, то это тривиально, а если $i \neq 1$, то в качестве сопрягающей матрицы можно взять матрицу перехода от фиксированной базы $e_1, \ldots, e_i, \ldots$ к базе $-e_i, \ldots, e_1, \ldots$, где все невыписанные векторы не меняются. Теорема доказана.

13.2.5. У п р а ж н е н и е. В связи с теоремой Жордана — Диксона естественно спросить, не получим ли мы новые простые конечные группы, если в определении $\boldsymbol{PSL}_n(K)$ возьмем вместо поля K кольцо вычетов $\mathbb{Z}_m$? Эти надежды несостоятельны: если m — простое число, то мы возвращаемся к случаю поля, если же m составное, то группа $\boldsymbol{PSL}_n(\mathbb{Z}_m)$ не проста.

13.2.6. У п р а ж н е н и е. Указать группу, центр которой определяет простую фактор-группу, но не выделяется прямым множителем.

Р е ш е н и е. Если бы в группе $G = \boldsymbol{SL}_2$ (5) центр Z, состоящий из матриц $\pm e$, имел прямое дополнение H, то одна из матриц

$$\pm\begin{pmatrix} \frac{1}{\zeta} & 0 \\ 0 & \zeta \end{pmatrix}$$

лежала бы в H, где ζ — порождающий мультипликативной группы поля из 5 элементов. Но тогда квадрат $-e$ этой матрицы лежал бы в пересечении $Z \cap H$, что невозможно.

Томпсон (Thompson J. G.— Pacif. J. Math., 1964, 14, № 1, p. 363—364) назвал подгруппу A конечной

группы G 2-*сигнализатором* группы G, если порядок $|A|$ и индекс $|G : N_G(A)|$ нечетны. Там же он высказал гипотезу, что 2-сигнализаторы простых конечных групп всегда абелевы. Мы закончим главу примером, опровергающим эту гипотезу. Он принадлежит В. Д. Мазурову (Алгебра и логика, 1968, 7, № 3, с. 60—62) и использует только простоту групп $\boldsymbol{PSL}$.

13.2.7. Пример. В простой группе $\boldsymbol{PSL}_7(q)$, где q нечетно, существуют неабелевы 2-сигнализаторы. Действительно, рассмотрим в $G = \boldsymbol{SL}_7(q)$ подгруппы A, B, состоящие соответственно из всевозможных матриц вида

$$\begin{pmatrix} 1 & * & * \\ 0 & e_2 & * \\ 0 & 0 & e_4 \end{pmatrix}, \quad \begin{pmatrix} \alpha(x,y) & 0 & 0 \\ 0 & x & 0 \\ 0 & 0 & y \end{pmatrix}, \quad \alpha(x,y) = \frac{1}{\det x \cdot \det y},$$

где e_k — единичная матрица степени k и клеточное разбиение оба раза одно и то же. Ввиду формулы (2) этого параграфа и формулы (4) из § 11

$$|G| = \frac{1}{q-1}(q^7-1)(q^7-q)\ldots(q^7-q^6), \quad |A| = \text{степень } q,$$

$$|B| = (q^2-1)(q^2-q)(q^4-1)(q^4-q)(q^4-q^2)(q^4-q^3).$$

Отсюда непосредственно видно, что $|A|$, $|G:B|$ — нечетные числа. Ясно, что B нормализует A, поэтому индекс $|G : N_G(A)|$ нечетен. Если φ — факторизация группы G по ее центру Z, то порядок подгруппы A^φ и индекс ее нормализатора в G^φ тоже нечетны, т. е. A^φ есть 2-сигнализатор в $\boldsymbol{PSL}_7(q)$. Но $A \cap Z = 1$, поэтому группа A^φ изоморфна A и, значит, неабелева.

Глава 5

СВОБОДНЫЕ ГРУППЫ И МНОГООБРАЗИЯ

§ 14. Свободные группы

В начале гл. 3 мы определили понятие группы, свободной в данном классе, и установили, что в классе абелевых групп свободные группы существуют и имеют ясное описание. В этом параграфе будет доказано существование, дано описание и изучены простейшие свойства свободных групп в классе всех групп.

14.1. Определение. Элементы порождающего множества M любой данной группы G могут быть связаны соотношениями в G, т. е. произведения самих этих элементов и элементов, к ним обратных, могут равняться единице в G. Например, $xx^{-1} = e$, $x^{-1}x = e$ для любого x из M. Будучи следствиями аксиом, последние соотношения неизбежны в любой группе и потому называются *тривиальными*. Оказывается, существуют группы, не допускающие в некотором порождающем множестве никаких нетривиальных соотношений — «свободные от соотношений». Цель этого пункта — дать конструкцию таких групп и доказать, что они и будут свободными группами в классе всех групп в смысле общего определения гл. 3 (этим объясняется, в частности, происхождение термина «свободная»).

Пусть I — множество. О какой бы группе G с порождающими x_i, $i \in I$, ни шла речь, ее элементы изображаются словами $x_{i_1}^{\varepsilon_1} \ldots x_{i_m}^{\varepsilon_m}$, $\varepsilon_j = \pm 1$, а их умножение — приписыванием слова к слову. Это и подсказывает идею конструкции: надо сами слова от букв $\{x_i, x_i^{-1} \mid i \in I\}$ без подслов типа $x_i^{\varepsilon} x_i^{-\varepsilon}$, $\varepsilon = \pm 1$, объявить элементами группы, а их приписывание друг к другу с последующим вычеркиванием таких подслов — умножением.

Более точно, зафиксируем два множества символов

$$X = \{x_i \mid i \in I\} \text{ и } X^{-1} = \{x_i^{-1} \mid i \in I\}.$$

Слово в алфавите X — это пустая (обозначается **1**) или конечная последовательность символов из $X \cup X^{-1}$. Число элементов этой последовательности называется *длиной* слова. Слово назовем *сократимым*, если оно содержит соседние символы вида x_i^{ε}, $x_i^{-\varepsilon}$, $\varepsilon = \pm 1$. Например, первое из слов

$$x_2x_1x_1x_2^{-1}x_3, \quad x_1x_2x_2^{-1}x_3$$

несократимо, а второе сократимо. Будем говорить, что два слова u и v *эквивалентны* (в символах: $u \sim v$), если v можно получить из u через конечное число вставок и сокращений слов вида $x_i^{\varepsilon}x_i^{-\varepsilon}$. Ясно, что отношение $\sim$ рефлексивно, симметрично и транзитивно. Все слова, эквивалентные u, образуют класс эквивалентных слов, который мы обозначим через $[u]$.

14.1.1. Т е о р е м а. *Пусть* $X = \{x_i \mid i \in I\}$. *На множестве* $\boldsymbol{F}(X)$ *классов эквивалентных слов в алфавите* X *определим умножение, полагая* $[u][v] = [uv]$. *Это определение не зависит от случайного выбора представителей в классах. Множество* $\boldsymbol{F}(X)$ *является группой относительно этого умножения.*

Д о к а з а т е л ь с т в о. а) Любой класс эквивалентных слов содержит единственное несократимое слово. Действительно, пусть $\rho(u)$ обозначает несократимое слово, полученное из u последовательными вычеркиваниями самого правого подслова $x_i^{\varepsilon}x_i^{-\varepsilon}$. Функция ρ обладает следующими свойствами (знак $\equiv$ обозначает графическое равенство):

$$\rho(u) \sim u, \tag{1}$$

$$\rho(u) \equiv u, \text{ если } u \text{ несократимо}, \tag{2}$$

$$\rho(uv) \equiv \rho(u\,\rho(v)), \tag{3}$$

$$\rho(x_i^{\varepsilon}x_i^{-\varepsilon}u) \equiv \rho(u) \text{ при } \varepsilon = \pm 1, \tag{4}$$

$$\rho(ux_i^{\varepsilon}x_i^{-\varepsilon}v) \equiv \rho(uv) \text{ при } \varepsilon = \pm 1, \tag{5}$$

$$\rho(uv) \equiv \rho(\rho(u)\,\rho(v)). \tag{6}$$

Свойства (1), (2), (3) следуют непосредственно из определения ρ, (4) вытекает из (3), формула (5) следует из (3),

(4), формула (6) — из (3), (4), (5) индукцией по длине u. Пусть теперь $u \sim v$, где u, v — несократимые слова. По определению существует последовательность слов

$$u \equiv u_1,\ u_2,\ \ldots,\ u_m \equiv v,$$

в которой соседние слова получаются друг из друга одной вставкой или одним сокращением подслова вида $x_i^{\varepsilon} x_i^{-\varepsilon}$. Ввиду (5) $\rho(u_{i+1}) \equiv \rho(u_i)$, поэтому $\rho(v) \equiv \rho(u)$. Ввиду несократимости слов u, v это означает, что $v \equiv u$.

б) Независимость произведения $[u][v]$ от случайного выбора представителей u, v вытекает из а) и формулы (6). Ассоциативность умножения классов ясна из определения. Единицей будет класс, содержащий пустое слово, а обратным к классу $[x_{i_1}^{\varepsilon_1} \ldots x_{i_m}^{\varepsilon_m}]$ — класс $[x_{i_m}^{-\varepsilon_m} \ldots x_{i_1}^{-\varepsilon_1}]$. Теорема доказана.

Группа $F(X)$ называется *свободной группой со свободным порождающим множеством* X, а мощность $|X|$ называется ее *степенью* (*свободы*). Если $X = \{x_1, \ldots, x_n\}$, $X = \{x_1, x_2, \ldots\}$, то вместо $F(X)$ пишут также $F_n(x)$, $F_\infty(x)$ соответственно. Если обозначения порождающих несущественны, то пишут просто F_n, F_∞. В дальнейшем для записи элементов свободной группы мы будем использовать представители классов, т. е. писать, например, $u = v$, $uv = w$ вместо $[u] = [v]$, $[u][v] = [w]$. Ввиду замечания а) можно говорить также о несократимой записи класса, подразумевая под этим несократимую запись $\rho(u)$ любого его представителя u.

14.1.2. Упражнение. Свободные группы степени $\geqslant 2$ некоммутативны.

14.1.3. Упражнение. Если u — непустое слово, то длина слова $\rho(u^n)$, $n \geqslant 2$, больше длин слов $\rho(u)$, $\rho(u^{-1})$. В частности, любая свободная группа является группой без кручения.

14.1.4. Упражнение. Несократимое слово назовем циклически несократимым, если оно начинается некоторым символом x_i^{ε}, а кончается символом, отличным от $x_i^{-\varepsilon}$. Вычеркивая в начале и конце слова одинаковые символы, входящие с разными показателями, можно любое несократимое слово u в конечное число шагов привести к циклически несократимому виду $\sigma(u)$. Доказать, что элементы u, v свободной группы тогда и только

тогда сопряжены в ней, когда $\sigma(u) \equiv w_1 w_2$, $\sigma(v) \equiv w_2 w_1$ при подходящих w_1, w_2.

Оказывается, любая группа, обладающая порождающим множеством мощности $\mathfrak{n}$, является гомоморфным образом свободной группы степени $\mathfrak{n}$. Больше того, следующая теорема показывает, что группы $\boldsymbol{F}(X)$ — это и есть группы, свободные в классе всех групп в смысле начала гл. 3.

14.1.5. Теорема. *Пусть группа G порождается множеством $M = \{g_i \mid i \in I\}$. Возьмем алфавит $X = \{x_i \mid i \in I\}$. Отображение $X \to M$ по правилу $x_i \mapsto g_i$ единственным образом продолжается до гомоморфизма $\boldsymbol{F}(X) \to G$.*

Доказательство. Ясно, что образом класса $[x_{i_1}^{\varepsilon_1} \ldots x_{i_m}^{\varepsilon_m}]$ надо объявить элемент $g_{i_1}^{\varepsilon_1} \ldots g_{i_m}^{\varepsilon_m}$. Корректность и гомоморфность этого отображения вытекают из определений. Теорема доказана.

Элементы ядра H гомоморфизма $\boldsymbol{F}(X) \to G$ называются *соотношениями* группы G в алфавите X. Если множество H' соотношений таково, что минимальная нормальная подгруппа в $\boldsymbol{F}(X)$, содержащая H', совпадает с H, то H' называется *определяющим множеством соотношений в алфавите X*. Так как $G \simeq \boldsymbol{F}(X)/H$, то задание алфавита X и множества H' полностью определяет группу G. Пара X, H' называется *генетическим кодом* группы G; символическая запись: $G = \text{гр}\,(X \parallel H')$. Иногда для краткости перечень порождающих элементов опускают, подразумевая, что группа порождается всеми элементами, упоминаемыми в определяющих соотношениях. Конечно, одна и та же группа допускает много различных генетических кодов, и польза того или иного кода зависит от конкретной задачи. Особый интерес представляют группы, допускающие конечный генетический код, они называются *конечно определенными*.

Иногда вместо слов u из H' в записи генетического кода пишут равенства $u = 1$ или даже $u_1 = u_2$, если u имеет вид $u_1 u_2^{-1}$.

14.1.6. Упражнение. Свободная абелева группа степени n допускает следующий генетический код:

$$\text{гр}\,(x_1, \ldots, x_n \parallel x_i^{-1} x_j^{-1} x_i x_j,\ 1 \leqslant i < j \leqslant n).$$

14.1.7. Упражнение:

$$\mathbb{C}_2 \times \mathbb{C}_2 = \text{гр}\,(x,\ y \parallel x^2 = 1,\ y^2 = 1,\ xy = yx).$$

Для отыскания генетического кода группы во многих случаях бывает удобен *метод перечисления смежных классов*, который мы поясним сейчас на примере группы $\mathfrak{S}_4$. Прежде всего, в рассматриваемой группе выбираются порождающие элементы и записываются соотношения между ними, представляющиеся по каким-то соображениям, хотя бы интуитивным, достаточными для определения группы. Например, в группе $\mathfrak{S}_4$ в качестве порождающих можно взять элементы $x = (1234)$, $y = (12)$ (см. упражнение 2.2.4). Так как $xy = (234)$, то

$$x^4 = 1,\quad y^2 = 1,\quad (xy)^3 = 1.$$

Поскольку наша группа не очень сложна, разумно предположить, что эти соотношения и достаточны для ее определения. Чтобы доказать это, рассмотрим группу

$$G = \text{гр}\,(x,\ y \parallel x^4 = 1,\ y^2 = 1,\ (xy)^3 = 1),$$

а в ней какую-нибудь подгруппу, скажем, $H = (x)$, и постараемся установить, что G содержит $|\mathfrak{S}_4| : 4 = 6$ смежных классов по H. Тогда будет

$$|G| = |H| \cdot |G : H| = 24,$$

а так как G имеет $\mathfrak{S}_4$ своим гомоморфным образом, то получим искомый изоморфизм $G \simeq \mathfrak{S}_4$.

Начертим в соответствии с определяющими соотношениями группы G три таблицы

x	x	x	x
1	1	1	1

y	y
1	1

x	y	x	y	x	y
1	1				1

и начнем перечислять смежные классы G по H, обозначив саму H цифрой 1. Очевидное равенство $1x = 1$ мы уже внесли во все таблицы. Что написать на пустом месте во второй таблице? Положим $1y = 2$, тогда как следствие получается $2y = 1$. Внесем эти соотношения во все таблицы, открыв одновременно в каждой из них новую строку:

x	x	x	x	x	y	y	x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2			2	1
2				2	2	1	2	2			2	1	1	2

Положим, далее, $2x = 3$, $3x = 4$. Таблицы примут вид

x	x	x	x	x	y	y	x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2	3		2	1
2	3	4		2	2	1	2	2	3		2	1	1	2
3	4		2	3	3		3	3	4					3
4		2	3	4	4		4	4						4

Пусть теперь $4x = 5$, тогда из первой таблицы $5x = 2$, из третьей $3y = 5$ и из второй $5y = 3$. Получаем

x	x	x	x	x	y	y	x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4			4	5	3
4	5	2	3	4	4		4	4	5	3	4			4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5

Таблицы явно густеют — верный признак того, что процесс перечисления смежных классов приближается к концу (в противном случае таблицы с увеличением числа строк все более пустеют). Теперь надо положить $4y = 6$, и мы получим

x	x	x	x	x	y	y	x	y	x	y	x	y
1	1	1	1	1	1	2	1	1	1	2	3	5	2	1
2	3	4	5	2	2	1	2	2	3	5	2	1	1	2
3	4	5	2	3	3	5	3	3	4	6	6	4	5	3
4	5	2	3	4	4	6	4	4	5	3	4	6	6	4
5	2	3	4	5	5	3	5	5	2	1	1	2	3	5
6	6	6	6	6	6	4	6	6	6	4	5	3	4	6

Таблицы закрылись — перечисление смежных классов закончено. Его результат: $|G : H| = 6$. Заметим, что на каком-то шаге мы могли и не заметить возможного заполнения некоторых мест, тогда какой-то класс получил бы несколько разных номеров. Таким образом, из закрытия таблиц следует лишь неравенство $|G : H| \leqslant 6$. Так как, однако, G имеет гомоморфным образом группу $\boldsymbol{S}_4$, то строгое неравенство на самом деле невозможно.

Отметим еще, что 3-я, 4-я и 5-я строки первой таблицы являются следствиями 2-й строки и их можно было бы вообще не писать; то же относится ко 2-й, 5-й, 6-й строкам второй таблицы и 2-й, 4-й, 5-й, 6-й строкам третьей таблицы. Впрочем, эти и некоторые другие упрощения метода перечисления носят уже технический характер, и мы не будем на них задерживаться. Добавим только, что описанный метод хорошо поддается программированию для вычислительных машин (см., например, сб. Вычисления в алгебре и теории чисел.— М.: Мир, 1976).

14.1.8. Упражнение:

$$\boldsymbol{S}_3 = \text{гр}(x,\ y \parallel x^2 = y^3 = (xy)^2 = 1).$$

14.1.9. Упражнение. Перечислить 5 смежных классов группы

$$G = \text{гр}(x,\ y,\ z \parallel x^3 = y^3 = z^3 = (yz)^2 = (zx)^2 = (xy)^2 = 1)$$

по подгруппе $H = \text{гр}(x, y)$.

14.1.10. Упражнение. Найти генетический код группы порядка pq, где p, q — простые числа, $p < q$.

14.1.11. Упражнение. Подгруппа, порожденная в $\boldsymbol{F}(x, y)$ элементами $x^n y x^n$, $n = 0, 1, 2, \ldots$, свободно порождается ими (т. е. описывается пустым множеством соотношений).

Задание групп генетическими кодами естественно возникает в топологии (например, в теории узлов) и других областях. Подробную теорию можно найти в [11, 17].

14.2. Матричное представление. В этом пункте мы докажем изоморфную вложимость счетных свободных групп в $\boldsymbol{SL}_2(\mathbb{Z})$. Так как группы $\boldsymbol{F}_1, \boldsymbol{F}_2, \ldots$ вкладываются в $\boldsymbol{F}_\infty$, а $\boldsymbol{F}_\infty$ в $\boldsymbol{F}_2$ (упражнение 14.1.11), то достаточно найти в $\boldsymbol{SL}_2(\mathbb{Z})$ свободную подгруппу степени 2.

14.2.1. Теорема. *Пусть m — целое число $\geqslant 2$. Подгруппа, порожденная в $SL_2(\mathbb{Z})$ трансвекциями*

$$t_{12}(m) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad t_{21}(m) = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},$$

порождается ими свободно, т. е. описывается пустым множеством соотношений.

Доказательство. Обозначим для краткости $a = t_{12}(m)$, $b = t_{21}(m)$. Пусть w — чередующееся произведение ненулевых степеней элементов a, b в группе $SL_2(\mathbb{Z})$. Надо показать, что $w \neq e$. Если w начинается со степени b, то можно сопрячь w этой степенью и рассмотреть полученное произведение, которое начинается уже со степени a. Поэтому пусть $w = a^{\alpha_1}b^{\alpha_2} \ldots c^{\alpha_r}$, где $c = a$ или b, все $\alpha_i \neq 0$. Пусть z_i — верхняя строчка матрицы $a^{\alpha_1}b^{\alpha_2} \ldots c^{\alpha_i}$. Если $z_{2k-1} = (x_{2k-1}, x_{2k})$, то

$$z_{2k} = z_{2k-1}b^{\alpha_{2k}} = (x_{2k+1}, x_{2k}), \quad z_{2k+1} = z_{2k}a^{\alpha_{2k+1}} = (x_{2k+1}, x_{2k+2}),$$

где

$$x_{2k+1} = x_{2k-1} + m\alpha_{2k}x_{2k}, \quad x_{2k+2} = x_{2k} + m\alpha_{2k+1}x_{2k+1}.$$

Объединяя последние две формулы, получаем

$$x_{i+2} = x_i + m\alpha_{i+1}x_{i+1} \text{ для } i = 1, 2, \ldots, r-1.$$

Нам достаточно доказать, что с ростом i от 1 до $r+1$ числа $|x_i|$ возрастают. Для $i = 1, 2$ это проверяется непосредственно. Дальше ведем индукцию:

$$|x_{i+2}| \geqslant m|\alpha_{i+1}||x_{i+1}| - |x_i| \geqslant$$
$$\geqslant 2|x_{i+1}| - |x_i| \geqslant |x_{i+1}| + 1.$$

Теорема доказана.

Указанные в ней канонические вложения $F_2 \to SL_2(\mathbb{Z})$ весьма полезны в теории свободных групп. Для иллюстрации отметим одно их применение.

14.2.2. Теорема. *Пусть p — простое число. Любая свободная группа $F(X)$ аппроксимируется конечными p-группами.*

Доказательство. Пусть X' — конечная часть X. Посылая остальные свободные порождающие в единицу, мы получим гомоморфизм $F(X) \to F(X')$. Так как ядра таких гомоморфизмов пересекаются по единице, то по теореме Ремака 4.3.9 $F(X)$ — поддекартово произве-

дение счетных свободных групп. Таким образом, можно считать, что $F'(X)$ счетна, а потому по теореме 14.2.1 вложена в конгруэнц-подгруппу $\Gamma_2(p)$. Напомним (см. упражнение 4.2.7), что по определению

$$\Gamma_2(m) = \{x \mid x \in SL_2(\mathbb{Z}),\ x \equiv e \pmod m\}.$$

Будучи ядрами гомоморфизмов $SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}_{p^k})$, подгруппы $\Gamma_2(p^k)$ — нормальные подгруппы конечных индексов в $SL_2(\mathbb{Z})$ и, очевидно, пересекаются по единице, $k = 1, 2, \ldots$ Поэтому, снова по теореме Ремака, $\Gamma_2(p)$ — поддекартово произведение конечных групп $\Gamma_2(p)/\Gamma_2(p^k)$. Наконец,

$$(e + pz)^p = \sum_{i=0}^{p} \binom{p}{i} (pz)^i \equiv e \pmod{p^2},$$

$$(e + p^2z)^p = \sum_{i=0}^{p} \binom{p}{i} (p^2z)^i \equiv e \pmod{p^3},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

поэтому $\Gamma_2(p)/\Gamma_2(p^k)$ есть p-группа. Теорема доказана.

Обратим внимание на то, что финитную аппроксимируемость свободных групп мы вывели здесь из финитной аппроксимируемости группы $GL_n(\mathbb{Z})$. Вообще, финитную аппроксимируемость группы часто удается извлечь из ее представимости матрицами ввиду следующей теоремы А. И. Мальцева (Матем. сб., 1940, 8, № 3, с. 405—421): *всякая конечно порожденная группа матриц над полем финитно аппроксимируема.* Простое доказательство этой теоремы можно найти в [20], стр. 408.

Легко проверить, что множество

$$G_m = \{x \mid x \in SL_2(\mathbb{Z}),\quad x_{11} \equiv x_{22} \equiv 1 \pmod{m^2},\ x_{12} \equiv x_{21} \equiv 0 \pmod m\}$$

является подгруппой в $SL_2(\mathbb{Z})$, причем

$$\text{гр}\,(t_{12}(m),\ t_{21}(m)) \leqslant G_m.$$

В общем случае равенства нет, но, как показал И. Н. Санов (ДАН СССР, 1947, **57**, № 7, с. 657—659),

$$\text{гр}\,(t_{12}(2),\ t_{21}(2)) = G_2,$$

т. е. любую матрицу из G_2 можно разложить в произведе-

ние степеней трансвекций $a = t_{12}(2)$ и $b = t_{21}(2)$. Идею такого разложения подсказывают формулы:

$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} a^{\alpha} = \begin{pmatrix} x_{11} & x_{12} + 2\alpha x_{11} \\ x_{21} & x_{22} + 2\alpha x_{21} \end{pmatrix},$$
$$\begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} b^{\beta} = \begin{pmatrix} x_{11} + 2\beta x_{12} & x_{12} \\ x_{21} + 2\beta x_{22} & x_{22} \end{pmatrix}.$$

Мы ограничимся тем, что поясним ее на примере матрицы

$$x = \begin{pmatrix} -23 & -86 \\ -4 & -15 \end{pmatrix}.$$

В ней $|x_{12}| > |x_{11}|$. Ищем такое α, чтобы в матрице $x' = xa^{\alpha}$ было $|x'_{12}| < |x'_{11}|$. Для этого делим $x_{12} + |x_{11}|$ на $2x_{11}$ с остатком: $-63 = (-46)\cdot 2 + 29$. Берем $\alpha = -2$ (частное с обратным знаком), тогда

$$x' = xa^{-2} = \begin{pmatrix} -23 & 6 \\ -4 & 1 \end{pmatrix}.$$

Теперь ищем такое β, чтобы в матрице $x'' = x'b^{\beta}$ было $|x''_{12}| > |x''_{11}|$. Делим $x''_{11} + |x'_{12}|$ на $2x'_{12}$ с остатком: $-17 = 12\cdot(-2) + 7$. Берем $\beta = 2$ (частное с обратным знаком), тогда

$$x'' = x'b^2 = \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} = a^3.$$

Значит, $x = a^3b^{-2}a^2$.

14.2.3. Упражнение. Описать и обосновать алгоритм разложения матриц из G_2 по порождающим $t_{12}(2)$, $t_{21}(2)$. Пользуясь им, разложить матрицу $\begin{pmatrix} 321 & -86 \\ 698 & -187 \end{pmatrix}$.

14.3. Подгруппы. Оказывается, что любая подгруппа свободной группы сама свободна. Эта теорема была доказана Нильсеном в 1921 году для конечно порожденных подгрупп, а в полном объеме — Шрайером в 1927 году. В этом пункте мы изложим метод Шрайера, позволяющий находить систему свободных порождающих для подгруппы свободной группы.

Пусть H — подгруппа произвольной группы G. Зафиксируем в каждом правом смежном классе G по H по представителю. Для подгруппы H выбираем представителем 1. Функция, принимающая на любом правом смежном классе постоянное значение — фиксированный представитель этого класса,—называется (правой) *выбирающей*

функцией. Непосредственно проверяются следующие свойства этой функции: $\bar{\bar{u}} = \bar{u}$ и $\overline{\bar{u}\bar{v}} = \overline{uv}$, где $u, v \in G$, а $\bar{u}$ — фиксированный представитель класса Hu.

Выбирающая функция позволяет по порождающим элементам группы строить порождающие элементы подгруппы.

14.3.1. Теорема. *Пусть M — порождающее множество группы G, H — ее подгруппа, $u \mapsto \bar{u}$ — функция, выбирающая правые представители G по H, S — множество выбранных представителей. Тогда*

$$H = \text{гр}\,(\overline{sxsx}^{-1} \mid s \in S,\ x \in M).$$

Доказательство. Ясно, что элементы $\overline{sxsx}^{-1}$ содержатся в подгруппе H. Покажем, что любой элемент из H можно записать как произведение элементов $\overline{sxsx}^{-1}$ и элементов, к ним обратных. Непосредственно проверяется, что

$$(\overline{sxsx}^{-1})^{-1} = s'x^{-1}\overline{s'x^{-1}}^{-1}, \text{ где } s' = \overline{sx},$$

причем по s' однозначно восстанавливается $s = \overline{s'x^{-1}}$. Пусть теперь элемент $u = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$, $x_i \in M$, $\varepsilon_i = \pm 1$, взят из H. Мы должны записать его в виде слова от элементов вида $\overline{sxsx}^{-1}$. Обозначим $u_1 = 1$, $u_{i+1} = x_1^{\varepsilon_1} \dots x_i^{\varepsilon_i}$. Тогда искомой записью будет

$$u = (\bar{u}_1 x_1^{\varepsilon_1} \overline{u_1 x^{\varepsilon_1}}^{-1})(\bar{u}_2 x_2^{\varepsilon_2} \overline{u_2 x_2^{\varepsilon_2}}^{-1}) \dots (\bar{u}_r x_r^{\varepsilon_r} \overline{u_r x_r^{\varepsilon_r}}^{-1}). \qquad (1)$$

Действительно,

$$\overline{u_i x_i^{\varepsilon_i}}^{-1}\ \overline{u_{i\ 1}} = 1, \quad i = 1, \dots, r-1,$$

поэтому правая часть соотношения (1) равна

$$\bar{u}_1 u u_r \overline{x_r^{\varepsilon_r}}^{-1} = 1 \cdot u \cdot \bar{u}^{-1} = 1 \cdot u \cdot 1 = u.$$

Теорема доказана.

14.3.2. Упражнение. Подгруппа конечного индекса в конечно порожденной группе конечно порождена.

14.3.3. Упражнение. Найти в свободной группе F_n порождающие элементы подгруппы слов четной длины.

14.3.4. Упражнение. Пользуясь доказательством теоремы 14.3.1 и формулой упражнения 2.2.4, найти порождающее множество для A_n.

Множество элементов свободной группы, представленных несократимыми словами, называется *шрайеровым*, если вместе с каждым своим элементом оно содержит и все его начальные отрезки.

14.3.5. Теорема (Нильсен — Шрайер). *Пусть X — произвольный алфавит, H — произвольная подгруппа свободной группы $F = F(X)$. Существует по крайней мере одна шрайерова система представителей F по H. Если $u \mapsto \bar{u}$ — соответствующая ей выбирающая функция, то H свободно порождается неединичными элементами $sxs\overline{x}^{-1}$, где s пробегает множество выбранных представителей, а x пробегает X.*

Доказательство. а) Существование шрайеровой системы правых представителей. Назовем *длиной смежного класса* группы F по подгруппе H длину самого короткого слова в нем. Построим шрайерову систему индукцией по длине класса.

Выберем пустое слово в качестве представителя для H. Если L — класс длины 1, то выберем любое слово длины 1 в качестве представителя этого класса. Пусть в классах длины, меньшей r, представители уже выбраны, т. е. на этих классах уже определена выбирающая функция $u \mapsto \bar{u}$, причем длина представителя совпадает с длиной класса. Пусть L — произвольный класс длины r. Возьмем в нем какое-нибудь слово $y_1 \ldots y_r$, $y_i \in X \cup X^{-1}$, и объявим представителем класса L слово $\overline{y_1 \ldots y_{r-1}} y_r$. Ясно, что так построенная система представителей шрайерова.

б) Пусть S — шрайерова система представителей F по H, $u \mapsto \bar{u}$ — соответствующая ей выбирающая функция. Покажем, что неединичные элементы

$$sx\overline{sx}^{-1}, \quad s \in S, \ x \in X, \tag{2}$$

свободно порождают H. Из теоремы 14.3.1 мы уже знаем, что они порождают H. Остается доказать, что эти элементы не связаны нетривиальными соотношениями.

Прежде всего, каждое слово (2) несократимо. Действительно, сокращения могут начаться только на стыках

с буквой x. Но если $s \equiv s_1 x^{-1}$, то $sx\overline{sx}^{-1} = s_1\overline{s_1}^{-1} = 1$, а если $\overline{sx}^{-1} \equiv x^{-1}s_2^{-1}$, то $s = s_2$ и $sx\overline{sx}^{-1} = 1$.

Далее, пусть u, v — неединичные слова вида (2) или к ним обратные, причем $uv \neq 1$. Из доказательства теоремы 14.3.1 мы знаем, что

$u = sx^{\varepsilon}\overline{sx^{\varepsilon}}^{-1}$, $v = ty^{\delta}\overline{ty^{\delta}}^{-1}$, $s, t \in S$, $x, y \in X$, $\varepsilon, \delta = \pm 1$.

Ввиду несократимости слов u, v процесс сокращений в произведении uv может начаться только на стыке. Он заглохнет, не дойдя до x^{ε} слева и y^{δ} справа. Действительно, ввиду шрайеровости системы представителей, если процесс сокращений захватил бы сначала x^{ε}, то было бы $t \equiv s_1 x^{-\varepsilon} w$, где $s_1 \equiv \overline{sx^{\varepsilon}}$, откуда

$$s_1 x^{-\varepsilon} \equiv \overline{s_1 x^{-\varepsilon}} = s.$$

Но это невозможно, поскольку $u \neq 1$. Если же процесс сокращений захватил бы сначала y^{δ}, то было бы $s_1 \equiv ty^{\delta}w$, где $s_1 \equiv \overline{sx^{\varepsilon}}$, откуда

$$ty^{\delta} = \overline{ty^{\delta}}.$$

Но это невозможно, так как $v \neq 1$. Наконец, сократиться одновременно x^{ε}, y^{δ} также не могут, поскольку $uv \neq 1$.

Пусть теперь дано непустое несократимое слово в символах (2). Надо доказать, что если рассматривать его как слово в алфавите X и произвести все возможные сокращения, то останется непустое слово. Но действительно, ввиду сказанного выше, сокращения могут начинаться только на стыках слов (2) и прекращаются, не доходя до их сердцевин x. Теорема доказана.

14.3.6. У п р а ж н е н и е. В группе $F(x, y)$ найти шрайерову систему представителей и с ее помощью свободные порождающие для коммутанта и для наименьшей нормальной подгруппы, содержащей x, y^r, где r — целое число.

Следующая теорема позволяет вычислять степени свободы подгрупп конечного индекса в свободных группах конечной степени.

14.3.7. Т е о р е м а. *Пусть* $F = F(x_1, \ldots, x_n)$, $H \leqslant F$, $|F : H| = j$. *Если* n, j *— конечные числа, то* H *имеет степень*

$$m = 1 + (n - 1)\, j.$$

Доказательство. В обозначениях предыдущей теоремы пусть M — множество всех nj записей вида (2). Нам надо понять, когда эти записи изображают единицу. С этой целью обозначим через S_0 множество S без единицы и определим отображение τ: $S_0 \to M$, полагая

$$s^\tau = \begin{cases} s'x\overline{s'x}^{-1} & \text{при } s \equiv s'x, \quad x \in X, \\ \overline{sxs}^{-1}x & \text{при } s \equiv s'x^{-1}, \quad x \in X. \end{cases}$$

Непосредственно проверяется, что τ — взаимно однозначное отображение S_0 на те записи из M, которые изображают единицу. Так как степень H равна числу остальных записей, т. е. $nj - (j-1)$, то все доказано.

14.3.8. Упражнение. Подгруппа конечного индекса в свободной группе бесконечной степени сама имеет бесконечную степень свободы.

14.3.9. Упражнение. Если F_1, F_2 — свободные подгруппы одного и того же конечного индекса в группе G, то $F_1 \simeq F_2$.

14.4. Ряды централов и коммутантов. Пусть G — произвольная группа. Определим в G убывающий ряд подгрупп

$$\gamma_1 G \geqslant \gamma_2 G \geqslant \ldots \tag{3}$$

следующим образом: $\gamma_1 G = G$, и если подгруппа $\gamma_n G$ уже определена, то $\gamma_{n+1} G = [\gamma_n G, G]$; здесь $[A, B]$ — взаимный коммутант групп A и B. Полученный ряд подгрупп называется *нижним центральным рядом*, а $\gamma_n G$ *n-м централом* группы G. Пересечение всех подгрупп ряда (3) — ω-й *централ* группы G.

Слова

$$\gamma_1(x_1) = x_1,$$
$$\gamma_{n+1}(x_1, \ldots, x_{n+1}) = [\gamma_n(x_1, \ldots, x_n), x_{n+1}], \quad n = 1, 2, \ldots,$$

называются *простыми коммутаторами*, число n — *весом* коммутатора γ_n.

14.4.1. Упражнение. Для любой группы G

$$\gamma_n G = \text{гр}\,(\gamma_n(g_1, \ldots, g_n) \mid g_i \in G), \; n = 1, 2, \ldots$$

14.4.2. Упражнение. Для любой группы G имеем

$$[\gamma_i G, \gamma_j G] \leqslant \gamma_{i+j} G, \quad i, j = 1, 2, \ldots$$

Указание. Применить индукцию и лемму о грех коммутантах 3.2.3.

14.4.3. Упражнение. Для любой группы n-й коммутант лежит в 2^n-м централе, n-й централ подгруппы лежит в n-м централе группы.

14.4.4. Теорема (Магнус). *Во всякой свободной группе F ω-й централ равен единице.*

Доказательство. а) Пусть сначала F счетна. По теореме 14.2.1 она вкладывается в конгруэнц-подгруппу $\Gamma_2(m)$, $m \geqslant 2$, поэтому достаточно убедиться, что ω-й централ группы $\Gamma_2(m)$ равен единице.

Возьмем матрицы

$$g = e + m^k a \in \Gamma_2(m^k) \text{ и } f = e + m^l b \in \Gamma_2(m^l).$$

Пусть $g^{-1} = e + m^k a'$ и $f^{-1} = e + m^l b'$. Тогда коммутатор

$$\begin{aligned}[g, f] &= (e + m^k a')(e + m^l b')(e + m^k a)(e + m^l b) = \\ &= e + (m^k a' + m^k a + m^{2k} a' a) + \\ &\quad + (m^l b' + m^l b + m^{2l} b' b) + \ldots = e + \ldots,\end{aligned}$$

где точками обозначены смешанные произведения типа $m^{2k+l} a' a b$. Ясно, что любое такое смешанное произведение сравнимо с нулевой матрицей по модулю m^{k+l}, а потому $[g, f] \in \Gamma_2(m^{k+l})$.

Проведенное вычисление показывает, что

$$[\Gamma_2(m^k), \Gamma_2(m^l)] \leqslant \Gamma_2(m^{k+l}),$$

поэтому $\gamma_i \Gamma_2(m) \leqslant \Gamma_2(m^i)$. Поскольку $\bigcap_i \Gamma_2(m^i) = e$, то для счетных групп теорема доказана.

б) Пусть теперь F — произвольная свободная группа. Допустим, что ω-й централ F содержит неединичный элемент f. Возьмем для каждого $n = 1, 2, \ldots$ разложение f в произведение простых коммутаторов веса n, соберем все коммутируемые элементы и выразим их через порождающие элементы группы F. Ясно, что при этом будет использовано лишь счетное множество порождающих элементов. Это множество порождает свободную подгруппу. Так как она счетна и не подчиняется теореме Магнуса, то мы получаем противоречие. Теорема доказана.

Ввиду 14.4.3 из нее вытекает, что ω-й коммутант свободной группы, т. е. пересечение всех коммутантов с натуральными номерами, равен единице.

Пусть u — слово в алфавите X. *Логарифмом u по основанию $x \in X$* называется целое число $\log_x u$, равное сумме показателей при букве x в слове u (очевидно, для эквивалентных слов значения логарифма одинаковы). Ясно, что отображение, сопоставляющее каждому u из $F(X)$ набор его логарифмов $\log_x u$ по всем $x \in X$, является гомоморфизмом свободной группы $F(X)$ на свободную абелеву группу того же ранга. Так как слова с одинаковыми логарифмами по всем основаниям лежат в одном смежном классе по коммутанту, то коммутант $[F(X), F(X)]$ будет ядром этого гомоморфизма. Применяя это рассуждение к коммутанту свободной группы и т. д., мы получаем следующий результат:

Секции ряда коммутантов свободной группы — свободные абелевы группы.

Отметим без доказательства, что секции нижнего центрального ряда свободной группы — также свободные абелевы группы (теорема Витта). Это устанавливается значительно более тонкими средствами.

14.4.5. Упражнение. Свободные группы различных степеней свободы не изоморфны.

14.4.6. Упражнение. Используя коммутаторные тождества п. 3.2, доказать, что секции нижнего центрального ряда свободной группы конечной степени являются конечно порожденными абелевыми группами.

§ 15. Многообразия

Подклассы, выделяемые в классе всех групп тождественными соотношениями, называются *многообразиями*. Например, класс абелевых групп — многообразие, выделяемое тождеством $xy = yx$. Многообразия тесно связаны со свободными группами, поскольку тождества — это элементы свободных групп. Теории многообразий посвящено значительное число работ, в том числе книга [21].

Здесь мы введем исходные понятия этой теории и установим, что многообразия совпадают с классами групп, замкнутыми относительно взятия подгрупп, гомоморфных образов и декартовых произведений.

15.1. Тождества и многообразия. Слово v в алфавите $x_1, x_2, \ldots$ называется *тождеством* на классе групп $\mathfrak{X}$, если на любой группе G из $\mathfrak{X}$ оно обращается в единицу, когда аргументы $x_1, x_2, \ldots$ пробегают G. Пусть V — множество слов в алфавите $x_1, x_2, \ldots$, G — группа. В общем случае слова из V не обязаны быть тождествами на G, и их значения на G порождают некоторую подгруппу

$$V(G) = \text{гр}\,(v(g_1, \ldots, g_{n(v)}) \mid v \in V,\ g \in G). \qquad (1)$$

Эта подгруппа называется *вербальной* (= словесной) в G относительно V и в некотором смысле измеряет отклонение группы G от групп многообразия, определяемого тождествами V. Очевидными примерами вербальных подгрупп служат коммутант и d-я степень группы — они определяются словами $[x, y]$, x^d и измеряют отклонение группы от коммутативных групп и от групп периода d.

15.1.1. Упражнение. Централы и последовательные коммутанты группы являются вербальными подгруппами.

15.1.2. Упражнение. Вербальная подгруппа вербальной подгруппы вербальна во всей группе.

15.1.3. Упражнение. Вербальные подгруппы в группе F_∞ — это в точности те подмножества H этой группы, которые удовлетворяют условиям: 1) $u, v \in H \Rightarrow uv \in H$, 2) $u \in H \Rightarrow u^{-1} \in H$, 3) $u \in H$, $v_1, \ldots, v_{n(u)} \in F_\infty \Rightarrow u(v_1, \ldots, v_{n(u)}) \in H$.

Докажем существование и одновременно дадим описание свободных групп в произвольном многообразии в смысле начала гл. 3.

15.1.4. Теорема. *Пусть $\mathfrak{X}$ — многообразие групп, определяемое тождествами V. Пусть X — алфавит,*

$$F_V(X) = F(X)/V(F(X)) \qquad (2)$$

и $*$ обозначает естественный гомоморфизм $F(X) \to F_V(X)$. Если $X = \{x_i \mid i \in I\}$, G — группа из $\mathfrak{X}$ с порождающим множеством $\{g_i \mid i \in I\}$, то отображение $x_i^* \mapsto g_i$ единственным образом продолжается до гомоморфизма $F_V(X) \to G$. Другими словами, группы $F_V(X)$ свободны в многообразии $\mathfrak{X}$. Ими исчерпываются все свободные группы из $\mathfrak{X}$.

Доказательство. а) Ясно, что для получения гомоморфизма $F_V(X) \to G$ надо слову от x_i^* сопоставить

это же слово от g_i. Корректность и гомоморфность этого отображения проверяются непосредственно. Следовательно, $\boldsymbol{F}_V(X)$ — свободная группа в $\mathfrak{V}$.

б) Пусть F — свободная группа в $\mathfrak{V}$ со свободными порождающими f_i, $i \in I$. Отображение $f_i \to x_i^*$ продолжается до гомоморфизма $F \to \boldsymbol{F}_V(X)$, а отображение $x_i^* \to f_i$ продолжается до гомоморфизма $\boldsymbol{F}_V(X) \to F$. Отсюда $F \simeq \boldsymbol{F}_V(X)$. Теорема доказана.

Множество $\{x_i^* \mid i \in I\}$ называется *свободным порождающим множеством* группы $\boldsymbol{F}_V(X)$, а его мощность — *степенью свободы* группы $\boldsymbol{F}_V(X)$. Частными случаями этих понятий являются одноименные понятия для свободных и свободных абелевых групп, встречавшиеся нам раньше. Свободную группу степени n в многообразии $\mathfrak{V}$ обозначают также $\boldsymbol{F}_n(\mathfrak{V})$.

Исчерпывающее описание групп, свободных в многообразии абелевых групп, было дано в § 7. В других многообразиях свободные группы могут быть устроены весьма сложно — см., в частности, § 23.

15.1.5. Упражнение. Группа кватернионов $\mathrm{гр}(x, y \parallel x^4, x^2y^2, x^{-1}yxy)$ не свободна ни в каком многообразии.

Пусть v — слово. Очевидно,

$$v(g_1, \ldots, g_r)^\varphi = v(g_1^\varphi, \ldots, g_n^\varphi)$$

для любого гомоморфизма $\varphi\colon G \to G^*$, поэтому гомоморфный образ вербальной подгруппы $V(G)$ лежит в вербальной подгруппе $V(G^*)$. В частности, всякая вербальная подгруппа эндоморфно допустима.

15.1.6. Упражнение. Указать в $\mathbb{C}_2 \times \mathbb{C}_4$ эндоморфно допустимую, но не вербальную подгруппу.

Для групп, свободных в многообразии, ситуация упрощается:

15.1.7. Теорема. *Пусть $\mathfrak{V}$ — многообразие групп, G — группа, свободная в $\mathfrak{V}$. Любая эндоморфно допустимая подгруппа H группы G вербальна.*

Доказательство. Возьмем в G свободно порождающее множество $\{g_i \mid i \in I\}$ и рассмотрим в $\boldsymbol{F}_\infty$ множество V слов $v(x_{i_1}, \ldots, x_{i_m})$ с условием, что $v(g_{i_1}, \ldots, g_{i_m}) \in H$. Покажем, что $H = V(G)$. Включение $H \leqslant V(G)$ очевидно. Обратно, пусть $v \in V$, $g_i \in G$.

Надо показать, что

$$v(g'_{i_1}, \ldots, g'_{i_m}) \in H.$$

Но ввиду свободы G в $\mathfrak{L}$ отображение $g_i \mapsto g'_i$ можно продолжить до эндоморфизма группы G. Так как $v(g_{i_1}, \ldots, g_{i_m}) \in H$ и H эндоморфно допустима, то $v(g'_{i_1}, \ldots, g'_{i_m}) \in H$. Теорема доказана.

Соответствие между многообразиями и определяющими их множествами слов из F_∞ не взаимно однозначно, поскольку два различных множества слов могут определять одно и то же многообразие. С другой стороны, множество всех тождеств, истинных на данном многообразии, является вербальной подгруппой в F_∞, и легко проверить, что это соответствие между многообразиями и вербальными подгруппами взаимно однозначно. Поэтому изучение многообразий и изучение вербальных подгрупп в F_∞ — равносильные задачи.

15.1.8. Упражнение. Подгруппа, порожденная в F_∞ вербальными подгруппами, вербальна. Какое многообразие она определяет?

Два множества тождеств V, W называются *эквивалентными*, если они определяют одно и то же многообразие групп или, что равносильно, если $V(F_\infty) = W(F_\infty)$.

15.1.9. Упражнение. Любое конечное множество тождеств эквивалентно одному тождеству.

(Отметим, однако, что далеко не каждое многообразие групп может быть задано одним тождеством.)

15.1.10. Теорема. *Любое множество V слов в алфавите $x_1, x_2, \ldots$ эквивалентно множеству вида $W = \{x_1^d, u_j \mid j \in J\}$, где $d > 0$, u_j — слова из коммутанта группы $F(x_1, x_2, \ldots)$.*

Доказательство. Запишем каждое v из V в виде

$$v = x_{i_1}^{m_1} \ldots x_{i_s}^{m_s} u,$$

где все значки $i_1, \ldots, i_s$ различны, а u — элемент коммутанта группы $F(x_1, x_2, \ldots)$. Пусть d — общий наибольший делитель чисел $m_1, \ldots, m_s$ по всем v из V. Число d и элементы u, взятые по всем v из V,— искомые. Действительно, ясно, что $V(F_\infty) \leqslant W(F_\infty)$. Обратно, слова $x_{i_k}^{m_k}$ содержатся в $V(F_\infty)$ — они получаются из v, когда ос-

тальные алфавитные буквы посылаются в единицу,— поэтому и слова x_1^d, u содержатся в $V(\boldsymbol{F}_\infty)$. Теорема доказана.

15.2. Другой подход к многообразиям. Если $\mathfrak{L}$ — класс групп, то пусть $S\mathfrak{L}$, $Q\mathfrak{L}$, $C\mathfrak{L}$ обозначают соответственно замыкания этого класса относительно операций взятия подгрупп, гомоморфных образов и декартовых произведений. Если $\mathfrak{L}$ — многообразие, то, очевидно, $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$, $C\mathfrak{L} = \mathfrak{L}$. Оказывается, справедлива и обратная

15.2.1. Теорема (Биркгоф). *Пусть $\mathfrak{L}$ — класс групп. Если $S\mathfrak{L} = \mathfrak{L}$, $Q\mathfrak{L} = \mathfrak{L}$, $C\mathfrak{L} = \mathfrak{L}$, то $\mathfrak{L}$ — многообразие.*

Доказательство. Пусть V — все тождества, истинные на $\mathfrak{L}$, $\overline{\mathfrak{L}}$ — многообразие, определяемое ими. Очевидно, $\mathfrak{L} \subseteq \overline{\mathfrak{L}}$ и надо убедиться, что $\overline{\mathfrak{L}} \subseteq \mathfrak{L}$. Поскольку $Q\mathfrak{L} = \mathfrak{L}$, то достаточно проверить, что любая группа F, свободная в $\overline{\mathfrak{L}}$, принадлежит $\mathfrak{L}$, а ввиду соотношений $C\mathfrak{L} = \mathfrak{L}$, $S\mathfrak{L} = \mathfrak{L}$ для этого достаточно вложить F в декартово произведение групп из $\mathfrak{L}$. Укажем такое вложение.

Согласно теореме 15.1.4

$$F = \boldsymbol{F}(X)/V(\boldsymbol{F}(X))$$

при подходящем алфавите $X = \{x_i \mid i \in I\}$. Для каждого слова $v(x_{i_1}, \ldots, x_{i_m})$, не принадлежащего множеству V, возьмем в $\mathfrak{L}$ группу G_v, а в ней элементы g_{vi}, $i \in I$, на которых

$$v(g_{vi_1}, \ldots, g_{vi_m}) \neq 1.$$

Возьмем декартово произведение

$$\overline{\prod_{v \notin V}} G_v,$$

а в нем подгруппу, порожденную элементами f_i, $i \in I$, где $f_i(v) = g_{vi}$. Так как элементы f_i не подчиняются никаким соотношениям, кроме тождеств из V, то порожденная ими подгруппа изоморфна F. Теорема доказана.

Легко видеть, что в действительности мы доказали равенство

$$\overline{\mathfrak{L}} = QSC\mathfrak{L} \tag{3}$$

для произвольного класса групп $\mathfrak{L}$.

15.2.2. Упражнение. Пусть G — конечная группа, $\mathfrak{M}$ — многообразие, определяемое всеми тождествами, истинными на G. Любая конечно порожденная группа из $\mathfrak{M}$ конечна.

Указание: воспользоваться формулой (3) при $\mathfrak{L} = \{G\}$.

15.2.3. Упражнение. В конечно порожденной группе G любая подгруппа H конечного индекса содержит вербальную подгруппу конечного индекса.

Решение. Ввиду 2.5.13 можно считать, что H нормальна в G. Пусть V — система всех тождеств, истинных на конечной группе G/H, $\mathfrak{M}$ — многообразие, определяемое этими тождествами. Так как группа $G/V(G)$ конечно порождена и принадлежит $\mathfrak{M}$, то она конечна (упражнение 15.2.2).

15.2.4. Упражнение. Указать классы групп $\mathfrak{L}$, $\mathfrak{M}$, $\mathfrak{N}$ с условиями:

$$\begin{array}{lll} S\mathfrak{L} \neq \mathfrak{L}, & Q\mathfrak{L} = \mathfrak{L}, & C\mathfrak{L} = \mathfrak{L}, \\ S\mathfrak{M} = \mathfrak{M}, & Q\mathfrak{M} \neq \mathfrak{M}, & C\mathfrak{M} = \mathfrak{M}, \\ S\mathfrak{N} = \mathfrak{N}, & Q\mathfrak{N} = \mathfrak{N}, & C\mathfrak{N} \neq \mathfrak{N}. \end{array}$$

Глава 6

НИЛЬПОТЕНТНЫЕ ГРУППЫ

В предыдущих главах мы познакомились с абелевыми и конечными группами. Произвольная группа не обязана принадлежать этим двум семействам, но всегда так или иначе связана с ними. Установить возможно больше таких связей и с их помощью изучить саму группу — вот привычный путь многих работ по теории групп. На этом пути придуманы многочисленные условия, близкие к условиям коммутативности или конечности группы, начиная от самых естественных и кончая весьма причудливыми и просто вздорными.

Важнейшие обобщения коммутативности — разрешимость и нильпотентность. Разрешимые группы — это группы, которые можно собрать из абелевых групп посредством нескольких последовательных расширений. Замечательны они, в частности, своей связью с задачей о разрешимости алгебраических уравнений в радикалах (см. введение), которой обязаны и самим названием.

Нильпотентные группы составляют класс, промежуточный между абелевыми и разрешимыми группами. Они определяются более сложно и допускают более глубокое изучение.

Мы посвятим эту главу изучению нильпотентных групп, а следующую главу — изучению разрешимых групп. Много интересных фактов теории нильпотентных и разрешимых групп можно найти в [15, 30, 39, 44].

§ 16. Общие свойства и примеры

16.1. Определение. Пусть G — группа. Нормальная матрёшка

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_s = G \qquad (1)$$

называется *центральной*, если все ее секции центральны, т. е.

$$G_{i+1}/G_i \leqslant Z(G/G_i) \text{ для всех } i \qquad (2)$$

или, что равносильно,

$$[G_{i+1},\ G] \leqslant G_i \text{ для всех } i. \tag{3}$$

Группа, обладающая центральными матрёшками, называется *нильпотентной* (название будет объяснено ниже), а минимальное число секций таких матрёшек — ее *ступенью нильпотентности*. Непосредственно из определения видно, что нильпотентные группы составляют класс, промежуточный между классами абелевых и разрешимых групп, причем абелевы группы — это в точности нильпотентные группы ступени 1.

16.1.1. Упражнение. Всякая матрёшка подгрупп с условием (3) автоматически является нормальной.

Пусть G — произвольная группа. Мы можем попытаться построить в ней центральную матрёшку, руководствуясь либо формулой (2), либо формулой (3). Именно, пусть

$$\zeta_0 G = 1,\ \zeta_{i+1}G/\zeta_i G = Z\,(G/\zeta_i G),\ i = 0,\ 1,\ 2,\ \ldots,$$
$$\gamma_1 G = G,\ \gamma_{j+1}G = [\gamma_j G,\ G],\ j = 1,\ 2,\ \ldots.$$

Подгруппы $\zeta_i G$ называются *гиперцентрами* группы G, а подгруппы $\gamma_i G$ — это знакомые нам *централы* группы G (те и другие легко определяются для произвольных трансфинитных номеров, но мы не хотим сейчас погружаться в эту трясину). Ясно, что если некоторый гиперцентр совпадает со всей группой или некоторый централ совпадает с единицей, то группа нильпотентна.

Обратно, пусть группа G нильпотентна и (1) — произвольная центральная матрёшка в ней. Положим для краткости $Z_i = \zeta_i G$, $\Gamma_j = \gamma_j G$. Определения и легкая индукция дают следующие включения:

$$\begin{array}{ccccccccc} 1 = Z_0 & \leqslant & Z_1 & \leqslant & \ldots & & & & \\ \vee & & \vee & & & & & & \\ 1 = G_0 & \leqslant & G_1 & \leqslant & \ldots & \leqslant & G_{s-1} & \leqslant & G_s = G, \\ & & & & & & \vee & & \vee \\ & & & & & & \Gamma_2 & \leqslant & \Gamma_1 = G. \end{array} \tag{4}$$

Отсюда видно, что в нильпотентной группе ряды гиперцентров и централов являются матрёшками, т. е. содержат 1 и G, и число секций в каждой из них равно ступени нильпотентности группы. Под влиянием диаграммы (4)

эти ряды называются *верхним центральным* и *нижним центральным* (второй термин формально уже был введен в п. 14.4, но только сейчас получил объяснение). Хотя верхняя и нижняя центральные матрёшки нильпотентной группы имеют одинаковое число членов, сами матрёшки не обязаны совпадать — см. упражнения 16.2.10 и 16.2.11.

16.1.2. Пример. Пусть K — поле, $n \geqslant 3$. Пользуясь формулами (9), (12) из 3.2.1, нетрудно проверить, что ряд

$$\boldsymbol{UT}_n(K) = \boldsymbol{UT}_n^1(K) \geqslant \boldsymbol{UT}_n^2(K) \geqslant \ldots \geqslant \boldsymbol{UT}_n^n(K) = 1$$

является одновременно верхней и нижней центральной матрёшкой в группе $\boldsymbol{UT}_n(K)$. В частности, эта группа нильпотентна ступени $n - 1$. В работе одного из авторов (Мерзляков Ю. И.— Алгебра и логика, 1964, 3, № 4, с. 49—58) вычислены центральные ряды других матричных групп, в том числе нижние центральные ряды главных конгруэнц-подгрупп над локальными кольцами и силовских p-подгрупп из $\boldsymbol{GL}_n(\mathbb{Z}_{p^m})$. В последнем случае, например, получается такое описание. Пусть для краткости $K = \mathbb{Z}_{p^m}$. Возьмем пустую матрицу степени n, т. е. квадрат, разбитый на n горизонтальных и n вертикальных полос, и покроем ее *ковром идеалов* K, pK, p^2K, ... следующим образом (на схеме $n = 3$):

$$\begin{array}{rccc|ccc|ccc}
\ldots p^2K & p^2K & p^2K & pK & pK & K & K & K & & \\
\ldots p^2K & p^2K & p^2K & pK & pK & pK & K & K & K & \\
\ldots p^2K & p^2K & p^2K & pK & pK & pK & pK & K & K & K \\
\underbrace{\qquad\qquad\qquad\qquad}_{n} & & & & \underbrace{\qquad\qquad\qquad}_{n} & & & \underbrace{\qquad\qquad}_{n} & &
\end{array}$$

Пусть G — силовская p-подгруппа из $\boldsymbol{GL}_n(K)$. Как мы знаем, она состоит из всех матриц степени n над K, сравнимых с единичной матрицей по модулю ковра идеалов в отмеченном положении (упражнение 11.3.3). Оказывается, что при $r \geqslant 2$ централ $\gamma_r G$ содержит те и только те матрицы из $\boldsymbol{SL}_n(K)$, которые сравнимы с единицей по модулю ковра идеалов, сдвинутого на $r - 1$ шагов вправо. Более формально, пусть K — ассоциативное кольцо с единицей. Система его идеалов $\mathfrak{a} = \{\mathfrak{a}_{ij} \mid i, j \in \mathbb{Z}\}$ называется *ковром идеалов*, если

$$\mathfrak{a}_{ik}\mathfrak{a}_{kj} \subseteq \mathfrak{a}_{ij} \quad \text{для всех } i, j, k \in \mathbb{Z}.$$

Легко проверить, что если K коммутативно, то

$$\Gamma_n(\mathfrak{a}) = \{x \in \boldsymbol{SL}_n(K) \mid x_{ij} \equiv \delta_{ij} \bmod \mathfrak{a}_{ij}\}$$

— группа; она называется (*специальной*) *конгруэнц-подгруппой по модулю ковра* $\mathfrak{a}$ или *ковровой подгруппой* (в частности, при $K = \mathbb{Z}$, $\mathfrak{a}_{ij} = (m)$ получается $\Gamma_n(m)$ из 4.2.7). В этих обозначениях упомянутый выше результат гласит (теперь уже на языке формул, а не рисунков): если G — силовская p-подгруппа группы $\boldsymbol{GL}_n(K)$, $K = \mathbb{Z}_{p^m}$, то

$$\gamma_r G = \Gamma_n(\mathfrak{a}^{(n,r)}), \quad r = 2, 3, \ldots,$$

где

$$\mathfrak{a}_{ij}^{(n,r)} = p^{-[(j-i-r)/n]}K;$$

квадратные скобки означают взятие целой части и $p^l K = K$ при $l \leqslant 0$. Отсюда видно, в частности, что силовская p-подгруппа группы $\boldsymbol{GL}_n(\mathbb{Z}_{p^m})$ нильпотентна ступени $mn - 1$.

Из замечания после формулы (4) ясно, что группа G тогда и только тогда нильпотентна ступени $\leqslant s$, когда $\gamma_{s+1}G = 1$. Поэтому класс $\mathfrak{N}_s$ всех нильпотентных групп ступени $\leqslant s$ есть многообразие, определяемое тождеством

$$\gamma_{s+1}(x_1, \ldots, x_{s+1}) \equiv [x_1, \ldots, x_{s+1}] = 1$$

(см. упражнение 14.4.1). В частности, $\mathfrak{N}_s$ замкнуто относительно взятия подгрупп, гомоморфных образов и декартовых произведений. Согласно общей теории гл. 5 многообразие $\mathfrak{N}_s$ обладает свободными группами; все они имеют вид

$$\boldsymbol{F}(X)/\gamma_{s+1}\boldsymbol{F}(X)$$

при подходящем алфавите X.

16.1.3. Упражнение. Пусть G — свободная нильпотентная группа ступени 2 со свободными порождающими a, b. Пусть еще $c = [b, a]$. Каждый элемент g из G единственным образом записывается в виде $g = a^\alpha b^\beta c^\gamma$ с целыми α, β, γ, причем

$$a^\alpha b^\beta c^\gamma \cdot a^{\alpha'} b^{\beta'} c^{\gamma'} = a^{\alpha+\alpha'} b^{\beta+\beta'} c^{\gamma+\gamma'+\alpha'\beta}.$$

Следовательно, отображение $a^\alpha b^\beta c^\gamma \mapsto \begin{pmatrix} 1 & \beta & \gamma \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$ является изоморфизмом G на $\boldsymbol{UT}_3(\mathbb{Z})$.

Несколько слов о терминологии. Свое нынешнее название нильпотентные группы получили не сразу — долго их называли ничего не говорящим словом «специальные». Между тем в теории колец уже давно работало понятие нильпотентного, т. е. «потенциально нулевого» кольца — это кольцо, в котором произведение данного числа любых элементов равно нулю:

$$x_1 \dots x_n = 0 \tag{5}$$

(таково, например, кольцо треугольных матриц степени n с нулевой диагональю). Классическая теория Ли установила соответствие между особым классом колец — кольцами Ли — и особым классом групп — группами Ли,— при котором умножению в кольцах соответствует коммутирование в группах и, в частности, тождеству (5) соответствует тождество

$$[x_1, \dots, x_n] = 1. \tag{6}$$

По этой причине термин «нильпотентная» в конце концов закрепился и за группами с тождеством (6). Отметим, что теория групп не осталась в долгу перед теорией колец — разрешимые кольца Ли были названы так по аналогии с разрешимыми группами.

Иногда ступень нильпотентности называют классом нильпотентности. Это менее удобно, так как порождает стилистические шедевры вроде «класса нильпотентных групп данного класса».

О связи между нильпотентностью в кольцах и группах еще раз напоминает

16.1.4. Упражнение. Пусть A — ассоциативное кольцо с единицей, B — его подкольцо, B^n — подкольцо, порожденное произведениями $b_1 \dots b_n$, $b_i \in B$. Если подкольцо B нильпотентно, т. е. $B^n = 0$ при некотором n, то множества $G^{(i)} = \{1 + x \mid x \in B^i\}$ являются группами относительно умножения в A, причем $[G^{(i)}, G^{(j)}] \leqslant G^{(i+j)}$. В частности, все они нильпотентны ступени $\leqslant n$. Это вновь доказывает нильпотентность некоторых групп примера 16.1.2, но уже без описания центральных матрёшек.

16.1.5. Упражнение. В любой нильпотентной группе без кручения единица — единственный элемент, сопряженный со своим обратным.

16.1.6. Упражнение. Периодические конечно порожденные нильпотентные группы конечны.

Указание: воспользоваться упражнением 14.3.2.

16.2. Общие свойства. Само определение нильпотентных групп подсказывает ясный и обычно безотказный путь их изучения — индукцию по ступени нильпотентности. Проводя индукцию, чаще всего работают с централами и гиперцентрами, но иногда используют и другие подгруппы. В этой связи полезна

16.2.1. Лемма. *Пусть G — нильпотентная группа ступени $s \geqslant 2$. Любая ее подгруппа, порожденная коммутантом и одним элементом, имеет ступень нильпотентности меньше s.*

Доказательство. Пусть $a \in G$, $H = (a, [G, G])$. Так как

$$[G, G] \leqslant (\zeta_{s-1}G) \cap H \leqslant \zeta_{s-1}H,$$

то группа $H/\zeta_{s-1}H$ циклическая. Поскольку фактор-группа по центру не может быть циклической, отличной от 1, то $\zeta_{s-1} H = H$, что и требовалось.

Свойства нильпотентных групп, которые мы установим в этом пункте, относятся в основном к подгруппам.

16.2.2. Теорема. *Любая подгруппа нильпотентной группы субнормальна. Более точно, если G — нильпотентная группа ступени s, то для любой ее подгруппы H ряд последовательных нормализаторов достигает G не позже чем через s шагов.*

Доказательство. Введем обозначения

$$Z_i = \zeta_i G, \quad H_0 = H, \quad H_{j+1} = N_G(H_j).$$

Достаточно проверить, что $Z_i \leqslant H_i$. Для $i = 0$ это очевидно. Перейдем от i к $i + 1$. Так как

$$[G, Z_{i+1}] \leqslant Z_i \leqslant H_i,$$

то

$$H_i^{Z_{i+1}} \leqslant H_i\,[H_i, Z_{i+1}] \leqslant H_i.$$

Это означает, что Z_{i+1} нормализует H_i, т. е. $Z_{i+1} \leqslant H_{i+1}$. Теорема доказана.

16.2.3. Теорема. *В нильпотентной группе любая нетривиальная нормальная подгруппа имеет нетривиальное пересечение с центром.*

Доказательство проводится индукцией по ступени нильпотентности. Пусть G — нильпотентная группа, $H \trianglelefteqslant G$, $H \neq 1$, $Z_i = \zeta_i G$. Если $H \leqslant Z_1$, то утверждение тривиально. Пусть $H \not\leqslant Z_1$. Тогда по индуктивному предположению, примененному к G/Z_1, пересечение $HZ_1 \cap Z_2$ содержит некоторый элемент $a \notin Z_1$. Так как

$$a = hz, \quad h \in H, \quad z \in Z_1,$$

то $h \in H \cap Z_2$, $h \notin Z_1$. Пусть элемент $g \in G$ таков, что $[h, g] \neq e$. Тогда

$$[h, g] \in H \cap [Z_2, G] \leqslant H \cap Z_1,$$

т. е. пересечение $H_i \cap Z_1$ нетривиально. Теорема доказана.

16.2.4. Упражнение. В нильпотентной группе любая нормальная подгруппа простого порядка лежит в центре.

16.2.5. Теорема. *Пусть G — нильпотентная группа. Если A — ее подгруппа с условием $A[G, G] = G$, то $A = G$. В частности,*

$$[G, G] \leqslant \Phi(G). \tag{7}$$

Доказательство. Пусть, напротив, $A \neq G$. Положим $A_i = A \cdot \zeta_i G$, $i = 0, 1, 2, \ldots$. Очевидно, $A_i \trianglelefteqslant A_{i+1}$. Пусть $A_m < G$, $A_{m+1} = G$. Так как секция A_{m+1}/A_m абелева, то $[G, G] \leqslant A_m$, откуда

$$A[G, G] \leqslant A_m < G.$$

Противоречие. Утверждение о подгруппе Фраттини вытекает из ее описания как множества непорождающих элементов (теорема 2.2.6). Теорема доказана.

[Откроем здесь одну тайну. Приводя примеры подгрупп Фраттини в 2.2.7, мы установили включение $\Phi(\boldsymbol{UT}_n(\mathbb{Z})) \leqslant \boldsymbol{UT}_n^2(\mathbb{Z})$ и сообщили (оставив доказательство читателю!), что верно и обратное включение. При этом мы имели в виду как раз теорему 16.2.5.]

16.2.6. Теорема. *В любой нильпотентной группе G любая максимальная абелева нормальная подгруппа A совпадает со своим централизатором. В частности, A — максимальная абелева подгруппа и G/A изоморфно вкладывается в* Aut A.

Доказательство. Обозначим $H = C_G(A)$, $Z_i = \zeta_i G$. Пусть уже доказано, что $H \cap Z_i \leqslant A$, и пусть

$x \in H \cap Z_{i+1}$. Для всякого $g \in G$ имеем $[x, g] \in H \cap Z_i \leqslant A$, поэтому гр (x, A) — абелева нормальная подгруппа из G, содержащая A. Ввиду максимальности A имеем $x \in A$, т. е. $H \cap Z_{i+1} \leqslant A$. Так как $Z_n = G$ при некотором n, то $H = A$, что и требовалось доказать.

Элементы конечных порядков будем коротко называть *периодическими элементами*.

16.2.7. Теорема. *В любой нильпотентной группе G совокупность τG периодических элементов есть подгруппа (периодическая часть группы G).*

Доказательство проводится индукцией по ступени нильпотентности с использованием леммы 16.2.1. Пусть a, b — периодические элементы группы G. Положим

$$A = (a, [G, G]), \quad B = (b, [G, G]).$$

По индуктивному предположению τA, τB — подгруппы в A, B соответственно. Так как τA эндоморфно допустима в A, а A нормальна в G, то τA нормальна в G. По той же причине τB нормальна в G. Так как любой элемент из $\tau A \cdot \tau B$ при возведении в подходящую степень попадает сначала в τB, а затем в 1, то группа $\tau A \cdot \tau B$ периодическая. В частности, элементы ab, a^{-1} периодические, что и требовалось доказать.

16.2.8. Теорема. *В любой нильпотентной группе G без кручения извлечение корней — однозначная операция (хотя и не обязательно всюду определенная), т. е. из $a^n = b^n$, $n \neq 0$, следует $a = b$.*

Доказательство проводится индукцией по ступени нильпотентности. Так как для абелевых групп теорема очевидна, то будем считать, что G неабелева. Рассмотрим подгруппу $(a, [G, G])$. Она нормальна в G и имеет меньшую ступень нильпотентности (лемма 16.2.1). Так как $a, a^b \in (a, [G, G])$ и, очевидно, $(a^b)^n = a^n$, то по индуктивному предположению $a^b = a$. Значит, элементы a и b перестановочны, откуда $(ab^{-1})^n = e$. Так как G без кручения, то $a = b$. Теорема доказана.

16.2.9. Упражнение. В любой нильпотентной группе без кручения $x^m y^n = y^n x^m$ $(m, n \neq 0) \Rightarrow xy = yx$.

Указание: $(y^{-n} x y^n)^m = x^m \Rightarrow y^{-n} x y^n = x$ и т. д.

16.2.10. Упражнение. В нильпотентных группах без кручения все факторы верхнего центрального ряда тоже без кручения.

16.2.11. Упражнение. Аналог для нижнего центрального ряда неверен: например, если

$$G=\begin{pmatrix}1 & n\mathbb{Z} & \mathbb{Z}\\ 0 & 1 & \mathbb{Z}\\ 0 & 0 & 1\end{pmatrix},\quad \text{то}\quad [G,G]=\begin{pmatrix}1 & 0 & n\mathbb{Z}\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix},$$

откуда $G/[G,\ G]\simeq\mathbb{Z}\oplus\mathbb{Z}\oplus\mathbb{Z}_n$.

Рассмотрим теперь нильпотентные нормальные подгруппы в произвольных группах.

16.2.12. Теорема (Фиттинг). *Во всякой группе произведение двух нормальных нильпотентных подгрупп ступеней s, t есть нормальная нильпотентная подгруппа ступени $\leqslant s+t$.*

Доказательство. Пусть $A\trianglelefteqslant G$, $B\trianglelefteqslant G$, $\gamma_{s+1}A=1$, $\gamma_{t+1}B=1$. Тогда

$$\gamma_n(AB)=[\underbrace{AB,\ldots,AB}_{n}]=\prod[H_1,\ldots,H_n], \tag{8}$$

где каждое H_i совпадает либо с A, либо с B (см. 3.2.6). Так как $\gamma_iA\overset{e}{\leqslant}A\trianglelefteqslant G$, то $\gamma_iA\trianglelefteqslant G$ и, значит,

$$[\gamma_iA,\ B]\leqslant\gamma_iA \text{ для всех } i.$$

Таким образом, если i членов из $H_1,\ \ldots,\ H_n$ совпадают с A, а остальные $n-i$ совпадают с B, то

$$[H_1,\ \ldots,\ H_n]\leqslant\gamma_iA\cap\gamma_{n-i}B. \tag{9}$$

Возьмем $n=s+t+1$. Тогда либо $i\geqslant s+1$, либо $n-i\geqslant t+1$, откуда ввиду (8), (9) $\gamma_n(AB)=1$. Теорема доказана.

16.2.13. Упражнение. Пусть класс $\mathfrak{K}$ состоит из всех групп G с условием

$$\gamma_\omega G\equiv\bigcap_{n=1}^{\infty}\gamma_nG=1.$$

Произведение двух нормальных подгрупп, принадлежащих $\mathfrak{K}$, не обязано принадлежать $\mathfrak{K}$ — противоречащим примером служит

$$SL_n(\mathbb{Z})=\Gamma_n(2)\cdot\Gamma_n(3).$$

16.3. Нильпотентные группы автоморфизмов. Как было отмечено в примере 16.1.2, любая группа унитреугольных

матриц нильпотентна. Но ведь матрицы — это автоморфизмы векторного пространства с фиксированной базой, а унитреугольные матрицы — это в точности те автоморфизмы, которые оставляют на месте матрёшку подпространств, натянутых на убывающие конечные отрезки базы, и действуют тождественно в секциях этой матрёшки. Оказывается, это свойство и есть подлинная причина нильпотентности.

16.3.1. Лемма. *Пусть в группе G задана $(r+1)$-членная нормальная матрёшка*

$$G = G_0 \geqslant G_1 \geqslant \ldots \geqslant G_r = 1 \tag{10}$$

и Φ — группа всех автоморфизмов группы G, оставляющих члены матрёшки (10) *инвариантными и действующих тождественно в секциях G_i/G_{i+1}* (стабилизатор *матрёшки* (10)). *Будем рассматривать G, Φ как подгруппы голоморфа* Hol G. *Группы Φ и $[G, \Phi]$ нильпотентны ступени $< r$.*

Доказательство. а) Группа Φ нильпотентна ступени $< r$. Действительно, по условию

$$G_i^{\Phi} = G_i,\ [G_i,\ \Phi] \leqslant G_{i+1} \text{ для всех } i. \tag{11}$$

Пусть Φ_j — централизатор в Φ секций G_i/G_{i+j}, $i = 0, 1, 2, \ldots$ Очевидно,

$$\Phi = \Phi_1 \geqslant \Phi_2 \geqslant \ldots \geqslant \Phi_r = 1,$$

и нам достаточно доказать, что это центральная матрёшка в Φ, т. е.

$$[\Phi_j,\ \Phi] \leqslant \Phi_{j+1} \text{ для всех } j$$

или

$$[G_i, [\Phi_j, \Phi]] \leqslant G_{i+j+1} \text{ для всех } i, j.$$

Но это следует из соотношений

$$[\Phi_j, [\Phi,\ G_i]] \leqslant [\Phi_j,\ G_{i+1}] \leqslant G_{i+j+1},$$
$$[\Phi, [G_i, \Phi_j]] \leqslant [\Phi, G_{i+j}] \leqslant G_{i+j+1}$$

ввиду леммы о трех коммутантах 3.2.3.

б) Группа $[G, \Phi]$ нильпотентна ступени $< r$. Действительно,

$$[G, [\Phi,\ G_i]] \leqslant [G,\ G_{i+1}] \leqslant G_{i+1},$$
$$[\Phi, [G_i, G]] \leqslant [\Phi,\ G_i] \leqslant G_{i+1},$$

поэтому, снова ввиду леммы о трех коммутантах,

$$[G_i, [G, \Phi]] \leqslant G_{i+1} \text{ для всех } i.$$

Это означает, что сопряжения элементами из $[G, \Phi]$ действуют тождественно в секциях матрёшки $G_1 \geqslant G_2 \geqslant \ldots \ldots \geqslant G_r = 1$. По уже доказанному утверждению а) группа этих сопряжений, т. е.

$$[G, \Phi]/C_{[G,\Phi]}(G_1),$$

нильпотентна ступени $< r - 1$. Но $[G, \Phi] \leqslant G_1$, поэтому $C_{[G,\Phi]}(G_1)$ лежит в центре $[G, \Phi]$. Отсюда и следует б). Лемма доказана.

Теперь естественно пойти дальше и спросить себя: не будет ли нильпотентным стабилизатор произвольной матрёшки подгрупп, не обязательно нормальной? Здесь под стабилизатором матрёшки (10) понимается максимальная подгруппа Φ из $\mathrm{Aut}\, G$ с условием (11). Оказывается, ответ и в этом случае будет утвердительный, хотя доказательство усложняется, а оценка ступени нильпотентности ухудшается:

16.3.2. Теорема (Ф. Холл). *Стабилизатор любой $(r+1)$-членной матрёшки подгрупп есть нильпотентная группа ступени $\leqslant \binom{r}{2}$.*

Доказательство проводится индукцией по r. Пусть Φ — стабилизатор матрёшки (10). Пусть еще $\Psi = C_\Phi(G_1)$. Так как Φ стабилизирует r-членную матрёшку $G_1 \geqslant G_2 \geqslant \ldots$, то по индуктивному предположению группа Φ/Ψ нильпотентна ступени $\leqslant \binom{r-1}{2}$, т. е.

$$\Phi^{(1+\binom{r-1}{2})} \leqslant \Psi.$$

Обозначим

$$\Psi_1 = \Psi, \qquad \Psi_{i+1} = [\Psi_i, \Phi].$$

Так как $\Psi \trianglelefteq \Phi$, то $\Psi = \Psi_1 \geqslant \Psi_2 \geqslant \ldots$ Нам достаточно доказать, что $[G, \Psi_r] = 1$. Для этого мы проверим, что $[G, \Psi_i] \leqslant G_i$ для всех i. Для $i = 1$ это очевидно. Перейдем от i к $i+1$. Пусть $g \in G$, $\psi_{i+1} \in \Psi_{i+1}$. Надо показать, что $[\psi_{i+1}, g] \in G_{i+1}$. Но ψ_{i+1} — слово от коммутаторов вида

$$[\psi_i, \varphi^{-1}], \quad \psi_i \in \Psi_i, \quad \varphi \in \Phi.$$

Элемент ψ_{i+1}^g — то же самое слово от произведений

$$[\psi_i, \varphi^{-1}]^g = [\psi_i, \varphi^{-1}]\,[\psi_i, \varphi^{-1}, g]. \tag{12}$$

Заметим, что

$$[\psi_i, \varphi^{-1}, g] \in G_{i+1}$$

ввиду тождества Ф. Холла (см. 3.2.3) и соотношений

$$[\varphi, g^{-1}, \psi_i] \in [\Phi, G, \Psi_i] \leqslant [G_1, \Psi] = 1,$$
$$[g, \psi_i^{-1}, \varphi] \in [G, \Psi_i, \Phi] \leqslant [G_i, \Phi] \leqslant G_{i+1}.$$

Таким образом, в произведении (12) левый множитель принадлежит Ψ, а правый G_{i+1}. Но Ψ централизует $G_1 \geqslant G_{i+1}$, поэтому $\psi_{i+1}^g \in \psi_{i+1} G_{i+1}$. Отсюда $[\psi_{i+1}, g] \in$ $\in G_{i+1}$ и всё доказано.

Вот как далеко привел нас пример 16.1.2!

§ 17. Важнейшие подклассы

17.1. Конечные нильпотентные группы. Другим важным источником нильпотентных групп является следующий

17.1.1. Пример. Любая конечная p-группа G нильпотентна. Действительно, группа G имеет нетривиальный центр. Для доказательства заметим, что элемент тогда и только тогда является центральным, когда он составляет полный класс сопряженных элементов. Так как

$$|\, a^G \,| = |\, G : N_G(a) \,|,$$

то мощности c_i классов сопряженных элементов группы G являются степенями числа p. Так как единица составляет полный класс сопряженных элементов, то по крайней мере одно из чисел c_i равно 1. Но их сумма $\sum c_i = |\, G \,|$ делится на p, поэтому еще несколько чисел c_i должны равняться 1. Таким образом, G имеет нетривиальный центр Z_1. По той же причине G/Z_1 имеет нетривиальный центр Z_2/Z_1 и т. д. Мы видим, что достаточно большой гиперцентр группы G совпадает с G. Значит, G нильпотентна.

17.1.2. Упражнение. Пусть p — простое число. Существуют только две неизоморфные группы порядка p^2: $\mathbb{Z}_{p^2}$ и $\mathbb{Z}_p \times \mathbb{Z}_p$. Групп порядка p^3 имеется пять — три абелевых:

$$\mathbb{Z}_{p^3}, \quad \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \quad \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$$

и две неабелевых: при $p = 2$ это группа диэдра

$$\text{гр}\ (a, b \parallel a^4 = 1,\ b^2 = 1,\ bab = a^{-1})$$

и группа кватернионов

$$\text{гр}\ (a, b \parallel a^4 = 1,\ b^2 = a^2,\ b^{-1}ab = a^{-1}),$$

а при $p > 2$ — группы

$$\text{гр}\ (a, b \parallel a^{p^2} = 1,\ b^p = 1,\ b^{-1}ab = a^{1+p}),$$

$$\text{гр}\ (a, b, c \parallel a^p = 1,\ b^p = 1,\ c^p = 1,$$
$$[a, b] = c,\ [a, c] = [b, c] = 1).$$

Бесконечные p-группы могут не быть нильпотентными,— например, прямое сплетение любой нетривиальной p-группы с бесконечной p-группой есть p-группа без центра (см. упражнение 6.2.3). Конкретный пример: $\mathbb{C}_{p^\infty} \wr \mathbb{C}_{p^\infty}$. Другой хороший способ лишить группу центра — постоянно смещать его в связи с укрупнением:

17.1.3. Упражнение. Пусть K — поле положительной характеристики p, $UT_\omega(K)$ — группа бесконечных матриц над K, у которых строки и столбцы занумерованы натуральными числами, по диагонали стоит 1, под ней — нули, а над диагональю лишь конечное число элементов отлично от нуля. Группа $UT_\omega(K)$ является p-группой без центра (см. формулу (2) из 3.1.1).

Оказывается, прямыми произведениями конечного числа конечных p-групп исчерпываются все конечные нильпотентные группы. Более того, справедлива

17.1.4. Теорема (Бернсайд — Виланд). *Пусть G — конечная группа. Следующие условия равносильны:*

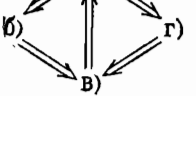
а) *G нильпотентна,*

б) *любая подгруппа из G субнормальна,*

в) *G — прямое произведение своих силовских p-подгрупп,*

г) $[G, G] \leqslant \Phi(G)$.

Доказательство проведем по следующей схеме:



а) $\Rightarrow$ б). См. теорему 16.2.2.

б) $\Rightarrow$ в). Пусть P — силовская p-подгруппа из G. Так как $N_G(P)$ совпадает со своим нормализатором в G (упражнение 11.1.4), а ввиду б) нормализатор всякой собственной подгруппы больше ее самой, то $N_G(P) = G$. Таким образом, силовские p-подгруппы нормальны в G. Отсюда уже легко получается в).

в) $\Rightarrow$ а). См. пример 17.1.1.

а) $\Rightarrow$ г). См. теорему 16.2.5.

г) $\Rightarrow$ в). Опять достаточно проверить, что любая силовская p-подгруппа P из G нормальна в G. Пусть, напротив, $N_G(P)$ — собственная подгруппа в G и H — содержащая ее максимальная подгруппа из G. Так как

$$[G, G] \leqslant \Phi(G) \leqslant H,$$

то H нормальна в G. С другой стороны, H содержит $N_G(P)$, а потому должна совпадать со своим нормализатором в G (упражнение 11.1.4). Этим противоречием заканчивается доказательство теоремы.

Из теоремы Бернсайда — Виланда непосредственно следует, что сплетение конечной p-группы, отличной от 1, с конечной q-группой, отличной от 1, тогда и только тогда нильпотентно, когда $p = q$.

17.1.5. Упражнение. Какова ступень нильпотентности сплетения $\mathbb{Z}_{p^m} \wr \mathbb{Z}_p$?

Исчерпывающий ответ на вопрос, когда бывают нильпотентными сплетения, содержится в следующем упражнении.

17.1.6. Упражнение. Пусть A, B — нильпотентные неединичные группы. Каждое из сплетений $A \wr B$, $A \bar{\wr} B$ тогда и только тогда нильпотентно, когда A, B являются p-группами, причем A имеет конечный период, а B конечна.

Указание: воспользоваться упражнениями 6.2.1 и 6.2.3 и естественным гомоморфизмом $\mathbb{Z} \wr \mathbb{Z}_p \to \mathbb{Z}_q \wr \mathbb{Z}_p$.

Отметим в заключение этого пункта факт, относящийся к произвольным конечным группам.

17.1.7. Теорема (Фраттини). *Подгруппа Фраттини конечной группы нильпотентна.*

Доказательство. Пусть G — конечная группа, A — ее подгруппа Фраттини. Ввиду теоремы 17.1.4 достаточно проверить, что любая силовская p-подгруппа

P группы A нормальна в A или, что равносильно, в G (см. упражнение 5.2.6), т. е. $N_G(P) = G$. Но это равносильно соотношению

$$G = A \cdot N_G(P),$$

так как множество A конечно и состоит из непорождающих элементов группы G (теорема 2.2.6). Последнее соотношение мы и докажем.

Пусть g — произвольный элемент из G. Сопряжение G посредством g отображает A в себя, поэтому P^g — снова силовская p-подгруппа из A. По теореме Силова 11.1.1 подгруппы P и P^g сопряжены некоторым элементом $a \in A$, т. е. $P^g = P^a$. Отсюда $ga^{-1} \in N_G(P)$, $g \in A \cdot N_G(P)$. Теорема доказана.

Отметим, что попутно нами доказана

17.1.8. Лемма Фраттини. *Пусть A — нормальная подгруппа конечной группы G, P — ее силовская p-подгруппа. Тогда $G = A \cdot N_G(P)$.*

17.1.9. Упражнение. Пусть A — нормальная подгруппа группы G и B — такая подгруппа из A, что B, $B' \leqslant A$ сопряжены в A тогда и только тогда, когда эти подгруппы сопряжены в G. Тогда $G = A \cdot N_G(B)$. (Обобщенная лемма Фраттини.)

17.2. Конечно порожденные нильпотентные группы. Очевидный пример таких групп — $\boldsymbol{UT}_n(\mathbb{Z})$. Оказывается, подгруппами унитреугольных групп над $\mathbb{Z}$ исчерпываются вообще все конечно порожденные нильпотентные группы без кручения, а произвольные конечно порожденные нильпотентные группы являются их конечными расширениями и, в частности, вкладываются в группы $\boldsymbol{SL}_n(\mathbb{Z})$. Мы установим здесь два эти факта, основные в теории конечно порожденных нильпотентных групп.

17.2.1. Лемма. *Пусть G — произвольная группа. Если G порождается множеством M, то централ $\gamma_i G$ порождается следующим централом $\gamma_{i+1}G$ и простыми коммутаторами веса i от элементов из M.*

Доказательство. Для $i = 1$ это очевидно. Перейдем от i к $i+1$. По определению $\gamma_{i+1}G$ порождается элементами $[x, y]$, $x \in \gamma_i G$, $y \in G$. По индуктивному предположению $x = x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m} z$, где каждое x_j — простой коммутатор веса i от элементов из M, $z \in \gamma_{i+1}G$, $\varepsilon_j = \pm 1$. Далее, y — слово от элементов из $M \cup M^{-1}$. Используя

коммутаторные соотношения (3) из п. 3.2, мы видим, что $[x, y]$ — слово от элементов вида

$$[x_j, a]^g = [x_j, a]\,[x_j, a, g],\ [z, a]^g,$$
$$a \in M,\ g \in G.$$

Так как $[x_j, a, g]$, $[z, a]$ принадлежат $\gamma_{i+2}G$, то всё доказано.

Мы будем говорить, что *группа почти* или *почти вся обладает некоторым свойством*, если она содержит нормальную подгруппу конечного индекса, обладающую этим свойством.

17.2.2. Т е о р е м а. *Любая конечно порожденная нильпотентная группа G обладает центральной матрёшкой с циклическими секциями и почти вся без кручения. Если G вся без кручения, то она обладает центральной матрёшкой с бесконечными циклическими секциями.*

Д о к а з а т е л ь с т в о. а) Пусть G конечно порождена и нильпотентна. Каждая секция ее нижней центральной матрёшки — конечно порожденная абелева группа (см. 17.2.1) и, значит, обладает матрёшкой с циклическими секциями. Поскольку уплотнение центральной матрёшки — снова центральная матрёшка, то G обладает центральной матрёшкой с циклическими секциями. Индукцией по числу членов матрёшки докажем, что G почти вся без кручения. Пусть H — максимальный член матрёшки, отличный от G, a — элемент, порождающий $G \pmod H$. По индуктивному предположению H почти без кручения, поэтому при некотором m подгруппа $H^m = (h^m \mid h \in H)$ без кручения. Ввиду 16.1.6 $|H : H^m| < \infty$. Если $|G : H| < \infty$, то H^m — искомая подгруппа без кручения в G. Пусть $|G : H| = \infty$. Тогда $(a)\,H^m$ содержит искомую подгруппу, так как она без кручения и

$$|G : (a)\,H^m| = |H : H \cap (a)\,H^m| \leqslant |H : H^m| < \infty.$$

б) Пусть G — нильпотентная группа без кручения. По доказанному она полициклическая, поэтому секции ее верхней центральной матрёшки — тоже полициклические (упражнение 4.4.3). Так как они — группы без кручения (упражнение 16.2.10), то верхняя центральная матрёшка уплотняется до матрёшки с бесконечными циклическими секциями. Теорема доказана.

17.2.3. У п р а ж н е н и е. Любая полициклическая группа почти вся не имеет кручения.

Указание: см. доказательство 17.2.2.

17.2.4. Упражнение. В любой конечно порожденной нильпотентной группе периодическая часть конечна. Более общо, в любой группе почти без кручения периодические подгруппы конечны.

Теорема 17.2.2 позволяет в конечно порожденную нильпотентную группу G без кручения внести целочисленные координаты специального вида и с их помощью представить G целочисленными унитреугольными матрицами. Более точно, пусть G — множество. Набор функций $f_i: G \to \mathbb{Z}$, $i = 1, \ldots, s$, называется *координатным*, если отображение $x \mapsto (f_1(x), \ldots, f_s(x))$ является взаимно однозначным отображением множества G в множество $\mathbb{Z}^s$ всех целочисленных s-ок. Пусть $G \subseteq \mathbb{Z}^s$. Отображение $\varphi: G \to \mathbb{Z}^r$ называется *полиномиальным*, если существуют такие многочлены $f_1, \ldots, f_r$ от s переменных с коэффициентами из поля $\mathbb{Q}$, что

$$x^\varphi = (f_1(x), \ldots, f_r(x)) \text{ для } x \in G.$$

Если $f_1, \ldots, f_r$ — многочлены первой степени, то φ называется *линейным*. Пусть теперь G — конечно порожденная нильпотентная группа без кручения. Рассмотрим в ней центральную матрёшку

$$G = G_1 > G_2 > \ldots > G_{s+1} = 1$$

с бесконечными циклическими секциями и возьмем элементы $a_1, \ldots, a_s$ с условием $G_i = \mathrm{гр}(a_i, G_{i+1})$. Очевидно, каждый элемент x из G однозначно записывается в виде

$$x = a_1^{t_1(x)} \ldots a_s^{t_s(x)}, \quad t_i(x) \in \mathbb{Z},$$

так что набор функций $t_1, \ldots, t_s$ является координатным. Упорядоченную систему $a_1, \ldots, a_s$ назовем *мальцевской базой* группы G, а числа $t_1(x), \ldots, t_s(x)$ — *координатами* элемента x в этой базе.

17.2.5. Теорема. *Пусть G — конечно порожденная нильпотентная группа без кручения с отмеченными на ней мальцевскими координатами $t_1, \ldots, t_s$. Существуют натуральное число $n = n(G)$ и такое изоморфное вложение $\varphi: G \to UT_n(\mathbb{Z})$, что отображение φ полиномиально на G, а обратное к нему отображение φ^{-1} линейно на G^φ (в матричных координатах, имеющихся на $UT_n(\mathbb{Z})$).*

В частности, умножение и возведение в степень в группе G записываются многочленами в мальцевских координатах. Более точно, если $x, y \in G$, $m \in \mathbb{Z}$, $1 \leqslant i \leqslant s$, то

$t_i(xy)$ = *многочлен над* $\mathbb{Q}$

$$\text{от } \{t_\alpha(x), t_\alpha(y) \mid \alpha < i\} + t_i(x) + t_i(y), \tag{1}$$

$t_i(x^m)$ = *многочлен над* $\mathbb{Q}$

$$\text{от } m \text{ и } \{t_\alpha(x) \mid \alpha < i\} + mt_i(x). \tag{2}$$

Доказательство. а) Выведем сначала утверждение «в частности». Для любой матрицы a из $\boldsymbol{UT}_n(\mathbb{Z})$ и любого m из $\mathbb{Z}$ мы имеем

$$a^m = \sum_{i=0}^{n-1} \binom{m}{i} (a-e)^i, \text{ где } \binom{m}{i} = \frac{m(m-1)\ldots(m-i+1)}{i!},$$

$$\binom{m}{0} = 1, \tag{3}$$

т. е. коэффициенты матрицы a^m являются многочленами от m и коэффициентов матрицы a. В силу основного утверждения теоремы координаты $t_i(xy)$, $t_i(x^m)$ линейно выражаются через коэффициенты матриц $(xy)^\varphi$, $(x^m)^\varphi$, которые полиномиально выражаются через коэффициенты матриц x^φ, y^φ и число m. Снова по основному утверждению теоремы коэффициенты матриц x^φ, y^φ полиномиально выражаются через координаты $t_\alpha(x)$, $t_\alpha(y)$, поэтому мальцевские координаты произведения xy и степени x^m являются многочленами от мальцевских координат элементов x, y и числа m. То, что эти многочлены имеют вид (1), (2), сразу вытекает из определения центральной матрёшки.

б) Теперь заметим, что вместо вложения φ достаточно указать полиномиальное вложение $\psi\colon G \to \boldsymbol{GL}_n(\mathbb{Z})$, обратное к которому ψ^{-1} линейно на G^ψ, причем G^ψ состоит из унипотентных матриц (матрица a называется *унипотентной*, если она имеет единственный характеристический корень 1 или, что равносильно, $(a-e)^n = 0$). Действительно, группу $H = G^\psi$ путем сопряжения в $\boldsymbol{GL}_n(\mathbb{Q})$ можно отобразить в $\boldsymbol{UT}_n(\mathbb{Z})$. Мы докажем сначала, что H сопряжена с подгруппой из $\boldsymbol{UT}_n(\mathbb{Q})$. Будем рассматривать $\boldsymbol{GL}_n(\mathbb{Q})$ как группу автоморфизмов n-мерного векторного пространства V над полем $\mathbb{Q}$ и возьмем неуплотняемую матрёшку $V = V_1 > V_2 > \ldots > V_{m+1} = 0$

подпространств, инвариантных относительно H. В базе, отнесенной к этой матрёшке, автоморфизмы из H записываются клеточно-треугольными матрицами, диагональные клетки которых изображают действие H в секциях V_i/V_{i+1}, поэтому достаточно доказать, что каждая такая секция U имеет размерность 1. Так как коммутант $[H, H]$ имеет меньшую ступень нильпотентности, то можно считать, что $[H, H]$ приводится к унитреугольному виду. Тогда существует ненулевой вектор $u \in U$, неподвижный относительно автоморфизмов из $[H, H]$. Пусть U' — подпространство всех таких векторов. Оно инвариантно относительно H, так как для $h \in H$, $h' \in [H, H]$ имеем

$$(uh)\, h' = u\,(hh'h^{-1})h = uh.$$

Так как секция U не содержит собственных подпространств, инвариантных относительно H, то $U' = U$. Отсюда $[H, H] = 1$ на U, т. е. H индуцирует абелеву группу автоморфизмов секции U. Но любое множество перестановочных линейных преобразований имеет общий собственный вектор над расширением основного поля с помощью характеристических корней этих преобразований. Так как группа H унипотентна, то она имеет общий собственный вектор в U. Так как подпространство, натянутое на этот вектор, инвариантно относительно H и U не содержит собственных инвариантных подпространств, то U одномерно. Этим доказано, что $H^a \leqslant \boldsymbol{UT}_n(\mathbb{Q})$ при подходящем $a \in \boldsymbol{GL}_n(\mathbb{Q})$. Возьмем теперь в H^a конечное число порождающих матриц, возьмем общий знаменатель N их коэффициентов и рассмотрим матрицу

$$b = \operatorname{diag}(1, N, N^2, \ldots, N^{n-1}).$$

Легко видеть, что $H^{ab} \leqslant \boldsymbol{UT}_n(\mathbb{Z})$.

в) Остается доказать существование ψ. Мы сделаем это индукцией по длине мальцевской базы. Пусть для групп с мальцевской базой длины $< s$ требуемое матричное представление уже найдено, а вместе с ним доказана и вся теорема (см. а), б)). Пусть группа G имеет мальцевскую базу $a_1, \ldots, a_s$ длины s. В качестве подготовки к построению ψ мы установим в этом пункте формулу (1) для группы G. Обозначим для краткости $t_i(x) = \xi_i$, $t_i(y) = \eta_i$. Очевидно,

$$xy = a_1^{\xi_1+\eta_1}(a_1^{-\eta_1}a_2^{-1}a_1^{\eta_1})^{-\xi_2}\ldots(a_1^{-\eta_1}a_s^{-1}a_1^{\eta_1})^{-\xi_s}a^{\eta_2}\ldots a_s^{\eta_s}$$

и

$$a_1^{-\eta} a_i^{-1} a_1^{\eta} = [a_1^{\eta}, a_i]\, a_i^{-1}.$$

По индуктивному предположению и ввиду а), б) формулы (1), (2) справедливы для групп с мальцевской базой длины $< s$, поэтому достаточно проверить, что координаты элементов $[a_1^{\eta}, a_i]$ в мальцевской базе $a_2, \ldots, a_s$ — многочлены от η. Очевидно,

$$[a_1^{\eta}, a_i] = a_1^{-\eta} (a_i^{-1} a_1 a_i)^{\eta}$$

и

$$a_i^{-1} a_1 a_i = a_1 a_{i+1}^{c_{i,\, i+1}} \ldots a_s^{c_{is}}, \quad c_{ij} \in \mathbb{Z}.$$

Применяя к гр $(a_1, a_{i+1}, \ldots, a_s)$ индуктивное предположение, мы заключаем, что

$$(a_i^{-1} a_1 a_i)^{\eta} = a_1^{\eta} a_{i+1}^{\zeta_{i,\, i+1}} \ldots a_s^{\zeta_{is}},$$

где ζ_{ij} — многочлены от η. Отсюда $[a_1^{\eta}, a_i] = a_{i+1}^{\zeta_{i,\, i+1}} \ldots a_s^{\zeta_{is}}$, и формула (1) доказана для группы G.

г) Построение ψ. Пусть $\mathbb{Q}[t]$ — кольцо многочленов над $\mathbb{Q}$ от функций $t_1, \ldots, t_s$. Определим на нем действие группы G, полагая для a из G

$$f^a(x) = f(ax), \quad f \in \mathbb{Q}[t], \quad x \in G$$

(«левый сдвиг аргумента»). Непосредственно проверяется, что оператор $\mathrm{op}(a)$, задаваемый этой формулой, является автоморфизмом кольца $\mathbb{Q}[t]$, а правило $a \mapsto \mathrm{op}(a)$ определяет изоморфизм $G \to \mathrm{Aut}(\mathbb{Q}[t])$.

Произведение вида $M(t) = t_1^{m_1} \ldots t_s^{m_s}$ назовем *одночленом* от $t_1, \ldots, t_s$. Ввиду (1)

$$t_i^a = t_i + \sum_j c_{ij}(a)\, M_j(t), \tag{4}$$

где $c_{ij}(a)$ — многочлен над $\mathbb{Q}$ от мальцевских координат элемента a, а одночлены $M_j(t)$, входящие с ненулевыми коэффициентами в выражение для t_i^a, не содержат переменных $t_i, \ldots, t_s$. Отсюда видно, что $\mathrm{op}(a) - \mathrm{op}(e)$ отображает произвольный одночлен $M(t)$ либо в 0, либо в линейную комбинацию меньших одночленов, если считать одночлены упорядоченными по последним различным показателям. Значит, при подходящем $m = m(a, M)$ преобразование $(\mathrm{op}(a) - \mathrm{op}(e))^m$ аннулирует $M(t)$.

Пусть H — аддитивная подгруппа, порожденная орбитой множества координатных функций $\{t_1, \ldots, t_s\}$ относительно операторов $\mathrm{op}(x)$, $x \in G$. Ввиду (4) H лежит в подгруппе, порожденной функциями $\{t_i, \frac{1}{N} M_j(t)\}$ при некотором натуральном N, а потому конечно порождена. Пусть $h_1, \ldots, h_n$ — база свободной абелевой группы H. Пусть еще

$$h_k^x = \sum_l \psi_{kl}(x)\, h_l, \tag{5}$$

т. е. $(\psi_{kl}(x))$ — матрица сужения $\mathrm{op}(x)$ на H в базе $h_1, \ldots, h_n$. Так как H содержит координатные функции $t_1, \ldots, t_s$, то правило $x \mapsto (\psi_{kl}(x))$ определяет изоморфизм $\psi\colon G \to GL_n(\mathbb{Z})$, причем G^ψ состоит из унипотентных матриц. Отображение ψ^{-1} линейно на G^ψ, так как множество $\{t_i\}$ линейно выражается через $\{h_k\}$, а вычисляя функции (5) в точке e, мы видим, что $\{h_k\}$ линейно выражается через $\{\psi_{kl}\}$. Само ψ полиномиально, т. е. функции ψ_{kl} являются сужениями на G некоторых многочленов над $\mathbb{Q}$. Действительно, пусть $x \in G$. Так как каждое h_k — линейная комбинация над $\mathbb{Z}$ от некоторых t_i^g, $g \in G$, то ввиду (4) h_k^x — такая же комбинация от

$$t_i^{gx} = t_i + \sum_j c_{ij}(gx)\, M_j(t).$$

Отсюда

$$h_k^x = \sum_j P_{kj}(x)\, M_j(t), \tag{6}$$

где P_{kj} — многочлен над $\mathbb{Q}$; в частности,

$$h_k = \sum_j P_{kj}(e)\, M_j(t). \tag{7}$$

Так как множество $\{h_k\}$ линейно независимо над $\mathbb{Q}$, то таковы и строки матрицы $(P_{kj}(e))$. Подставляя (6), (7) в (5) и пользуясь линейной независимостью $\{M_j(t)\}$, получим для $\psi_{kl}(x)$ систему линейных уравнений

$$P_{kj}(x) = \sum_l \psi_{kl}(x)\, P_{lj}(e),$$

откуда и видно, что функции ψ_{kl} полиномиальны над $\mathbb{Q}$. **Теорема доказана.**

В связи с приведенным доказательством уместно отметить здесь общий *метод расщепляемых координат* (Мерзляков Ю. И.— Алгебра и логика, 1968, **7**, № 3, с. 63—104), позволяющий устанавливать изоморфную представимость групп матрицами. Изложение этого метода можно найти в [20].

17.2.6. Упражнение. Пусть p — простое число. Любая конечно порожденная нильпотентная группа без кручения аппроксимируется конечными p-группами.

Указание: см. доказательство теоремы 14.2.2.

В начале пункта мы отметили, что из теорем 17.2.2 и 17.2.5 следует вложимость произвольной конечно порожденной нильпотентной группы G в группу $SL_n(\mathbb{Z})$ при некотором n. Ясно, что достаточно указать вложение $\varphi\colon G \to GL_m(\mathbb{Z})$, так как тогда вложение $x \mapsto \begin{pmatrix} x^\varphi & 0 \\ 0 & x^\varphi \end{pmatrix}$ будет требуемым. Остается воспользоваться следующим общим замечанием. Пусть H — подгруппа конечного индекса m в произвольной группе G. Пусть $a_1, \ldots, a_m$ — правые представители G по H. Если σ — точное представление группы H матрицами степени n, то формула

$$g \mapsto \| (a_i g a_j^{-1})^\sigma \|$$

задает точное представление группы G матрицами степени mn (здесь считается $x^\sigma = 0$ при $x \notin H$). Очевидно, это не что иное, как представление группы G, индуцированное представлением σ (см. п. 12.2).

17.2.7. Упражнение. Группа, почти вся представимая матрицами над кольцом с единицей, вся представима матрицами над этим кольцом.

17.2.8. Упражнение. Любая конечно порожденная нильпотентная группа финитно аппроксимируема.

17.2.9. Упражнение. Существуют конечно порожденные нильпотентные группы без кручения A, B, изоморфно вложимые одна в другую, но не изоморфные,— таковы, например,

$$A = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & n\mathbb{Z} & \mathbb{Z} \\ 0 & 0 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix} \text{ при } n \neq 0, 1.$$

17.2.10. Упражнение. Конечно порожденная нильпотентная группа с конечным центром сама конечна.

17.3. Нильпотентные группы без кручения. В этом классе групп наиболее интересна и содержательна теория извлечения корней, которая и будет сейчас изложена. Ее исходным пунктом служит теорема 16.2.8 предыдущего параграфа, согласно которой в любой нильпотентной группе G без кручения извлечение корней есть частичная операция, т. е. оно однозначно, хотя и не обязательно всюду определено. Оказывается, группу G всегда можно вложить в полную нильпотентную группу (где извлечение корней всюду определено), причем любые два «минимальных» нильпотентных пополнения группы G изоморфны друг другу и исчерпываются корнями из элементов группы G.

Напомним, что произвольная группа G называется *полной*, если для любого ее элемента g и любого натурального m в G существует решение уравнения $x^m = g$. Примером полной группы является группа $UT_n(K)$ над полем K нулевой характеристики. Действительно, для любых $a \in UT_n(K)$, $\mu \in K$ положим по определению, обобщая формулу (3):

$$a^\mu = \sum_{i=0}^{n-1} \binom{\mu}{i} (a-e)^i,$$

где

$$\binom{\mu}{i} = \frac{\mu(\mu-1)\ldots(\mu-i+1)}{i!}, \quad \binom{\mu}{0} = 1.$$

Непосредственно проверяется, что

$$a^{\mu+\nu} = a^\mu a^\nu, \quad a^{\mu\nu} = (a^\mu)^\nu.$$

Отсюда, в частности, следует, что $a^{\frac{1}{m}}$ — корень m-й степени из a, т. е. группа $UT_n(K)$ полна.

Полная нильпотентная группа $\bar{G}$ без кручения называется (*нильпотентным*) *пополнением* группы G, если она содержит G и не содержит собственных полных подгрупп, содержащих G.

17.3.1. Т е о р е м а. *Пусть H — подгруппа полной нильпотентной группы G без кручения. Множество $\sqrt{H}$ всех элементов из G, попадающих в некоторой степени в H* (корень *из подгруппы H в группе G*), *является подгруппой и, значит, пополнением H в G. Гиперцентры подгрупп H*

и $\sqrt{H}$ *связаны следующим образом*:

$$\zeta_i \sqrt{H} = \sqrt{\zeta_i H}, \quad \zeta_i H = H \cap \sqrt{\zeta_i H}.$$

Доказательство. а) Докажем сначала, что $\sqrt{H}$ — подгруппа, т. е. $xy \in \sqrt{H}$, если $x \in \sqrt{H}$, $y \in \sqrt{H}$. Пусть $A = (x, y)$, $B = A \cap H$, $A_i = \gamma_i A$. Достаточно проверить, что все $|BA_i : BA_{i+1}| < \infty$, так как тогда будет $|A : B| < \infty$. Ряд

$$BA_1 \geqslant BA_2 \geqslant \ldots$$

субнормальный с абелевыми секциями, так как ввиду коммутаторных тождеств (3) из п. 3.2

$$[BA_i, BA_i] \leqslant [B, B]^{A_i} [A_i, B]^{A_i} [A_i, A_i] \leqslant BA_{i+1}.$$

Пусть $x^m, y^m \in B$ и уже доказано, что секция BA_{i-1}/BA_i конечна и имеет период m^{i-1}. Докажем, что секция BA_i/BA_{i+1} конечно порождена и имеет период m^i. Первое вытекает из полициклличности A (теорема 17.2.2). Далее, $[A_{i-1}, A, A] \equiv 1 \pmod{A_{i+1}}$, поэтому функция $[u, v] \pmod{A_{i+1}}$, $u \in A_{i-1}$, $v \in A$, гомоморфна по обоим аргументам (снова коммутаторные тождества!). Отсюда

$$A_i^{m^i} = [A_{i-1}, A]^{m^i} \leqslant [A_{i-1}^{m^{i-1}}, A^m] A_{i+1}.$$

Так как

$$A_{i-1}^{m^{i-1}} \leqslant (B \cap A_{i-1}) A_i, \quad A^m \leqslant BA_2,$$

то, применяя еще раз коммутаторные тождества, получаем

$$A_i^{m^i} \leqslant BA_{i+1},$$

что и требовалось.

б) Для доказательства формул о гиперцентрах обозначим $H_i = \zeta_i H$ и перейдем от i к $i + 1$. Прежде всего, $\zeta_{i+1} \sqrt{H} \leqslant \sqrt{H_{i+1}}$, так как для любого x из $\zeta_{i+1} \sqrt{H}$ имеем $x^m \in H$ при подходящем m и

$$[x^m, H] \leqslant H \cap \sqrt{H_i} = H_i,$$

откуда $x^m \in H_{i+1}$, $x \in \sqrt{H_{i+1}}$. Обратно, $\sqrt{H_{i+1}} \leqslant \zeta_{i+1} \sqrt{H}$, т. е. подгруппы $\sqrt{H}$, $\sqrt{H_{i+1}}$ поэлементно перестановочны по модулю $\sqrt{H_i}$. Действительно, пусть

$x \in \sqrt{H}$, $y \in \sqrt{H_{i+1}}$, т. е. $x^m \in H$, $y^n \in H_{i+1}$ при подходящих m, n. Так как $[H, H_{i+1}] \leqslant H_i \leqslant \sqrt{H_i}$, то $x^m y^n \equiv y^n x^m \pmod{\sqrt{H_i}}$. Так как $\sqrt{H}/\sqrt{H_i}$ — группа без кручения (упражнение 16.2.10), то $xy \equiv yx \pmod{\sqrt{H_i}}$ (упражнение 16.2.9), что и требовалось.

Наконец, $H \cap \sqrt{H_{i+1}} = H_{i+1}$. Докажем только нетривиальное включение $H \cap \sqrt{H_{i+1}} \leqslant H_{i+1}$. Пусть $x \in H \cap \sqrt{H_{i+1}}$, $x^m \in H_{i+1}$. Тогда x^m перестановочно с любым элементом из H по модулю H_i, а, значит, таково и x (упражнения 16.2.9 и 16.2.10). Отсюда $x \in H_{i+1}$. Теорема доказана.

17.3.2. Т е о р е м а (А. И. Мальцев). *Любая нильпотентная группа G без кручения обладает нильпотентным пополнением той же ступени нильпотентности. Любые два нильпотентных пополнения группы G изоморфны; более того, для любого автоморфизма φ группы G существует изоморфизм между ними, продолжающий φ.*

Д о к а з а т е л ь с т в о. а) Е д и н с т в е н н о с т ь. Пусть G_1, G_2 — группы, изоморфные G, φ — изоморфизм G_1 на G_2, $\sqrt{G_i}$ — нильпотентное пополнение группы G_i. Возьмем прямое произведение $P = \sqrt{G_1} \times \sqrt{G_2}$, в нем подгруппу $D = \{x x^\varphi \mid x \in G_1\}$ и рассмотрим ее корень $\sqrt{D}$ в этом произведении. Проверим, что

$$P = \sqrt{D} \cdot \sqrt{G_i}, \quad \sqrt{D} \cap \sqrt{G_i} = 1 \text{ при } i = 1, 2. \tag{8}$$

Действительно, если $x \in \sqrt{D} \cap \sqrt{G_i}$, то $x^m \in D \cap G_i$ при подходящем m. Отсюда $x = 1$, и вторая из формул (8) доказана. Из нее следует, что сужение проектирования $\pi\colon P \to \sqrt{G_1}$ на группу $\sqrt{D}$ есть изоморфизм, следовательно, $\sqrt{D}^\pi = \sqrt{D^\pi}$. Далее, сужение π на $\sqrt{G_1}$ — тоже изоморфизм, поэтому $\sqrt{G_1}^\pi = \sqrt{G_1^\pi}$. Но $D^\pi = G_1^\pi$, поэтому $\sqrt{D}^\pi = \sqrt{G_1^\pi}$. Возвращаясь к полным прообразам относительно π, получаем первую из формул (8) для $i = 2$. По симметрии она верна и для $i = 1$.

Формулы (8) показывают, что любой элемент x_1 из $\sqrt{G_1}$ является проекцией точно одного элемента x из $\sqrt{D}$ на множитель $\sqrt{G_1}$. Сопоставляя элементу x_1 проекцию

элемента x на множитель $\sqrt{G_1}$, мы получим изоморфизм $\sqrt{G_1}$ на $\sqrt{G_2}$, продолжающий φ.

б) Существование. Если группа G конечно порождена, то она вкладывается в полную нильпотентную группу $\boldsymbol{UT}_n(\mathbb{Q})$ при некотором n (теорема 17.2.5). Корень $\sqrt{G}$ из подгруппы G в группе $\boldsymbol{UT}_n(\mathbb{Q})$ будет нильпотентным пополнением группы G. Для g из G и натурального m обозначим $\sqrt[m]{g}$ решение уравнения $x^m = g$ в группе $\sqrt{G}$. Очевидно,

$$\sqrt[m]{g} = \sqrt[m']{g'} \Leftrightarrow g^{m'} = g'^{m}, \tag{9}$$

причем ввиду а) таблица умножения в $\sqrt{G}$ полностью определяется таблицей умножения в G. Отбросим теперь предположение, что G конечно порождена, и рассмотрим множество формальных символов $\sqrt[m]{g}$, $g \in G$, $m = 1, 2, \ldots$ Определим на этом множестве формулой (9) отношение равенства и обозначим через $\sqrt{G}$ получившееся множество классов равных элементов. Условимся умножать $\sqrt[m]{g}$, $\sqrt[m']{g'}$ как элементы нильпотентного пополнения группы гр(g, g'). Тогда $\sqrt{G}$ становится группой, содержащей подгруппу G. Если группа G нильпотентна ступени s, то пополнения ее конечно порожденных погрупп имеют ступени $\leqslant s$ (теорема 17.3.1), поэтому $\sqrt{G}$ удовлетворяет тождеству $[x_1, \ldots, x_{s+1}] = 1$. Значит, $\sqrt{G}$ — нильпотентное пополнение группы G с той же самой ступенью нильпотентности. Теорема доказана.

Нильпотентная группа, содержащая периодические элементы, уже не всегда вкладывается в полную нильпотентную группу, так как периодическая часть полной нильпотентной группы G обязана лежать в центре. Действительно, по индуктивным соображениям можно считать, что любой периодический элемент g из G лежит во втором гиперцентре. Если $g^m = 1$, $m \neq 0$, то $[g, x^m] = [g, x]^m = [g^m, x] = 1$ для произвольного x из G. Ввиду полноты G элемент x^m пробегает всю группу, поэтому элемент g центральный.

§ 18. Обобщения нильпотентности

Из многочисленных обобщений нильпотентности мы рассмотрим только три: локальную нильпотентность, нормализаторное условие и энгелевость.

18.1. Локальная нильпотентность. Говорят, что группа *локально нильпотентна*, если все ее конечно порожденные подгруппы нильпотентны. При этом сама группа может не быть нильпотентной, как показывает пример прямого произведения нильпотентных групп неограниченно растущих ступеней или пример группы $UT_\omega(K)$ из упражнения 17.1.3. Более общо, если σ — свойство групп, которое переносится на подгруппы, то говорят, что группа G *локально* обладает свойством σ, если все конечно порожденные подгруппы из G обладают свойством σ (определение для произвольного σ см. в следующей главе).

18.1.1. Упражнение. Подгруппы и факторгруппы локально нильпотентных групп сами локально нильпотентны. Всякая локально нильпотентная группа является локально полициклической.

18.1.2. Теорема. 1) *Во всякой группе произведение двух нормальных локально полициклических подгрупп есть локально полициклическая подгруппа.*

2) (Б. И. Плоткин) *Во всякой группе произведение двух нормальных локально нильпотентных подгрупп есть локально нильпотентная подгруппа.*

Доказательство. 1) Пусть K, L — нормальные локально полициклические подгруппы произвольной группы G. Надо показать, что любая конечно порожденная подгруппа из KL полициклическая. Возьмем в KL такую подгруппу и запишем ее порождающие в виде произведений ab, $a \in K$, $b \in L$. Пусть A — подгруппа, порожденная левыми множителями, B — правыми. По условию, группы A, B полициклические. Очевидно, достаточно убедиться, что их порождение $H = \text{гр}(A, B)$ — полициклическая группа. Воспользуемся леммой 3.2.2, описывающей строение H (отметим, что в нашем случае множества I, J, C конечны). Ввиду этой леммы и упражнения 4.4.3 достаточно проверить полицикличность группы A $[A, B]$.

Так как K, L нормальны в G, то $[K, L] \leqslant K \cap L$. Так как A, гр (C) конечно порождены и лежат в локально полициклической группе K, то гр (A, C) полициклическая. Значит, лежащая в ней подгруппа гр (C^A) также полициклическая. С другой стороны, она лежит в L, поэтому гр(гр(C^A), B) — конечно порожденная подгруппа из L и, значит, тоже полициклическая. По лемме 3.2.2 в ней содержится $[A, B]$, поэтому $[A, B]$ — полициклическая группа. Так как A и $[A, B]$ обе лежат в K и конечно порождены, то их произведение — полициклическая группа.

2) Доказывается по той же схеме.

Теперь снова, как и после теоремы Фиттинга, полезно обратиться к упражнению 16.2.13.

Не все свойства нильпотентных групп из § 16 имеют место для локально нильпотентных групп — так, в примере 18.2.2 следующего пункта мы увидим, что подгруппы локально нильпотентных групп не всегда субнормальны. Что же остается от теоремы 16.2.2 в случае локально нильпотентных групп? Справедлива, например, такая

18.1.3. Т е о р е м а (Маклейн). *Любая максимальная подгруппа H локально нильпотентной группы G нормальна.*

Д о к а з а т е л ь с т в о. Пусть, напротив, H не нормальна в G. Тогда существует $x \in [G, G]$, $x \notin H$. Ввиду максимальности H гр $(H, x) = G$. Пусть

$$x = [y_1, z_1] \ldots [y_n, z_n], \quad y_i, z_i \in G.$$

Пусть y_i, z_i выражаются как слова от x и $h_1, \ldots, h_m$ из H, и

$$H^* = \text{гр } (h_1, \ldots, h_m), \; G^* = \text{гр } (h_1, \ldots, h_m, x).$$

По условию группа G^* нильпотентна. Очевидно, $x \in [G^*, G^*]$, $x \notin H^*$, поэтому H^* — собственная подгруппа в G^*. По теореме 16.2.2 можно включить H^* в субнормальную матрёшку группы G^*, которая по теореме 17.2.2 уплотняется до полициклической матрёшки

$$1 < \ldots < H^* < H_1 < \ldots < H_s < G^*. \qquad (1)$$

Так как секция G^* / H_s коммутативна, то $[G^*, G^*] \leqslant H_s$ и, значит, $x \in H_s$. Но тогда $G^* \leqslant H_s$, что противоречит строгим включениям (1). Теорема доказана.

18.1.4. Упражнение. Во всякой локально нильпотентной группе G периодические элементы составляют подгруппу (называемую *периодической частью* группы G).

Указание: см. 16.2.7.

18.1.5. Упражнение. Всякая периодическая локально нильпотентная группа разлагается в прямое произведение силовских подгрупп.

Указание: учитывая 16.1.6 и 17.1.4, доказать единственность силовской p-подгруппы для каждого простого числа p.

18.2. Нормализаторное условие. Как показали Хайнекен и Мохамед (Heineken H., Mohamed I. J.— J. Algebra, 1968, **10**, p. 368—376), обратить теорему 16.2.2, вообще говоря, нельзя, т. е. существуют ненильпотентные группы, у которых все подгруппы субнормальны. Отметим, однако, что для всякого натурального числа n существуют такие натуральные числа $r(n)$ и $s(n)$, что всякая группа, у которой всякая подгруппа с $r(n)$ порождающими включается в субнормальный ряд длины $\leqslant n$, является нильпотентной группой ступени $\leqslant s(n)$ (Roseblade J. E.— J. Algebra, 1965, 2, № 4, p. 402—412).

Более слабым условием по сравнению с субнормальностью всех подгрупп является следующее *нормализаторное условие*: каждая собственная подгруппа отлична от своего нормализатора.

18.2.1. Теорема (Б. И. Плоткин). *Всякая группа G с нормализаторным условием локально нильпотентна.*

Доказательство. По лемме Цорна всякий элемент из G лежит в некоторой максимальной локально нильпотентной подгруппе H. Достаточно показать, что H нормальна в G (тогда G будет покрываться локально нильпотентными нормальными подгруппами, а потому по теореме 18.1.2 сама будет локально нильпотентной). Обозначим $N = N_G(H)$. Если $N^g = N$, то H^g, H нормальны в N. По теореме 18.1.2 их произведение H^gH локально нильпотентно. Ввиду максимальности H имеем $H^gH = H$, откуда $H^g = H$, $g \in N$. Таким образом, N совпадает со своим нормализатором. Ввиду нормализаторного условия $N = G$, что и требовалось доказать.

Обращение этой теоремы неверно, как показывает следующий пример, решающий и другие вопросы.

18.2.2. Пример (М. И. Каргаполов). Определим для каждого трансфинитного числа α группу G_α, полагая

$$G_0 = \mathbb{C}_p,\ G_\alpha = \begin{cases} \mathbb{C}_p \wr G_{\alpha-1} \text{ при непредельном } \alpha, \\ \bigcup\limits_{\beta<\alpha} G_\beta \text{ при предельном } \alpha. \end{cases}$$

Из построения видно, что каждое G_α является p-группой, причем все ее конечно порожденные подгруппы конечны и $|G_\alpha| \geqslant |\alpha|$. В частности, все группы G_α локально нильпотентны.

Пусть γ — первое несчетное трансфинитное число. Ясно, что все G_α при $\alpha < \gamma$ счетны, а группа G_γ несчетна. Покажем, что G_γ не удовлетворяет нормализаторному условию. Действительно, в противном случае в G_γ существовала бы последовательность подгрупп H_λ, занумерованных трансфинитными числами $\lambda \leqslant \nu$, с условиями:

а) $H_0 = 1$, $H_\mu \lhd H_{\mu+1}$, $H_\lambda = \bigcup\limits_{\mu<\lambda} H_\mu$ при предельном λ, $H_\nu = G_\gamma$,

б) все факторы $H_{\mu+1}/H_\mu$ коммутативны.

(Такую последовательность можно было бы построить, например, беря первую и третью формулы из а) за определение H_λ, а в качестве $H_{\mu+1}$ беря порождение H_μ и любого элемента из $N(H_\mu)$, лежащего вне H_μ.) Мы покажем сейчас, что группа G_γ в действительности не содержит подгрупп с условиями а), б).

Пусть, напротив, такие H_λ существуют. Уплотнив, если нужно, последовательность этих подгрупп, можно считать, что все факторы $H_{\mu+1}/H_\mu$ циклические. Тогда все H_n с натуральными номерами n счетны, а потому и их объединение H_ω счетно. Занумеруем элементы из H_ω: $h_1, h_2, \ldots$ Очевидно, $h_m \in G_{\beta_m}$ при некотором $\beta_m < \gamma$. Объединение всех G_{β_m} есть некоторое G_β, причем $\beta < \gamma$, поскольку G_β счетно, а группа G_γ несчетна. Мы получим противоречие, если установим, что G_β содержит все H_λ при $\omega < \lambda \leqslant \nu$. Сделаем это индукцией по λ. Для предельных λ утверждение очевидно, поэтому пусть λ — непредельное число. Пусть уже доказано, что $H_{\lambda-1} \leqslant G_\beta$, но существует $h \in H_\lambda$, $h \notin G_\beta$. Пусть α таково, что $h \in G_\alpha$, $h \notin G_{\alpha-1}$. Очевидно, $\beta \leqslant \alpha - 1$, поэтому $H_{\lambda-1} \leqslant G_{\alpha-1}$. По определению сплетения,

$$h = bf,\ b \in G_{\alpha-1},\ f \in \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p),$$

причем $f \neq 1$. Для всех $x \in H_{\lambda-1}$ имеем

$$[x^b, f] = x^{-b}x^{bf} \in G_{\alpha-1} \cap \operatorname{fun}(G_{\alpha-1}, \mathbb{C}_p) = 1,$$

т. е. $H^b_{\lambda-1}$ централизует f. Таким образом, элемент $f' = bfb^{-1} \neq 1$ имеет в $G_{\alpha-1}$ бесконечный централизатор. С другой стороны, этот централизатор, действуя на $G_{\alpha-1}$ правыми сдвигами, должен переводить $\operatorname{supp}(f')$ в себя. Значит, он изоморфен группе подстановок конечного множества $\operatorname{supp}(f')$ и потому не может быть бесконечным.

18.2.3. У п р а ж н е н и е. Группа G_γ имеет тривиальный центр.

Группы с нормализаторным условием столь близки к группам с центральными матрёшками (вообще говоря, бесконечными), что долго никто не знал, существуют ли группы с нормализаторным условием и без центра. Этот старый вопрос был положительно решен Хайнекеном и Мохамедом (см. статью, цитированную в начале пункта).

Однако по-прежнему неизвестно ([13], вопрос 2.80), имеет ли произвольная группа с нормализаторным условием отличную от единицы абелеву нормальную подгруппу.

18.3. Энгелевость. Источником этого обобщения нильпотентности служит коммутаторное тождество

$$[x_0, x_1, \ldots, x_n] = 1, \tag{2}$$

определяющее, как мы знаем, нильпотентные группы ступени $\leqslant n$. Стремление иметь возможно меньше переменных приводит нас к тождеству

$$[x, \underbrace{y, \ldots, y}_{n}] = 1 \tag{3}$$

(отсутствие внутренних скобок означает, конечно, «правильную» их расстановку: $[[[x, y], y], \ldots, y]$). Группа с тождеством (3) называется *ограниченно энгелевой группой* ступени $\leqslant n$ — в честь Энгеля, заложившего вместе с Ли основы теории групп и алгебр Ли, упоминавшейся в начале главы. Очевидно, в многообразии ограниченно энгелевых групп ступени $\leqslant n$ содержится многообразие всех нильпотентных групп ступени $\leqslant n$. Эти многообразия не совпадают, как показывает

18.3.1. Пример (Уэстон). Пусть M — множество натуральных чисел, разлагающихся в произведение различных простых чисел, т. е. не делящихся на квадраты. Каждому $m \in M$ сопоставим циклическую группу второго порядка с порождающим a_m и обозначим через A прямое произведение всех (a_m). Каждому простому числу p сопоставим автоморфизм φ_p группы A, задаваемый на порождающих следующим образом:

$$a_m^{\varphi_p} = \begin{cases} a_m a_{m/p} & \text{при } p \mid m, \\ a_m & \text{в остальных случаях.} \end{cases}$$

Очевидно, $\varphi_p^2 = 1$ и $\varphi_p \varphi_q = \varphi_q \varphi_p$, так что группа Φ, порожденная всеми φ_p, коммутативна периода 2. Пусть G — расширение A посредством Φ (см. п. 6.1). Из определения видно, что при q, не делящем m,

$$a_m = [a_{mq}, \varphi_q].$$

Отсюда $[G, G] = A$, $[G, A] = A$ и, значит, группа G не нильпотентна. С другой стороны, она удовлетворяет тождеству $[x, y, y, y] = 1$. Действительно, если $a, a' \in A$, $\varphi, \varphi' \in \Phi$, то имеем последовательно: $[a, a'\varphi] = [a, \varphi]$ ввиду тождества $[x, yz] = [x, z]\,[x, y]^z$ и коммутативности группы A, $[a, \varphi, \varphi] = 1$ ввиду тождества $[x, y, z] = [y, x]\,[z, x]\,[x, yz]$ и соотношения $[a, \varphi]^2 = 1$, наконец, $[a\varphi, a'\varphi', a'\varphi', a'\varphi'] = [a\varphi, a'\varphi', \varphi', \varphi'] = 1$ в силу предыдущего. Отметим еще тот очевидный факт, что группа Уэстона имеет период 4.

Группа называется *энгелевой*, если для любых ее элементов x, y выполняется соотношение (3) при некотором n, зависящем, вообще говоря, от этих элементов. Очевидно, класс энгелевых групп содержит класс всех локально нильпотентных групп. Эти классы различны, как показывает такой

18.3.2. Пример (Е. С. Голод). Для любого $d \geqslant 2$ существует ненильпотентная группа G с d порождающими, у которой любая подгруппа с $d - 1$ порождающими нильпотентна. Такая группа строится с помощью аналогичного примера для алгебр, а именно с помощью ненильпотентной (бесконечномерной) алгебры A с d порождающими, у которой любая подалгебра с $d - 1$ порождающими нильпотентна. Указанная конструкция, детально изложенная

в § 26 Дополнения, дает A в виде F'/I, где F' — подалгебра «многочленов без свободного члена» свободной ассоциативной алгебры F с порождающими $x_1, \ldots, x_d$ над каким-нибудь полем k, I — однородный идеал в F'. Пусть p — простое число, $k = GF(p)$. Возьмем в F/I множество

$$1 + A = \{1 + a \mid a \in A\}.$$

Очевидно, $(1 + a)(1 + b) = 1 + a + b + ab$, $(1 + a)^{-1} = 1 - a + a^2 - \ldots + (-1)^{n-1}a^{n-1}$, если $a^n = 0$, поэтому $1 + A$ — группа. Далее, для всякого $a \in A$ существует такое m, что $a^{p^m} = 0$, откуда

$$(1 + a)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} a^i = 1,$$

поскольку все биномиальные коэффициенты, кроме первого и последнего, делятся на p. Значит, $1 + A$ является p-группой. Пусть G — подгруппа, порожденная в ней элементами $1 + \bar{x}_1, \ldots, 1 + \bar{x}_d$, где $\bar{x}_i = x_i + I$. Ясно, что подгруппа, порожденная элементами $1 + a_1, \ldots, 1 + a_{d-1}$, $a_i \in A$, лежит в $1 + A^*$, где A^* — подалгебра, порожденная элементами $a_1, \ldots, a_{d-1}$. По условию алгебра A^* нильпотентна, поэтому и группа $1 + A^*$ нильпотентна (упражение 16.1.4). Таким образом, все подгруппы с $d - 1$ порождающими из G нильпотентны. Однако сама группа G ненильпотентна. В самом деле, в противном случае ввиду 16.1.6 она была бы конечной. Но тогда и групповое кольцо $k[G]$ и его естественный гомоморфный образ $F/I = k \oplus A$ были бы конечными, что противоречит бесконечности алгебры A.

Пока неизвестно, будет ли группа локально нильпотентной, если для любых ее элементов x, y выполняется соотношение (3) при n, зависящем только от y. Неизвестно также, будет ли в произвольной группе произведение нормальных энгелевых подгрупп снова энгелевой подгруппой.

Глава 7

РАЗРЕШИМЫЕ ГРУППЫ

§ 19. Общие свойства и примеры

19.1. Определения. Как было сказано в начале предыдущей главы, разрешимые группы — это группы, которые можно собрать последовательными расширениями из абелевых групп. Возможны и другие равносильные определения разрешимости.

19.1.1. Теорема. *Для произвольной группы G равносильны следующие утверждения:*

а) *группа G обладает субнормальной матрёшкой с абелевыми секциями,*

б) *группа G обладает нормальной матрёшкой с абелевыми секциями,*

в) *ряд коммутантов $G \geqslant G' \geqslant \ldots \geqslant G^{(n)} \geqslant \ldots$ группы G через конечное число шагов обрывается на единице, т. е. является (конечной) матрёшкой,*

г) *группа G удовлетворяет одному из тождеств*

$$\delta_n(x_1, \ldots, x_{2^n}) = 1, \quad n = 0, 1, 2, \ldots,$$

где $\delta_0(x) = x$, $\delta_{n+1}(x_1, \ldots, x_{2^{n+1}}) = [\delta_n(x_1, \ldots, x_{2^n}), \delta_n(x_{2^n+1} \ldots, x_{2^{n+1}})]$.

Доказательство. в) $\Rightarrow$ б) $\Rightarrow$ а). Очевидно.

а) $\Rightarrow$ в). Пусть группа G обладает субнормальной матрёшкой с абелевыми секциями:

$$1 = H_0 < H_1 < \ldots < H_s = G.$$

Так как фактор-группа G/H_{s-1} абелева, то $G' \leqslant H_{s-1}$. Предположим, что уже установлено включение $G^{(k)} \leqslant H_{s-k}$, $1 \leqslant k < s$. Ввиду коммутативности секции H_{s-k}/H_{s-k-1} коммутант $(G^{(k)})' = G^{(k+1)}$ содержится в H_{s-k-1}. Отсюда $G^{(s)} = 1$. Следовательно, доказана равносильность первых трех утверждений.

в) $\Rightarrow$ г). Допустим, что s-й коммутант $G^{(s)}$ группы G равен единице. Так как $(s-1)$-й коммутант группы $G/G^{(s-1)}$ равен единице, то, используя индуктивные сооб-

ражения, можно считать, что $\delta_{s-1}(g_1, \ldots, g_{2^{s-1}}) \in G^{(s)}$, где $\delta_{s-1}(g_1, \ldots, g_{2^{s-1}})$ — значение слова δ_{s-1} на элементах g_i. Отсюда в силу коммутативности группы $G^{(s)}$ получаем $\delta_s(g_1, \ldots, g_{2^s}) = 1$ для любых $g_i \in G$.

г) $\Rightarrow$ в). Обратно, пусть на группе G справедливо тождество $\delta_s = 1$. Очевидно, подгруппа H, порожденная значениями слова δ_{s-1}, нормальна и коммутативна. На фактор-группе G/H выполняется тождество $\delta_{s-1} = 1$ и поэтому можно считать $G^{(s-1)} \leqslant H$, что влечет $G^{(s)} = 1$. Теорема доказана.

Группа G называется *разрешимой*, если для нее верно одно из утверждений а), б), в), г). Матрёшки пунктов а), б) также называют *разрешимыми*. Если группа G разрешима, то наименьшее положительное число n, для которого $G^{(n)} = 1$, называется *ступенью разрешимости* этой группы.

Из доказательства теоремы 19.1.1 видно, что на разрешимых группах ступени разрешимости $\leqslant n$ и только на них выполняется тождество $\delta_n = 1$. Следовательно, класс разрешимых групп ступени разрешимости $\leqslant n$ есть многообразие. Непосредственным следствием этого замечания является замкнутость класса разрешимых групп относительно взятия подгрупп, гомоморфных образов и конечных прямых произведений, а также декартовых произведений при условии ограниченности ступеней разрешимости сомножителей. Прямое (декартово) произведение произвольных разрешимых групп может не быть разрешимой группой.

19.1.2. Упражнение. Треугольные матричные группы $T_n(K)$ разрешимы. Их прямое произведение по $n = 1, 2, \ldots$ не является разрешимой группой.

19.1.3. Упражнение. Расширение разрешимой группы посредством разрешимой группы само разрешимо.

19.1.4. Упражнение. В произвольной группе произведение двух разрешимых нормальных подгрупп является разрешимой подгруппой.

19.1.5. Упражнение. В произвольной конечной группе существует (единственная) разрешимая нормальная подгруппа, фактор-группа по которой не содержит отличных от единицы абелевых нормальных подгрупп.

19.1.6. Упражнение. Конечная разрешимая группа обладает субнормальной матрёшкой с циклическими секциями простых порядков.

19.1.7. Упражнение. Минимальная нормальная подгруппа конечной разрешимой группы является элементарной абелевой, т. е. разлагается в прямое произведение циклических групп одного и того же простого порядка.

19.1.8. Упражнение. Периодические конечно порожденные разрешимые группы конечны (ср. с 16.1.6).

19.1.9. Упражнение. Пусть p — простое число, T_p — группа матриц вида

$$\begin{pmatrix} 1 & * & * & * \\ & * & * & * \\ & & * & * \\ & & & 1 \end{pmatrix}$$

над кольцом $\mathbb{Q}_p$ p-ичных дробей с положительными диагональными элементами. Доказать, что 1) центр $Z(T_p)$ группы T_p состоит из матриц с единственной звёздочкой в правом верхнем углу и, следовательно, изоморфен аддитивной группе $\mathbb{Q}_p$; 2) группа T_p порождается диагональными матрицами

$$d_2 = \mathrm{diag}\,(1,\ p,\ 1,\ 1),\quad d_3 = \mathrm{diag}\,(1,\ 1,\ p,\ 1)$$

и трансвекциями $t_{ij} = e + e_{ij}$, $i < j$. Как показал Абельс (Abels H.— London Math. Soc. Lecture Note Ser., 1979, 36, p. 205—211), T_p имеет в этих порождающих конечный генетический код

$$[d_2,\ d_3] = 1,\quad [t_{ij},\ t_{kl}] = t_{il}^{\delta(j,\ k)},$$
$$t_{i,\ i+1}^{p^{\delta(i,\ j)}} d_j = d_j t_{i,\ i+1}^{p^{\delta(i+1,\ j)}},$$

где $\delta\,(i, j)$ обозначает единицу при $i = j$ и нуль при $i \neq j$. Таким образом, группы T_p доставляют пример конечно определенных разрешимых групп, у которых центр не конечно порожден и существуют бесконечные возрастающие ряды $N_1 < N_2 < \ldots$ нормальных (даже центральных) подгрупп.

Другой важный пример, вскрывающий уже не структурную, а алгоритмическую сложность конечно определенных разрешимых групп, указала недавно О. Г. Харлампович (Изв. АН СССР: Сер. матем., 1981, 45, № 4, с. 852—873) — она построила 3-ступенно разрешимую

группу с конечным генетическим кодом

$$G = \text{гр}\,(x_1, \ldots, x_n \parallel v_1 = 1, \ldots, v_m = 1)$$

и неразрешимой проблемой равенства. Последнее означает, что для группы G не существует алгоритма, который по любым двух словам в алфавите $x_1, \ldots, x_n$ распознавал бы их равенство или неравенство как элементов группы G.

19.2. Полицикличность и сверхразрешимость. Очевидный пример разрешимых групп — полициклические группы. Важный подкласс полициклических групп составляют *сверхразрешимые группы* — это группы, обладающие нормальной (а не просто субнормальной) матрёшкой с циклическими секциями. Знакомый нам пример сверхразрешимых групп дают конечно порожденные нильпотентные группы.

19.2.1. Упражнение. Подгруппы и факторгруппы сверхразрешимых групп сверхразрешимы.

19.2.2. Теорема. *Коммутант сверхразрешимой группы нильпотентен.*

Доказательство. Пусть в группе G задана нормальная полициклическая матрёшка $1 = G_0 \leqslant G_1 \leqslant \ldots \ldots \leqslant G_n = G$, и пусть G' — коммутант группы G. По теореме 4.4.2 ряд

$$1 = H_0 \leqslant H_1 \leqslant \ldots \leqslant H_n = G', \text{ где } H_i = G_i \cap G',$$

является нормальной полициклической матрёшкой в G'. Покажем, что на самом деле она центральна в G', т. е. $[G', H_{i+1}] \leqslant H_i$ для всех $i = 0, 1, 2, \ldots, n-1$. Очевидно, сопряжения группы G элементами из G индуцируют автоморфизмы в секциях H_{i+1}/H_i. Так как группа автоморфизмов циклической группы абелева (см. 5.1.1), то коммутант G' должен индуцировать во всех секциях H_{i+1}/H_i тождественное преобразование. Но это и означает нужные нам включения. Теорема доказана.

Отметим одно свойство конечных сверхразрешимых групп.

Пусть G — конечная группа порядка $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где p_i — простые числа, $p_1 > \ldots > p_k$. Нормальная матрёшка

$$1 = H_0 < H_1 < \ldots < H_k = G$$

называется *силовской матрёшкой* группы G, если секция

H_{i+1}/H_i, $i = 0, 1, \ldots, k-1$, является силовской p_{i+1}-подгруппой группы G/H_i. (Иногда в этом определении не требуют упорядоченности $p_1 > \ldots > p_k$.)

19.2.3. Т е о р е м а. *Конечная сверхразрешимая группа обладает силовской матрёшкой.*

Д о к а з а т е л ь с т в о. Пусть p — наибольший простой делитель порядка сверхразрешимой группы G, и пусть H — какая-нибудь ее нормальная подгруппа простого порядка q. Фактор-группа G/H сверхразрешима и $|G/H| < |G|$. По индуктивным соображениям можно считать, что в фактор-группе G/H силовская p-подгруппа P/H нормальна. При $p = q$ подгруппа P будет силовской p-подгруппой в G и $P \trianglelefteqslant G$. Если $p \neq q$, то в G/H найдется нормальная подгруппа H_1/H порядка p. По теореме Силова, как легко видеть, силовская p-подгруппа H_2 группы H_1 единственна и потому ввиду соотношения $H_1 \trianglelefteqslant G$ нормальна в G. Снова применяя к G/H_2 индуктивные соображения, получаем нормальность силовской p-подгруппы группы G. На этом по существу доказательство заканчивается.

§ 20. Конечные разрешимые группы

Заметим, прежде всего, что конечные разрешимые группы — это в точности конечные полициклические группы.

В первом пункте этого параграфа излагается теория холловых и картеровых подгрупп в конечной разрешимой группе, которая напоминает теорию силовских p-подгрупп в произвольной конечной группе. В третьем пункте будет указан один критерий сверхразрешимости конечной группы. Второй пункт носит подготовительный характер, однако излагаемые в нем теоремы Машке и Шура о произвольных конечных группах очень важны сами по себе.

20.1. Холловы и картеровы подгруппы. По теореме Силова 11.1.1 в произвольной конечной группе порядка $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ (p_i — различные простые числа) всегда существует подгруппа порядка $p_i^{\alpha_i}$ и любые две такие подгруппы сопряжены между собой. Ф. Холл нашел обобщение теоремы Силова для конечных разрешимых групп, а именно доказал существование и сопряженность

подгрупп порядка k в конечной разрешимой группе порядка n для всякого k с условием $k \mid n, \left(k, \frac{n}{k}\right) = 1$. Такие делители числа n называют *холловыми*, а всякую подгруппу, порядок которой равен некоторому холлову делителю порядка группы, называют *холловой подгруппой*. Отметим без доказательства, что из существования холловых подгрупп конечной группы G по всевозможным холловым делителям порядка группы G вытекает разрешимость G. Этот факт установлен Ф. Холлом (Hall P.— J. London Math. Soc., 1937, 12, p. 198—200) и С. А. Чунихиным (Изв. НИИММ Томского ун-та, 1938, 2, с. 220—223).

20.1.1. Теорема (Ф. Холл). *Пусть G — конечная разрешимая группа порядка n и k — холлов делитель числа n. Тогда*

1) *в группе G существует по крайней мере одна подгруппа порядка k;*

2) *любые две подгруппы порядка k сопряжены в G;*

3) *любая подгруппа порядка $k' \mid k$ содержится в подгруппе порядка k.*

Доказательство будем вести индукцией по n. Допустим, что все утверждения теоремы справедливы для произвольной конечной разрешимой группы, порядок которой меньше n. Обозначим через A минимальную нормальную подгруппу группы G. Согласно упражнению 19.1.7 подгруппа A разлагается в прямое произведение циклических подгрупп простого порядка p, $|A| = p^m$.

Если $p \mid k$, то ввиду индуктивного допущения в факторгруппе G/A существует подгруппа B/A порядка k/p^m. Тогда порядок B равен k. Кроме того, любые подгруппы B_1, B_2 порядка k содержат, очевидно, подгруппу A. По индукции подгруппы B_1/A и B_2/A сопряжены в G/A. Следовательно, подгруппы B_1, B_2 сопряжены в G.

Пусть теперь p не делит k. Обозначим через D наибольшую нормальную подгруппу группы G, порядок которой взаимно прост с k, а через H/D — минимальную нормальную подгруппу группы G/D. Порядок H/D имеет вид q^s, $q^s \mid k$.

Если нормализатор $N(Q)$ силовской q-подгруппы Q из H совпадает с G, то $Q \trianglelefteq G$ и доказательство пп. 1), 2) проводится так же, как при первоначальном допущении $p \mid k$.

Пусть $N(Q) \neq G$. Из равенства $G = N(Q)H = N(Q)D$ (см. лемму Фраттини 17.1.8) следует, что порядок $N(Q)$ делится на k. Отсюда ввиду индуктивных предположений вытекает существование в $N(Q)$, а значит, и в группе G, подгруппы порядка k.

Возьмем две подгруппы B_1, B_2 порядка k. Пересечения $B_1 \cap H$, $B_2 \cap H$ являются в H силовскими q-подгруппами, поэтому, ввиду их сопряженности, можно считать, что $B_1 \cap H = B_2 \cap H = Q$. Подгруппа Q, очевидно, нормальна в подгруппе (B_1, B_2). На основании индукции подгруппы B_1/Q и B_2/Q сопряжены в $(B_1, B_2)/Q$. Отсюда следует сопряженность подгрупп B_1, B_2.

Итак, утверждения 1), 2) доказаны. Докажем 3).

Пусть B' — подгруппа порядка k'. При $p \mid k$ порядок подгруппы AB', очевидно, делит k. В силу индуктивного допущения подгруппа AB'/A содержится в некоторой подгруппе порядка k/p^m. Тогда AB' содержится в подгруппе порядка k. Пусть теперь p не делит k. На основании индуктивных предположений подгруппа AB'/A содержится в подгруппе C/A порядка k. На том же основании можно считать, что $C = G$. По доказанному п. 1) в G существует подгруппа B порядка k. Очевидно, произведение AB совпадает с G и потому $AB'B = G$. Из формул

$$|G| = \frac{|AB'| \cdot |B|}{|AB' \cap B|}, \quad |G| = p^m k, \quad |AB'| = p^m k', \quad |B| = k$$

получаем, что порядок $D = AB' \cap B$ равен k'. По доказанному п. 2) подгруппы B' и D сопряжены в $AB' : B' = D^g$. Отсюда следует, что B' содержится в подгруппе B^g порядка k. Теорема доказана.

20.1.2. Упражнение. Индекс произвольной максимальной подгруппы конечной разрешимой группы G есть степень простого числа. Для всякого простого делителя p порядка группы G существует максимальная в G подгруппа, индекс которой есть степень p.

20.1.3. Упражнение. Пусть A — холлова подгруппа конечной разрешимой группы G, H — подгруппа, содержащая нормализатор $N_G(A)$. Тогда $N_G(H) = H$.

Ф. Холл ввел понятие силовской базы и обобщил свою теорему в этих терминах, что послужило толчком к дальнейшим ее обобщениям в различных направлениях.

Совокупность G_{p_1}, G_{p_2}, . . . силовских p_i-подгрупп группы G называется (*полной*) *силовской базой*, если

1) $G = \text{гр}\,(G_{p_1}, G_{p_2}, \ldots)$,

2) $G_{p_i}G_{p_j} = G_{p_j}G_{p_i}$ для всех i, j.

Иногда в определении силовской базы вместо 2) требуют выполнение условия

2′) Множество простых делителей порядков элементов подгруппы гр $(G_{p_{i_1}}, \ldots, G_{p_{i_s}})$ совпадает с $\{p_{i_1}, \ldots, p_{i_s}\}$ для всех $i_1, \ldots, i_s$.

Обычно эти определения оказываются равносильными.

Две силовские базы $\{G_{p_i}\}$, $\{G'_{p_i}\}$ называются *сопряженными*, если существует такой элемент g, что $G'_{p_i} = G^g_{p_i}$ для всех i.

Обобщение, полученное Холлом, состоит в следующем (Hall P. — Proc. London Math. Soc., 1937, **43**, p. 316—323). Произвольная конечная разрешимая группа G обладает силовскими базами и любые две базы сопряжены в ней. Любая силовская база подгруппы продолжается до силовской базы группы G.

Понятие силовской базы имеет смысл для произвольных периодических групп, поэтому естественно пытаться распространить теорему о существовании силовских баз на периодические разрешимые группы. Такие распространения получены для ряда классов бесконечных групп, однако произвольная периодическая разрешимая группа не обязана обладать силовскими базами (Каргаполов М. И.— ДАН СССР, 1959, **127**, № 6, с. 1164—1166; Алгебра и логика, 1963, **2**, № 5, с. 19—28).

Подгруппа H группы G называется *картеровой*, если H нильпотентна и совпадает со своим нормализатором в G.

20.1.4. Теорема (Картер). *Конечная разрешимая группа G обладает по крайней мере одной картеровой подгруппой и любые две картеровы подгруппы группы G сопряжены между собой.*

Доказательство будем вести индукцией по порядку группы G.

Пусть A — минимальная нормальная подгруппа группы G и $|A| = p^m$. В силу индуктивного предположения фактор-группа G/A обладает картеровой подгруппой, скажем, K'/A. Пусть Q — холлова p'-подгруппа группы

K', т. е. p не делит $|Q|$ и $|K'| = |Q|p^l$. Покажем, что $K = N_{K'}(Q)$ будет картеровой подгруппой в G.

Действительно, по обобщенной лемме Фраттини 17.1.9 имеем $K' = N_{K'}(Q) \cdot QA = KA$. Подгруппа K разлагается в прямое произведение нильпотентных подгрупп Q и $K \cap P$, где P — силовская p-подгруппа группы K'. Поэтому подгруппа K нильпотентна. Далее, пусть $K^g = K$. Так как $A \trianglelefteqslant G$ и $K' = KA$, то $K'^g = K'$ и, следовательно, $g \in K'$. Нормализатор холловой подгруппы совпадает со своим нормализатором (см. 20.1.3), поэтому элемент g содержится в K, что и требовалось доказать.

Пусть теперь K_1, K_2 — картеровы подгруппы группы G. Докажем их сопряженность в G.

Сначала докажем, что K_iA/A, $i = 1, 2$, является, картеровой подгруппой группы G/A. Нильпотентность подгруппы K_iA/A очевидна. Если $(K_iA)^g = K_iA$, $g \notin K_iA$, то $|K_iA| < |G|$ и, значит, в силу индуктивного предположения, примененного к картеровым подгруппам из K_iA, существует такой элемент $a \in K_iA$, что $K_i^g = K_i^a$ или $K_i^{ga^{-1}} = K_i$. Но подгруппа K_i совпадает со своим нормализатором, поэтому $ga^{-1} \in K_i$, что противоречит допущению $g \notin K_iA$.

Легко понять, что холлова p'-подгруппа Q_i из K_i является холловой p'-подгруппой группы K_iA. Кроме того, нормализатор $N(Q_i)$ подгруппы Q_i в K_iA нильпотентен и содержит K_i. Следовательно, K_i совпадает с $N(Q_i)$. По индуктивному допущению картеровы подгруппы K_1A/A, K_2A/A сопряжены между собой. Поэтому можно считать, что $K_1A = K_2A$. Как было отмечено, подгруппа K_i совпадает с нормализатором $N(Q_i)$ в K_1A. Но холловы p'-подгруппы Q_1, Q_2 групп K_1, K_2, являющиеся холловыми p'-подгруппами группы K_1A, сопряжены между собой. Поэтому должны быть сопряженными и их нормализаторы, т. е. K_1 и K_2. Теорема доказана.

20.2. О полной приводимости представлений. Здесь мы сделаем отступление в теорию матричных представлений. Основная цель этого пункта — изложить классическую теорему Машке о полной приводимости представлений конечных групп. Она понадобится нам в следующем пункте. Попутно будут изложены и другие сведения о полной приводимости.

Пусть V — линейное пространство над полем K, G — группа линейных преобразований пространства V. Если в V существует собственное подпространство, допустимое относительно G, то группу G называют *приводимой*. В противном случае группу G называют *неприводимой* или *неприводимо действующей* на пространстве V. Группа G называется *вполне приводимой*, если для всякого допустимого подпространства $U \leqslant V$ существует допустимое дополнение, т. е. такое допустимое подпространство W, что $V = U \oplus W$.

Произвольный гомоморфизм φ абстрактной группы G в группу линейных преобразований n-мерного векторного пространства над полем K называется *линейным представлением* группы G. Если группа линейных преобразований G^φ неприводима (приводима, вполне приводима), представление φ также называется *неприводимым* (соответственно *приводимым* или *вполне приводимым*). Произвольный гомоморфизм ψ группы G в группу матриц $\boldsymbol{GL}_n(K)$ называется *матричным представлением*. Представления φ и ψ тесно связаны между собой. Так, линейному представлению φ при фиксированной базе Σ пространства V сопоставляется матричное представление φ_Σ, где g^{φ_Σ} — матрица линейного преобразования g^φ в базе Σ. При выборе другой базы Σ' получается новое матричное представление $\varphi_{\Sigma'}$, эквивалентное φ_Σ, т. е. связанное с φ_Σ соотношением $g^{\varphi_{\Sigma'}} = tg^{\varphi_\Sigma}t^{-1}$, где t — матрица перехода от Σ к Σ', $g \in G$.

20.2.1. Пример. Пусть G — конечная группа, A — ее нормальная подгруппа, разлагающаяся в прямое произведение n циклических групп порядка p. На множестве A введем сложение и умножение на элементы поля $\boldsymbol{GF}(p)$ из p элементов, полагая по определению $a + b = ab$, $\alpha a = a^\alpha$, где показатель $\alpha \in \boldsymbol{GF}(p)$ естественным образом отождествляется с некоторым целым числом. Нетрудно видеть, что при введенных операциях A становится линейным пространством над полем $\boldsymbol{GF}(p)$. Далее, преобразование $\hat{g}: x \mapsto x^g$, $g \in G$, $x \in A$, будет линейным преобразованием пространства A, а отображение $\widehat{\ }$ гомоморфизмом G в группу линейных преобразований A. Таким образом, получено линейное представление группы G, причем, очевидно, $\hat{G} \simeq G/C_G(A)$.

20.2.2. Теорема (Машке). *Пусть* φ *— представление конечной группы* G *линейными преобразованиями линейного пространства* V *над полем* K. *Если порядок* G *не делится на характеристику поля* K, *то представление* φ *вполне приводимо.*

Доказательство. Будем считать, что G действует на V в силу представления φ. Пусть U — допустимое относительно G подпространство из V. Обозначим через W какое-нибудь дополнение подпространства U, $V = U \oplus W$. Далее, обозначим через π_W проектирование V на подпространство W и положим

$$vt = \frac{1}{m} \sum_{g \in G} vg^{-1}\pi_W g, \quad v \in V,$$

где m — порядок группы G. Отображение t является линейным преобразованием пространства V. При фиксированном $h \in G$ элемент gh вместе с g пробегает все элементы группы G. Поэтому справедливы равенства

$$(vt)h = \frac{1}{m} \sum_{g} vh \cdot h^{-1}g^{-1}\pi_W gh = (vh)t,$$

из которых следует допустимость линейного подпространства $W_0 = Vt$ относительно G.

Остается установить разложение $V = U \oplus W_0$. Произвольный элемент $v \in V$ представим в виде суммы $v = (v - vt) + vt$, $vt \in W_0$. Первое слагаемое $v - vt$ равно

$$v - \frac{1}{m} \sum_{g} vg^{-1}\pi_W g = \frac{1}{m} \sum_{g} (vg^{-1} - vg^{-1}\pi_W)\, g.$$

Так как $vg^{-1} - vg^{-1}\pi_W \in U$ и U допустимо, то $v - vt$ принадлежит U. Отсюда следует равенство $V = U + W_0$. Предположим, наконец, что $v \in U \cap W_0$. Так как $v \in U$, U допустимо относительно G и для любого элемента $u \in U$ проекция $u\pi_W$ равна 0, то

$$vt = 0. \tag{1}$$

С другой стороны, элемент v принадлежит W_0, поэтому существует такой элемент $v' \in V$, что

$$v't = v. \tag{2}$$

Но тогда $vt = v't^2$. Как было отмечено выше, $v' - v't \in U$ и, значит, $v't - v't^2 = 0$. Отсюда $vt = v't$, что вместе с равенствами (1), (2) влечет $v = 0$. Теорема доказана.

20.2.3. Пример. Пусть G, A имеют тот же смысл, что и в примере 20.2.1. Очевидно, подгруппа $B \leqslant A$ нормальна в группе G тогда и только тогда, когда линейное подпространство B пространства A допустимо относительно группы линейных преобразований $\hat{G}$. Предположим, что p не делит порядок группы $G/C_G(A)$ и B — некоторая нормальная подгруппа группы G, содержащаяся в A. Так как порядок группы преобразований $\hat{G}$ не делится на p, то по теореме Машке группа $\hat{G}$ вполне приводима и, значит, подпространство B обладает допустимым дополнением C. Множество C будет нормальной подгруппой группы G и $A = B \times C$.

20.2.4. Упражнение (обобщение теоремы Машке). Пусть G — конечная группа линейных преобразований линейного пространства V над полем характеристики $p > 0$, P — силовская p-подгруппа группы G. Если G-допустимое подпространство U обладает P-допустимым дополнением, то U обладает также G-допустимым дополнением.

Решение. Пусть $V = U \oplus W$, где W есть P-допустимое подпространство. Обозначим через π_W проектирование V на подпространство W и положим

$$vt = \frac{1}{m} \sum_{g \in S} vg^{-1}\pi_W g, \quad v \in V,$$

где $m = |G : P|$ и S — некоторое множество элементов, выбранных по одному в каждом правом смежном классе группы G по подгруппе P. Очевидно, проектирование π_W перестановочно с каждым элементом подгруппы P. Поэтому линейное преобразование t не зависит от выбора множества S. Доказательство G-допустимости подпространства $W_0 = Vt$ и справедливости разложения $V = U \oplus W_0$ дословно повторяет соответствующие рассуждения из доказательства теоремы Машке.

20.2.5. Упражнение. Пусть $A = B \times C$ — абелева нормальная подгруппа группы G и $(|A|, |G : A|) = 1$. Если B нормальна в G, то существует такая нормальная в G подгруппа D, что $A = B \times D$.

Теорему Машке удобно использовать для доказательства следующего важного предложения:

20.2.6. Т е о р е м а (Шур). *Пусть конечная группа G порядка n содержит такую нормальную подгруппу A порядка k, что $(k, l) = 1$, $l = n/k$. Тогда A обладает по крайней мере одним дополнением, т. е. подгруппой B с условиями $G = A \cdot B$, $A \cap B = 1$.*

Д о к а з а т е л ь с т в о. а) Пусть сначала A абелева и имеет простой период p. По теореме Фробениуса 6.2.8 можно считать G подгруппой сплетения $W = A \wr B$, $B = G/A$, причем

$$W = G \cdot \bar{A}, \quad G \cap \bar{A} = A, \text{ где } \bar{A} = \mathrm{Fun}(B, A)$$

(см. упражнение 6.2.9). Так как $|G : A|$ не делится на p и $A \lhd W$, то ввиду теоремы Машке 20.2.2 существует такая нормальная в W подгруппа C, что $\bar{A} = A \times C$. Из соотношений $W/C = \bar{A}/C \cdot BC/C$, $\bar{A} \cap BC = C$ и естественного изоморфизма φ: $W/C \to G$ следует, что $G = AD$, где D — образ подгруппы BC/C относительно φ.

б) Теперь докажем теорему в общих предположениях. Доказательство будем вести индукцией по порядку группы. Допустим, что теорема неверна для выбранной группы G, но справедлива для всякой группы меньшего порядка. Отметим, что существование дополнения к подгруппе A равносильно существованию в G подгруппы порядка l, так как $(k, l) = 1$.

Пусть P — силовская p-подгруппа из A и $N(P)$ — ее нормализатор в G. Так как $G = A \cdot N(P)$, то $N(P)$ обладает нормальной подгруппой $A \cap N(P)$, порядок которой взаимно прост с индексом $l = |N(P) : A \cap N(P)|$. Поэтому, если $|N(P)| < n$, то по индуктивному предположению подгруппа $N(P)$, а следовательно и группа G, обладает подгруппой порядка l, что противоречит выбору G. Значит, всякая силовская p-подгруппа из A нормальна в G, и поэтому коммутант $A' < A$. Пусть $A' \neq 1$. Тогда группа G/A' удовлетворяет условиям теоремы и $|G : A'| < n$. Следовательно, в G/A' существует подгруппа C/A' порядка l. Применяя индуктивное предположение к группе C, приходим к существованию в ней подгруппы порядка l. Из полученного противоречия с выбором G вытекает коммутативность A. Если, далее, $p \mid k$, $A^p \neq 1$, то, беря A^p в роли A', получаем аналогич-

ное противоречие. Значит, A абелева периода p. Ввиду а) теорема доказана.

Существенным дополнением к теореме Шура является утверждение о сопряженности в G любых двух подгрупп порядка l. Это утверждение было доказано Цассенхаузом при условии разрешимости подгруппы A, а С. А. Чунихиным — при условии разрешимости фактор-группы G/A. Но на основании теоремы Файта — Томпсона о разрешимости конечных групп нечетного порядка (см. о ней в начале § 13) по крайней мере одна из групп A, G/A разрешима, поэтому сопряженность дополнений в теореме Шура имеет место всегда.

Приведем в заключение пункта несколько общих замечаний о полной приводимости и неприводимости.

20.2.7. Л е м м а. *Группа G линейных преобразований линейного пространства V над полем K вполне приводима тогда и только тогда, когда V разлагается в прямую сумму допустимых неприводимых подпространств.*

Д о к а з а т е л ь с т в о. Пусть G вполне приводима. Обозначим через U_1 какое-нибудь допустимое неприводимое подпространство и предположим, что построены такие допустимые неприводимые подпространства $U_1, \ldots, U_s$, что $U \equiv (U_1, \ldots, U_s) = U_1 \oplus \ldots \oplus U_s$. Пусть $U \neq V$. Тогда существует допустимое дополнение W, $V = U \oplus W$, в котором можно выбрать допустимое неприводимое подпространство U_{s+1}. Сумма $U + U_{s+1}$, очевидно, будет прямой, и соображения индукции заканчивают доказательство. Обратно, пусть $V = U_1 \oplus \ldots \oplus U_r$, $U_i G \leqslant U_i$, U_i — неприводимое подпространство. Возьмем какое-нибудь допустимое подпространство U. Обозначим через I максимальное подмножество множества индексов $\{1, 2, \ldots, r\}$ с условием $U \cap \sum_{i \in I} U_i = 0$ и докажем, что $V = U \oplus \sum_{i \in I} U_i$. Действительно, в противном случае найдется такое j, что $U_j \cap \left(U \oplus \sum_{i \in I} U_i\right) = 0$. Но тогда

$$U \cap \left(U_j \oplus \sum_{i \in I} U_i\right) = 0,$$

что противоречит выбору I.

20.2.8. У п р а ж н е н и е. Группа линейных преобразований пространства V вполне приводима тогда и

только тогда, когда для всякого допустимого неприводимого подпространства существует допустимое дополнение.

20.2.9. Лемма. *Неприводимое представление абелевой группы G над алгебраически замкнутым полем одномерно.*

Доказательство. Пусть группа G неприводимо действует на пространстве V над алгебраически замкнутым полем K. Если $g \in G$, λ — характеристическое число линейного преобразования g и $vg = \lambda v$, $0 \neq v \in V$, то из $(vf)g = (vg)f = \lambda(vf)$, $f \in G$, следует, что совокупность U всех собственных векторов преобразования g, соответствующих числу λ, является допустимым подпространством. Ввиду неприводимости G получаем $V = U$. Таким образом, каждый ненулевой вектор пространства V является собственным для каждого $g \in G$. Отсюда и из неприводимости G следует одномерность V.

20.3. Критерий сверхразрешимости. Здесь будет установлена

20.3.1. Теорема (Хупперт). *Конечная группа сверхразрешима тогда и только тогда, когда все ее максимальные подгруппы имеют простые индексы.*

Доказательство. Необходимость. Допустим, что G — конечная сверхразрешимая группа, и докажем индукцией по $|G|$ простоту индексов ее максимальных подгрупп.

Ввиду сверхразрешимости в G существует нормальная подгруппа N некоторого простого порядка p. Если теперь M — максимальная подгруппа группы G, то $M \cap N = 1$ или $N \leqslant M$. В первом случае, очевидно, индекс M в G равен p. Во втором случае подгруппа M/N максимальна в G/N и по индуктивному предположению имеет простой индекс. Отсюда следует простота индекса M в G.

Достаточность. Пусть максимальные подгруппы группы G имеют простые индексы, и пусть доказано, что все группы с таким условием, имеющие порядки $< |G|$, сверхразрешимы. Докажем сначала разрешимость группы G. Обозначим через p наибольший простой делитель порядка $|G|$ и через M' какую-нибудь максимальную подгруппу, содержащую силовскую p-подгруппу группы G. Тогда $|G : M'| < p$ и согласно упражнению 11.3.6 пересечение $M'' = \bigcap_{g \in G} M'^g$ отлично от единицы и,

конечно, нормально в G. Таким образом, некоторая минимальная нормальная подгруппа M группы G отлична от G. Возьмем силовскую q-подгруппу Q из M по наибольшему простому делителю q порядка $|M|$ и предположим, что ее нормализатор $N(Q)$ не равен G. Так как $N(Q)M = G$ (лемма Фраттини 17.1.8), то для произвольной максимальной подгруппы $H \geqslant N(Q)$ группы G тем более выполняется равенство $HM = G$, откуда $|G : H| = |M : M \cap H|$. Простой индекс $|M : M \cap H| = q'$ делит число $|M : N_M(Q)|$, взаимно простое с q, и, следовательно, $q' < q$. Снова ввиду упражнения 11.3.6 можно утверждать, что в M существует собственная нормальная подгруппа M_0, содержащая все q-элементы из M. Этим же свойством обладает и всякая подгруппа, сопряженная с M_0. Поэтому пересечение $\bigcap\limits_{g \in G} M_0^g$ отлично от 1, M и нормально в G, что противоречит выбору M. Из полученного противоречия следует, что $N(Q) = G$, т. е. $Q \trianglelefteqslant G$ и, значит, $Q = M$. Таким образом, в группе G есть разрешимая нормальная подгруппа M, фактор-группа по которой согласно индукции сверхразрешима. Отсюда получается разрешимость G.

Как мы знаем, минимальная нормальная подгруппа M разрешимой группы G абелева и разлагается в прямое произведение циклических групп простого порядка q (упражнение 19.1.7). Остается доказать, что $|M| = q$, или по крайней мере существование в G какой-либо циклической нормальной подгруппы. Рассмотрим две возможности.

1) Наибольший простой делитель p порядка группы G больше q. В этом случае в G/M найдется нормальная подгруппа A/M порядка p (теорема 19.2.6). При $N(P) = G$, где $P < A$ — подгруппа порядка p, в группе G существует циклическая нормальная подгруппа, что влечет сверхразрешимость G. Если $N(P) \neq G$, то максимальная подгруппа $H \geqslant N(P)$ не содержит M (иначе было бы $G = N(P)A = HPM \leqslant H$), откуда $G = HM$ и пересечение $H \cap M$ нормально в G. Ввиду минимальности M это пересечение равно единице и, следовательно, так как индекс $|G : H|$ прост, порядок M равен q, что и требовалось доказать.

2) Число q является наибольшим простым делителем порядка группы G. В данной ситуации ввиду сверхразре-

шимости группы G/M и теоремы 19.2.6 силовская q-подгруппа G_q нормальна в G. Из нормальности центра Z подгруппы G_q в группе G и $Z \cap M \neq 1$ (см. 16.2.3) следует $M \leqslant Z$.

Если $M = G_q$, то в фактор-группе G/M найдется нормальная подгруппа A/M простого порядка p, отличного от q. Тогда сверхразрешимость G доказывается так же, как в случае 1).

Пусть теперь $M \neq G_q$. Обозначим через B/M нормальную подгруппу группы G/M порядка q. Очевидно, подгруппа B абелева. Все элементы группы B имеют порядок q — в противном случае B^q была бы искомой подгруппой порядка q, нормальной в группе G.

Предположим сначала, что B не лежит в центре Z. Разумеется, B принадлежит второму гиперцентру группы G_q. В силу сверхразрешимости группы G/B существует такая матрёшка

$$1 < B = B_0 < B_1 < \ldots < B_s = G_q,$$

что $B_i \trianglelefteq G$, $|B_{i+1}: B_i| = q$. Найдется такой номер k, что $B \leqslant Z(B_k)$, но $B \not\leqslant Z(B_{k+1})$. Пусть $B = (M, b)$, $B_{k+1} = (B_k, b_{k+1})$. Тогда совокупность всевозможных элементов вида $[b, x]$, $x \in B_{k+1}$, будет подгруппой порядка q, нормальной в G. Действительно, для произвольных элементов $x = c_1 b_{k+1}^l$, $y = c_2 b_{k+1}^m$, $c_1, c_2 \in B_k$, $g \in G$, имеем:

$$[b, x][b, y] = [b, b_{k+1}^l][b, b_{k+1}^m] = [b, b_{k+1}]^{l+m},$$

$$[b, b_{k+1}]^g = [b^g, b_{k+1}^g] = [ab^n, c_3 b_{k+1}^r] = [b, b_{k+1}]^{n+r},$$

где a, c_3 — некоторые элементы соответственно из M и B_k.

Таким образом, можно считать, что B принадлежит центру группы G_q. Далее, группу B можно рассматривать как линейное пространство над полем $GF(q)$, а группу F автоморфизмов B, индуцированных внутренними автоморфизмами группы G, — как группу линейных преобразований этого пространства (см. пример 20.2.1). Так как $B \leqslant Z$, то порядок группы F, изоморфной $G/C_G(B)$, взаимно прост с q. Поэтому на основании теоремы Машке 20.2.2 допустимое относительно F подпространство M имеет в B допустимое дополнение A размерности 1. На групповом языке это означает, что A является циклической нормальной подгруппой группы G.

Итак, в любом случае G обладает нормальной подгруппой простого порядка. Как отмечалось выше, это доказывает теорему.

20.3.2. Упражнение. Конечная группа сверхразрешима тогда и только тогда, когда сверхразрешима ее фактор-группа по подгруппе Фраттини.

§ 21. Разрешимые группы матриц

В начале главы мы отметили треугольные матричные группы как пример разрешимых групп (упражнение 19.1.2). Другим примером разрешимых матричных групп по существу служит любая конечная разрешимая группа, так как по теореме Кэли 12.1.1 она представима подстановками, а, значит, и матрицами. Объединяя эти примеры, мы можем рассмотреть класс расширений треугольных матричных групп посредством конечных разрешимых групп: согласно упражнению 17.2.7 все такие расширения представимы матрицами. Оказывается, этот класс будет содержать любую разрешимую группу матриц над алгебраически замкнутым полем, так как она почти треугольна с точностью до сопряжения в общей линейной группе. Мы установим эту теорему Колчина — Мальцева в первом пункте настоящего параграфа. Во втором пункте будут рассмотрены разрешимые подгруппы из $GL_n(\mathbb{Z})$ и будет установлено, что все они полицикличны. Наконец, в третьем пункте будет доказано, что голоморф произвольной полициклической группы изморфно вкладывается в $GL_n(\mathbb{Z})$ при подходящем n.

21.1. Почти триангулируемость. Говорят, что группа матриц $H \leqslant GL_n(K)$ *триангулируема*, если при некотором $g \in GL_n(K)$ группа H^g треугольна. Прежде чем доказывать почти триангулируемость разрешимых матричных групп, мы рассмотрим общие свойства неприводимых и вполне приводимых матричных групп (определения и начальные сведения см. в п. 20.2). При этом мы обычно будем отождествлять группу матриц G с группой линейных преобразований некоторого пространства, матрицы которых в фиксированной базе совпадают с элементами из G.

21.1.1. Лемма (Клиффорд). *Нормальная подгруппа H вполне приводимой группы G линейных преобразований векторного пространства V сама вполне приводима.*

Доказательство. Пусть U_1 — допустимое неприводимое относительно H подпространство. Тогда существует минимальное множество элементов $g_1, \ldots, g_s$ группы G такое, что допустимое относительно G замыкание $\bar{U}_1$ подпространства U_1 порождается подпространствами $U_i \equiv U_1 g_i$, $i = 1, \ldots, s$. Легко видеть, что U_i допустимы относительно H и $\bar{U}_1 = U_1 \oplus \ldots \oplus U_s$. При $\bar{U}_1 \neq V$ существует допустимое дополнение B, в котором можно выбрать допустимое неприводимое относительно H подпространство U'. По аналогии с $\bar{U}_1$ строим $\bar{U}_2 = U_{s+1} \oplus \ldots \oplus U_k \leqslant B$. Очевидно, $\bar{U}_1 \oplus \bar{U}_2 = U_1 \oplus \ldots \oplus U_k$. Продолжая аналогичные рассуждения, покажем, что V разлагается в прямую сумму допустимых неприводимых относительно H подпространств. Ввиду леммы 20.2.7 это заканчивает доказательство.

21.1.2. Лемма. *Центр неприводимой группы матриц над алгебраически замкнутым полем состоит из скалярных матриц.*

Доказательство. Пусть G неприводимо действует на линейном пространстве V над алгебраически замкнутым полем. По лемме Клиффорда ее центр Z вполне приводим, и поэтому существует база $v_1, \ldots, v_n$ пространства V, составленная из собственных векторов элементов из Z (см. лемму 20.2.9). Пусть $c \in Z$, $v_i c = \lambda_i v_i$ и, например, $\lambda_1 \neq \lambda_2$. Обозначим через U подпространство, порожденное теми v_i, для которых $\lambda_i = \lambda_1$. Подпространство U будет (собственным) допустимым. Действительно, для произвольного $g \in G$ вектор $v_1 g$ можно представить в виде $v_1 g = \alpha_1 v_1 + \ldots + \alpha_n v_n$. Из неравенств

$$v_1 (gc) = \alpha_1 \lambda_1 v_1 + \ldots + \alpha_n \lambda_n v_n,$$
$$v_1 (cg) = \lambda_1 (\alpha_1 v_1 + \ldots + \alpha_n v_n)$$

в силу $gc = cg$ получаем $\alpha_j = 0$, если $\lambda_j \neq \lambda_1$, и, значит, $v_1 g \in U$. Включение $v_i g \in U$ справедливо, конечно, для всякого $v_i \in U$. Тем самым доказана допустимость U, что противоречит неприводимости группы G. Из полученного противоречия следует, что $\lambda_1 = \lambda_j$, $j = 1, 2, \ldots, n$.

Следующая лемма позволит нам проводить индукцию по степени матриц.

21.1.3. Лемма. *Пусть в неприводимой группе матриц G степени n над алгебраически замкнутым полем существует нецентральная абелева нормальная подгруппа*

H. Тогда в G есть приводимая нормальная подгруппа конечного индекса $\leqslant (n!)!$.

Доказательство. По лемме Клиффорда 21.1.1 подгруппа H вполне приводима. Поэтому ввиду лемм 20.2.7 и 20.2.9 можно считать, что H диагональна. Так как H не лежит в центре G, то существует нескалярная матрица $b \in H$. Для произвольного $g \in G$ элемент b^g принадлежит H и имеет те же характеристические числа, что и b. Поэтому $| b^G | \leqslant n!$. Отображение $G \to S(b^G)$ по правилу

$$g \mapsto \begin{pmatrix} b^x \\ b^{xg} \end{pmatrix}$$

будем гомоморфизмом. Его ядро A, очевидно, содержится в $C_G(b)$ и $| G : A | \leqslant (n!)!$. В центре A содержится нескалярная матрица b, поэтому согласно 21.1.2 группа A приводима.

21.1.4. Лемма. *Если G имеет абелеву нормальную подгруппу A индекса n, то в G существует абелева автоморфно допустимая подгруппа конечного индекса, не превосходящего некоторого числа, зависящего только от n.*

Доказательство. Очевидно, существуют такие автоморфно сопряженные с A подгруппы $A = A_1, A_2, \ldots, A_s$, $s \leqslant n$, что $S = \text{гр}(A_1, \ldots, A_s)$ совпадает с подгруппой, порожденной всеми автоморфно сопряженными с A подгруппами. Подгруппа S автоморфно допустима. Ее центр Z содержит $\bigcap A_i$, и поэтому индекс $| G : Z |$ не превосходит числа n^n. Подгруппа Z будет искомой.

Теперь почти все готово для доказательства теоремы Колчина — Мальцева. Нам понадобится еще только упражнение 27.3.2 из Дополнения, решаемое прямым применением одной локальной теоремы логики. Мы советуем читателю принять это упражнение пока на веру, отложив изучение локальных теорем до § 22, где мы специально их обсуждаем. Можно испробовать и другой путь: решить упражнение непосредственно.

21.1.5. Теорема (Колчин — А. И. Мальцев). *Разрешимая группа G матриц степени n над алгебраически замкнутым полем обладает триангулируемой подгруппой конечного индекса, не превосходящего некоторого числа, зависящего только от n.*

Доказательство. а) Допустим сначала, что группа G неприводима и нильпотентна. Ввиду леммы

20.2.9 достаточно доказать, что G обладает нормальной абелевой подгруппой конечного индекса, не превосходящего некоторого числа $\tau(n)$, зависящего только от n. Мы сделаем это индукцией по n.

Если G неабелева, то в ней найдется нецентральная абелева нормальная подгруппа (такова, например, любая максимальная абелева нормальная подгруппа — см. теорему 16.2.6). Тогда ввиду 21.1.3 в G содержится приводимая нормальная подгруппа H конечного индекса $\leqslant (n!)!$. По лемме Клиффорда 21.1.1 группа H вполне приводима и потому является подпрямым произведением неприводимых нильпотентных групп H_i, степени которых меньше n. В силу индуктивного предположения в каждой группе H_i существует нормальная абелева подгруппа конечного индекса, не превосходящего $\tau(n-1)$. Но тогда в H существует абелева нормальная подгруппа A индекса $< \tau(n-1)^n$. Ввиду $|G:A| < (n!)!\,\tau(n-1)^n$ пересечение B подгрупп, сопряженных с A, имеет в G индекс, не превосходящий некоторого числа, которое можно взять в качестве $\tau(n)$.

б) Откажемся от нильпотентности группы G, т. е. будем считать, что G неприводима и разрешима. Индукцией по n покажем, что G опять обладает нормальной абелевой подгруппой конечного индекса, не превосходящего некоторого числа $\rho(n)$, зависящего только от n.

Если в G существует хотя бы одна нецентральная абелева нормальная подгруппа, то можно дословно повторить доказательство а). Допустим поэтому, что каждая нормальная абелева подгруппа группы G центральна. Обозначим через R подгруппу, порожденную всеми нормальными нильпотентными подгруппами группы G. Ввиду а) и упражнения 27.3.2 из Дополнения в R существует абелева нормальная подгруппа конечного индекса $\leqslant \tau_0(n)$. Согласно 21.1.4 в R существует абелева автоморфно допустимая подгруппа B конечного индекса $\leqslant \tau_1(n)$, где τ_1 — некоторая функция. Отметим, что R нильпотентна, B содержится в центре G. Оценим индекс $|G:R|$.

Пусть $1 < B = B_0 < B_1 < \ldots < B_s = R$ — центральная матрёшка автоморфно допустимых подгрупп группы R. Пусть Z — централизатор этой матрёшки в G, т. е. $Z = \bigcap Z_i$, где Z_{i+1}/B_i — централизатор секции B_{i+1}/B_i в G/B_i. Очевидно, $R \leqslant Z$. Если $R < Z$ и A/R — неэди-

ничная абелева автоморфно допустимая подгруппа в Z/R, отличная от единицы, то A — нильпотентная нормальная подгруппа в G, строго содержащая R, что невозможно. Значит, $Z = R$. Так как $B \leqslant Z(G)$ и $|R:B| \leqslant \tau_1(n)$, то $|G:R| \leqslant \tau_2(n)$, где τ_2 — функция. Таким образом, можно взять $\rho(n) = \tau_1(n)\,\tau_2(n)$, и B будет искомой подгруппой.

в) Рассмотрим, наконец, общий случай. Пусть V — пространство с фиксированной базой $e_1, \ldots, e_n$, на котором действует G. Возьмем неуплотняемую матрёшку

$$V = V_1 > V_2 > \ldots > V_{s+1} = 0 \qquad (1)$$

G-допустимых подпространств. Группа G на каждой секции V_i/V_{i+1} действует неприводимо. Ввиду б) в ней существуют такие нормальные подгруппы G_i, что $|G:G_i| \leqslant \rho(n)$ и G_i/A_i абелева, где A_i — ядро индуцированного в V_i/V_{i+1} представления группы G. Положим $G_0 = \bigcap_i G_i$. Тогда на основании леммы 20.2.9 матрёшку (1) можно уплотнить до G_0-допустимой матрёшки

$$V = V_1' > V_2' > \ldots > V_{n+1}' = 0$$

с одномерными секциями. Матрицы линейных преобразований из G_0 в базе $f_1, \ldots, f_n$, $f_j \in V_j' \setminus V_{j+1}'$, имеют треугольный вид. Следовательно, подгруппа G_0 сопряжением с помощью матрицы перехода от $\{f_j\}$ к $\{e_i\}$ приводится к треугольному виду. Индекс подгруппы G_0, очевидно, ограничен некоторым числом, зависящим только от n. Теорема доказана.

21.1.6. Упражнение. Ступень разрешимости произвольной разрешимой группы матриц степени n не превосходит некоторого числа, зависящего только от n. Вывести отсюда, что если в группе матриц все конечно порожденные подгруппы разрешимы, то она сама разрешима.

21.1.7. Упражнение. Разрешимая матричная группа степени n обладает нормальной подгруппой, коммутант которой нильпотентен, а индекс не превосходит некоторого числа, зависящего только от n. Этот результат бывает, в частности, полезным при доказательстве непредставимости матрицами тех или иных абстрактных

групп (см., например, Смирнов Д. М.— Матем.сб., 1965, 67, № 3, с. 366—383).

21.2. Полициклическая разрешимых групп из $GL_n(\mathbb{Z})$. Пусть $\overline{\mathbb{Q}}$ — алгебраическое замыкание поля $\mathbb{Q}$ рациональных чисел. Элементы из $\overline{\mathbb{Q}}$ называются *алгебраическими числами*. Элемент из $\overline{\mathbb{Q}}$ называется *целым* алгебраическим числом, если он является корнем многочлена с целыми коэффициентами и старшим коэффициентом 1.

Пусть K — поле алгебраических чисел, имеющее конечную степень над полем $\mathbb{Q}$. Согласно § 28 Дополнения множество k всех целых алгебраических чисел поля K является кольцом, причем аддитивная и мультипликативная группы кольца k конечно порождены. С помощью этих результатов теории чисел сейчас будет доказана

21.2.1. Теорема (А. И. Мальцев). *Всякая разрешимая группа целочисленных матриц полициклична.*

Доказательство. Пусть G — разрешимая группа целочисленных матриц степени n. По теореме Колчина — Мальцева 21.1.5 существует такая матрица $g = (g_{ij})$ и такая подгруппа $A \leqslant G$ конечного индекса, что $B = A^g$ принадлежит группе треугольных матриц $T_n(K)$ над алгебраическим расширением

$$K = \mathbb{Q}(g_{11}, g_{12}, \ldots, g_{nn})$$

поля $\mathbb{Q}$. Элементы g_{ij} можно считать, очевидно, целыми числами поля K. Отсюда получаем, что всякий элемент произвольной матрицы из B представляется в виде дроби, числитель которой есть некоторое целое алгебраическое число, а знаменатель равен определителю матрицы g. Пусть k обозначает кольцо всех целых алгебраических чисел из K, k^* — мультипликативная группа кольца k. Диагональные элементы матриц из B удовлетворяют характеристическим уравнениям матриц из A, старшие коэффициенты которых равны 1, значит, эти диагональные элементы принадлежат k^*. Рассмотрим гомоморфизм $B \to k^* \times \ldots \times k^*$ (n раз), сопоставляющий каждой матрице $b \in B$ ее диагональ. Пусть C — ядро этого гомоморфизма. По теореме 28.1.12 из Дополнения фактор-группа B/C конечно порождена. Ядро C состоит из всевозможных унитреугольных матриц группы B. Обозначим через C_i подгруппу всех матриц из C, имеющих i нулевых

диагоналей выше главной. Очевидно, матрёшка

$$C = C_0 \geqslant C_1 \geqslant \ldots \geqslant C_{n-1} = 1$$

будет нормальной матрёшкой группы C. Легко понять, что каждая секция C_i/C_{i+1} изоморфна подгруппе прямой суммы $n - i - 1$ экземпляров аддитивной группы кольца k, которая по теореме 28.1.6 из Дополнения конечно порождена. Отсюда следует конечная порожденность C, а значит и группы B. Так как $B = A^g$ и индекс $|G : A|$ конечен, то вся группа G конечно порождена. Ясно, что это доказывает теорему.

С помощью этой теоремы можно получить следующее более сильное утверждение.

21.2.2. Теорема. *Разрешимая группа автоморфизмов конечно порожденной абелевой группы полициклична.*

Доказательство. Пусть A — конечно порожденная абелева группа, Φ — некоторая разрешимая группа ее автоморфизмов. Обозначим через H периодическую часть группы A и рассмотрим гомоморфизм $\tau\colon \Phi \to \mathrm{Aut}\,(A/H)$, сопоставляющий произвольному $\varphi \in \Phi$ автоморфизм $\bar{\varphi}$ фактор-группы A/H, индуцированный φ, т. е. $(Ha)^{\bar{\varphi}} = Ha^{\varphi}$. По предыдущей теореме фактор-группа Φ/Ψ, где $\Psi = \ker \tau$, конечно порождена. Докажем конечность Ψ. Действительно, если $a_1, \ldots, a_n$ — система порождающих группы A, то для произвольного $\psi \in \Psi$ имеем $a_i^{\psi} = h_i a_i$, $h_i \in H$. Ввиду конечности периодической части H имеется лишь конечное число возможностей для образов порождающих a_i при отображениях из Ψ. Отсюда следует конечность группы Ψ и, значит, конечная порожденность Φ. Теперь ясно, что Φ — полициклическая группа, что и требовалось доказать.

21.3. **Вложение голоморфов полициклических групп в $GL_n(\mathbb{Z})$.** Пусть G — группа. Легко видеть, что мы получим действие голоморфа $\mathrm{Hol}\,G$ на целочисленном групповом кольце $\mathbb{Z}[G]$, если положим

$$(\sum \alpha_i g_i)^{\varphi g} = \sum \alpha_i g_i^{\varphi} g,\ \alpha_i \in \mathbb{Z},\ \varphi \in \mathrm{Aut}\,G,\ g_i, g \in G. \quad (2)$$

21.3.1. Лемма. *Пусть $G \leqslant GL_n(\mathbb{Z})$, N — унитреугольная нормальная подгруппа в G, а G/N конечно порождена. Если Φ — подгруппа из* Aut G, *отображающая N в себя и действующая тождественно в G/N, то существует*

изоморфное вложение $\Phi G \to GL_m(\mathbb{Z})$, *унитреугольное на* N.

Доказательство. Продолжим заданное вложение $G \leqslant GL_n(\mathbb{Z})$ до кольцевого гомоморфизма ρ: $\mathbb{Z}[G] \to M_n(\mathbb{Z})$; пусть K — его ядро. Пусть I — идеал кольца $\mathbb{Z}[G]$, порожденный всевозможными разностями $1 - x$, $x \in N$. Так как группа N унитреугольна, то

$$((1 - x_1) \dots (1 - x_n))^\rho = 0 \text{ при } x_i \in N,$$

откуда $I^n \subset K$ и, следовательно, $(I + K)^n \subset K$. По теореме 26.1.4 Дополнения аддитивная группа $\mathbb{Z}[G]/(I + K)^n$ конечно порождена. Пусть $T/(I + K)^n$ — ее периодическая часть. Так как аддитивная группа $\mathbb{Z}[G]/K$ не имеет кручения, то $T \subset K$. По условию, для любых $\varphi \in \Phi$, $g \in G$ имеем $g^\varphi = gx$, $x \in N$, поэтому $g^\varphi - g = g(x - 1) \in I$. Отсюда видно, что аддитивная группа $I + K$ ΦG-допустима. Следовательно, действие группы ΦG на $\mathbb{Z}[G]$ в силу (2) индуцирует действие ΦG на конечно порожденной аддитивной группе $\mathbb{Z}[G]/T$. Оно точное, так как $T \subset K$. Остается проверить, что N действует на $\mathbb{Z}[G]/T$ унитреугольно. Для этого из соображений индукции достаточно указать в $\mathbb{Z}[G]/T$ N-неподвижный элемент, отличный от нуля. Так как $I^n \subset T$, то существует такое $s \geqslant 0$, что $I^s \not\subset T$, $I^{s+1} \subset T$ (мы считаем здесь, что $I^0 = \mathbb{Z}[G]$). Всякий элемент из $I^s \setminus T$ по модулю T отличен от нуля и N-неподвижен. Лемма доказана.

21.3.2. Теорема (Ю. И. Мерзляков). *Голоморф* Hol G *произвольной полициклической группы* G *изоморфно вкладывается в* $GL_n(\mathbb{Z})$ *при подходящем* n.

Доказательство. а) Группа G обладает автоморфно допустимой матрёшкой $G \geqslant M \geqslant N \geqslant 1$, где $|G : M| < \infty$, M — группа без кручения, M/N — абелева группа без кручения, N — максимальная нильпотентная нормальная подгруппа в M. В самом деле, возьмем в G нормальную матрёшку $G = G_1 > G_2 > \dots > G_{l+1} = 1$, каждая секция которой либо имеет простой период, либо не имеет кручения. Группа G действует в этих секциях сопряжениями, что определяет матричные представления $G \to \mathrm{Aut}(G_i/G_{i+1})$. По теореме Колчина — Мальцева 21.1.5 для каждого i существует подгруппа T_i конечного индекса в G, вызывающая в векторном пространстве G_i/G_{i+1} треугольные автоморфизмы. Пересечение $T =$

$= \bigcap T_i$ также имеет конечный индекс в G и действует треугольно во всех секциях. Ввиду 17.2.3 можно считать, что T не имеет кручения. Так как коммутант T' действует унитреугольно, то $[G_i, T', \ldots, T'] \leqslant G_{i+1}$. Следовательно, $[G, T', \ldots, T'] = 1$, если число коммутирований достаточно велико. В частности, группа T' нильпотентна. Мы знаем, что в конечно порожденной группе всякая подгруппа конечного индекса содержит вербальную подгруппу конечного индекса (упражнение 15.2.3). Пусть V — такая вербальная подгруппа в G, что $V \leqslant T$, $|G : V| < \infty$, и пусть N — максимальная нильпотентная нормальная подгруппа в V. Так как $V' \leqslant T' \cap V \leqslant N$, то группа V/N абелева. Пусть m — период ее периодической части. Положим $M = V^m N$. Ясно, что группы M, N — искомые.

б) Пусть Φ — группа всех автоморфизмов группы M, действующих в M/N тождественно. Покажем, что существует изоморфное матричное представление группы ΦM над $\mathbb{Z}$, унитреугольное на N. Докажем сначала представимость самой M индукцией по степени r свободной абелевой группы M/N. Если $r = 0$, то это следует из теоремы 17.2.5. Пусть

$$M = (a) \cdot M_0, \quad (a) \cap M_0 = 1, \quad N \leqslant M_0 \lhd M$$

и степень M_0/N равна $r - 1$. По индукции можно считать, что M_0 имеет требуемое представление. Тогда, ввиду леммы 21.3.1, такое представление имеет и M. Применив 21.3.1 еще раз, получим представление для ΦM.

в) Голоморф $\mathrm{Hol}\, M$ изоморфно представим матрицами над $\mathbb{Z}$. В самом деле, ввиду б) и 17.2.7 достаточно убедиться, что $|\mathrm{Aut}\, M : \Phi| < \infty$. Это мы и проверим. Прежде всего, из коммутативности M/N и коммутаторных соотношений (см. п. 3.2) следует, что в $\mathrm{Hol}\, M$

$$[M/N, \alpha]^m \leqslant [(M/N)^m, \alpha] \leqslant [M^m, \alpha]\, N/N \qquad (3)$$

для всех $\alpha \in \mathrm{Aut}\, M$, $m = 1, 2, \ldots$ Пусть $\beta \in \mathrm{Aut}\, M$. Так как подгруппа $(\beta) M$ из голоморфа $\mathrm{Hol}\, M$ полициклическая, то она содержит нормальную подгруппу T некоторого конечного индекса m, коммутант которой T' нильпотентен (см. а)). Так как N — максимальная нильпотентная нормальная подгруппа в M, то

$$[M^m, \beta^m] \leqslant T' \cap M \leqslant N.$$

Отсюда и из (3) следует, что $[M/N, \beta^m]^m = 1$. Так как M/N без кручения, то $[M/N, \beta^m] = 1$, т. е. $\beta^m \in \Phi$. Таким образом, группа $(\mathrm{Aut}\, M)/\Phi$ периодическая. Если r — ранг M/N, то имеем очевидное вложение $(\mathrm{Aut}\, M)/\Phi \to \to \boldsymbol{GL}_r(\mathbb{Z})$. Так как $\boldsymbol{GL}_r(\mathbb{Z})$ почти вся без кручения (упражнение 19.3.4), то $(\mathrm{Aut}\, M)/\Phi$ конечна.

г) Голоморф $\mathrm{Hol}\, G$ изоморфно представим матрицами над $\mathbb{Z}$. В самом деле, воспользуемся тем, что для произвольной группы X существует вложение

$$\mathrm{Hol}\, X \to \mathrm{Aut}\,(X \wr \mathbb{Z}_2). \tag{4}$$

Чтобы получить это вложение, зададим действие $\mathrm{Hol}\, X$ на $X \wr \mathbb{Z}_2$, полагая

$$\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}^{\varphi g} = \begin{pmatrix} x^{\varphi g} & 0 \\ 0 & y^{\varphi} \end{pmatrix}, \quad \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}^{\varphi g} = \begin{pmatrix} 0 & g^{-1}x^{\varphi} \\ y^{\varphi} g & 0 \end{pmatrix} \tag{5}$$

для всех $\varphi \in \mathrm{Aut}\, X$, $x, y, g \in X$. Все нужные свойства без труда проверяются. Если X — полициклическая группа, то, очевидно, группа $X \wr \mathbb{Z}_2$ такая же, поэтому вместо $\mathrm{Hol}\, G$ достаточно представить матрицами $\mathrm{Aut}\, G$. Далее, пусть Γ — группа всех автоморфизмов группы G, действующих тождественно в (конечной) секции G/M. Так как $|\mathrm{Aut}\, G : \Gamma| < \infty$, то достаточно представить Γ. Пусть S — конечное порождающее множество группы G по модулю M. Рассмотрим отображение $\Gamma \to \mathrm{Hol}\, M \times \ldots \times \mathrm{Hol}\, M$ по правилу

$$\gamma \mapsto \prod_{s \in S} \gamma|_M \cdot [\gamma, s]. \tag{6}$$

Непосредственно проверяется, что это изоморфное вложение. Так как $\mathrm{Hol}\, M$ изоморфно представима матрицами над $\mathbb{Z}$ (см. в)), то и Γ такая же. Теорема доказана.

21.3.3. Упражнение. Если M — автоморфно допустимая подгруппа конечного индекса в некоторой группе G и $\mathrm{Hol}\, M$ изоморфно представима матрицами, то и $\mathrm{Hol}\, G$ изоморфно представима матрицами.

21.3.4. Упражнение. Голоморф произвольной полициклической группы почти весь не имеет кручения и для всякого простого числа p почти весь аппроксимируется конечными p-группами.

У к а з а н и е. См. доказательство теоремы 14.2.2.

Роль теоремы 21.3.2 состоит в том, что она открывает путь в теорию полициклических групп методам алгебраической геометрии, теории чисел и p-адического анализа — в зависимости от выбора основного кольца коэффициентов, в которое мы погружаем $\mathbb{Z}$. Например, как заметил Верфриц, эта теорема позволяет доказать конечную определенность группы автоморфизмов произвольной полициклической группы G (Auslander L.— Ann. Math., 1969, 89, № 2, p. 314—322) следующим образом. Если $\mathrm{Hol}\, G \leqslant \leqslant GL_n(\mathbb{Z})$ и G замкнута в полиномиальной топологии, то ее нормализатор и централизатор в $GL_n(\mathbb{Z})$ также замкнуты и, значит, конечно определены (Borel A.— Proc. Internat. Congress of Mathns, Stockholm, 1962, p. 10—22). Поэтому группа $\mathrm{Aut}\, G \simeq N_*(G)/C_*(G)$ конечно определена. Если G не замкнута, то рассуждения несколько усложняются. Подробности и другие интересные комментарии к теореме 21.3.2 можно найти в докладе Верфрица, прочитанном 22 июня 1973 года на симпозиуме в Лондоне [44].

В связи с конструкцией, встретившейся нам мимоходом в конце доказательства 21.3.2, отметим следующий

21.3.5. В о п р о с [13]. Пусть C — фиксированная неединичная группа (например, $C = \mathbb{Z}_2$). Известно (Алгебра и логика, 1970, 9, № 5, с. 539—558), что для любых групп A, B все расщепляемые расширения группы B посредством группы A вкладываются некоторым единым способом в прямое произведение $A \times \mathrm{Aut}\,(B\ r\ C)$. Как они в нем расположены?

§ 22. Обобщения разрешимости

22.1. **Классы Куроша — Черникова.** Мы знаем, что разрешимость можно определить как наличие конечной субнормальной матрёшки с абелевыми секциями или конечной нормальной матрёшки с абелевыми секциями, а также как обрыв ряда коммутантов на единице,— все эти условия равносильны. Возникает мысль рассмотреть бесконечные субнормальные матрёшки разных типов и выяснить свойства получающихся классов и связи между ними (естественно ожидать, что равносильные условия перестанут быть таковыми в общем случае). Такая теория «обобщенно разрешимых» групп была создана и осново-

полагающей тут явилась работа А. Г. Куроша и С. Н. Черникова [15]. Мы будем называть классы обобщенно разрешимых групп, возникающие в рамках этой теории, *классами Куроша — Черникова*, хотя некоторые из них рассматривались и до работы [15]. В настоящем пункте будут приведены определения и обозначения этих классов.

Основным понятием теории классов Куроша — Черникова является следующее понятие субнормальной матрёшки, не обязательно конечной.

Система $\mathcal{M}$ подгрупп группы G называется *субнормальной матрёшкой*, если она:

1) содержит 1 и G;

2) линейно упорядочена по вложению, т. е. для всяких A, B из $\mathcal{M}$ либо $A \leqslant B$, либо $B \leqslant A$;

3) замкнута относительно объединений и пересечений, в частности, вместе с каждым $A \neq G$ содержит пересечение $A^{\#}$ всех $H \in \mathcal{M}$ с условием $H > A$ и вместе с каждым $B \neq 1$ содержит объединение $B^{\flat}$ всех $H \in \mathcal{M}$ с условием $H < B$;

4) удовлетворяет условию $A \trianglelefteqslant A^{\#}$ для всех $A \in \mathcal{M}$, $A \neq G$.

Фактор-группы $A^{\#}/A$ называются *секциями* субнормальной матрёшки $\mathcal{M}$. Говорят, что $\mathcal{M}$ *вполне упорядочена по возрастанию*, если $A^{\#} \neq A$ для всех $A \neq G$, и *вполне упорядочена по убыванию*, если $B^{\flat} \neq B$ для всех $B \neq 1$. Субнормальная матрёшка называется *нормальной*, если все ее члены нормальны в группе. Если одна субнормальная матрёшка содержит другую, то первая называется *уплотнением* второй. Обобщая определение из п. 16.1, нормальную матрёшку $\mathcal{M}$ называют *центральной*, если все ее секции центральны, т. е.

$$A^{\#}/A \leqslant Z(G/A) \text{ для всех } A \in \mathcal{M},\ A \neq G,$$

или, что равносильно,

$$[A^{\#}, G] \leqslant A \text{ для всех } A \in \mathcal{M},\ A \neq G.$$

Наконец, субнормальную матрёшку называют *разрешимой*, если все ее секции абелевы.

Возникают следующие *классы Куроша — Черникова* (мы сохраняем традиционные обозначения, хотя и не считаем их вполне удачными):

RN: группа обладает разрешимой субнормальной матрёшкой (не обязательно конечной — эта оговорка в дальнейшем не повторяется, но всегда предполагается);

RN^*: группа обладает разрешимой субнормальной матрёшкой, вполне упорядоченной по возрастанию;

$\overline{RN}$: всякую субнормальную матрёшку группы можно уплотнить до разрешимой субнормальной матрёшки;

RI: группа обладает разрешимой нормальной матрёшкой;

RI^*: группа обладает разрешимой нормальной матрёшкой, вполне упорядоченной по возрастанию;

$\overline{RI}$: всякую нормальную матрёшку группы можно уплотнить до разрешимой нормальной матрёшки;

Z: группа обладает центральной матрёшкой;

ZA: группа обладает центральной матрёшкой, вполне упорядоченной по возрастанию;

ZD: группа обладает центральной матрёшкой, вполне упорядоченной по убыванию;

$\overline{Z}$: всякую нормальную матрёшку можно уплотнить до центральной матрёшки;

$\bar{N}$: всякую подгруппу можно включить в субнормальную матрёшку;

N: всякую подгруппу можно включить в субнормальную матрёшку, вполне упорядоченную по возрастанию.

Сами матрёшки, упоминаемые в этих определениях, удобно называть соответственно *RN-матрёшками*, *RN*-матрёшками* и т. д.

22.1.1. Упражнение. Условие N равносильно нормализаторному условию из п. 18.2.

22.1.2. Упражнение. Для конечных групп условия RN, RN^*, $\overline{RN}$, RI, RI^*, $\overline{RI}$ равносильны разрешимости, а условия Z, ZA, ZD, $\overline{Z}$, $\bar{N}$, N — нильпотентности.

22.1.3. Упражнение. Группа тогда и только тогда обладает свойством $\overline{RI}$ (соответственно $\overline{Z}$), когда все ее гомоморфные образы обладают свойством RI (соответственно Z).

22.1.4. Упражнение. Свойства RN^*, RI^*, ZA, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\bar{N}$, N переносятся на гомоморфные образы.

Многие свойства разрешимых и нильпотентных групп без труда переносятся (вместе с доказательством) на их обобщения:

22.1.5. Упражнение. Стабилизатор произвольной нормальной матрёшки обладает центральной матрёшкой. (Ср. с 16.3.1.)

22.1.6. Упражнение. Коммутант всякой группы, обладающей нормальной матрёшкой с циклическими секциями, обладает центральной матрёшкой. (Ср. с 19.2.2.)

22.1.7. Упражнение. Во всякой ZA-группе G всякая максимальная абелева нормальная подгруппа A совпадает со своим централизатором. В частности, A — максимальная абелева подгруппа и G/A изоморфно вкладывается в $\mathrm{Aut}\, A$. (Ср. с 16.2.6.)

Классы Куроша — Черникова весьма широки,— например, класс Z содержит ввиду теоремы Магнуса 14.4.4 все свободные группы. Более тонким является утверждение, что всякая счетная свободная группа изоморфно вкладывается в некоторую группу класса $\overline{Z}$,— это покажет один из примеров, к которым мы сейчас переходим.

22.2. Примеры. Важный пример обобщенно разрешимых групп дают упорядочиваемые группы.

22.2.1. Пример. Всякая упорядочиваемая группа G обладает свойством RN (напомним, что группа называется *упорядочиваемой*, если на ней можно задать линейное упорядочение $\leqslant$, устойчивое относительно умножения; подробнее см. п. 27.2 Дополнения). Действительно, пусть G — группа с линейным упорядочением $\leqslant$. Ее подмножество V называется *выпуклым*, если вместе с любыми двумя своими элементами a, b оно содержит и все промежуточные элементы, т. е.

$$a \in V, b \in V, a \leqslant x \leqslant b \Rightarrow x \in V.$$

Оказывается, система $\mathscr{M}$ всех выпуклых подгрупп упорядоченной группы G является разрешимой субнормальной матрёшкой. Действительно, условие 1) из определения субнормальной матрёшки очевидно. Проверим условие 2). Пусть A, B — выпуклые подгруппы и существует элемент $b \in B$, $b \notin A$. Пусть, скажем, $b > 1$. Ясно, что $a \leqslant b$ для любого $a \in A$. Так как $1 \leqslant a \leqslant b$ или $1 \leqslant a^{-1} \leqslant b$, то $A \leqslant B$, что и требовалось. Условие 3) очевидно. Проверим 4), т. е. условие $A \lhd B$, где A, B — выпуклые подгруппы, причем $A < B$ и между ними не содержится никаких других выпуклых подгрупп. Для любого $b \in B$ имеем $A^b < B^b$, причем ясно, что A^b, B^b — снова вы-

пуклые подгруппы и между ними нет других выпуклых подгрупп. Так как $B^b = B$, то $A^b = A$, что и требовалось доказать. Наконец, каждая секция $A^{\#}/A$ матрёшки $\mathcal{M}$ есть упорядоченная группа, не содержащая собственных выпуклых подгрупп. По классической теореме Гёльдера об упорядоченных группах (она доказывается в [10] на одной странице на основе определений) секция $A^{\#}/A$ изоморфно вкладывается в аддитивную группу поля $\mathbb{R}$, в частности, абелева. Значит, $\mathcal{M}$ — разрешимая субнормальная матрёшка.

Теперь обратимся к примерам обобщенно нильпотентных групп. Важный тип таких примеров доставляют разного рода конгруэнц-подгруппы — как классические $\Gamma_n(m)$ над кольцом $\mathbb{Z}$, так и их аналоги над другими кольцами. Рассмотрим здесь

22.2.2. Пример (Мерзляков Ю. И.— Алгебра и логика, 1963, **2**, № 5, с. 29—36). Пусть k — множество, состоящее из нуля и всех рациональных чисел, имеющих в несократимой записи нечетный знаменатель. Очевидно, k — кольцо. Пусть

$$G_n = \begin{pmatrix} 1+2^n k & 2^n k \\ 2^n k & 1+2^n k \end{pmatrix}, \quad n = 1, 2, \ldots,$$

т. е. G_n — совокупность матриц, элементы которых независимо друг от друга пробегают соответствующие множества рациональных чисел. Легко понять, что каждое G_n — группа. Как мы знаем, группа G_1 содержит свободную подгруппу ранга 2 (см. теорему 14.2.1), а поэтому и свободные подгруппы любого конечного или счетного ранга. Покажем, что G_1 обладает также свойством $\overline{Z}$, т. е. что фактор-группа группы G_1 по любой нормальной подгруппе H обладает центральной матрёшкой (см. упражнение 22.1.3).

Прежде всего, если H лежит в центре G_1, то система фактор-групп

$$G_1/H \geqslant G_2H/H \geqslant \ldots \geqslant \bigcap_{n=1}^{\infty} (G_nH/H) \geqslant 1$$

будет, как нетрудно проверить, центральной матрёшкой фактор-группы G_1/H. Допустим теперь, что нормальная подгруппа H не лежит в центре G_1, и покажем, что тогда

$$H \geqslant T \cap G_n \text{ при некотором } n, \qquad (1)$$

где T — совокупность матриц из G_1 с определителем 1. Этим всё будет доказано, так как группа G_1/H будет тогда гомоморфным образом группы $G_1/T \cap G_n$, вкладывающейся по теореме Ремака 4.3.9 в прямое произведение абелевой группы G_1/T и нильпотентной группы G_1/G_n. А для доказательства утверждения (1) мы снова применим плодотворный философский метод вытягивания цепи (см. стр. 117).

а) Подгруппа H содержит матрицу h с условием $h_{11}^2 \neq h_{22}^2$. Действительно, пусть c — какая-нибудь нескалярная матрица из H. Непосредственно проверяется, что в качестве h годится одна из матриц c, c^a, c^b, $c^a c$, $c^b c$, $c^a c^b$, где $a = t_{12}(2)$, $b = t_{21}(2)$.

б) Если H содержит h, то H содержит также трансвекции $t_{12}(\lambda)$, $t_{21}(\lambda)$, где $\lambda = 2\mu((h_{22}^2 / h_{11}^2) - 1)$, μ — произвольное рациональное число с нечетными числителем и знаменателем. В самом деле, непосредственно проверяется, что $t_{12}(\lambda) = [a, h^u h]^v$, где $a = t_{12}(2)$, $u = \operatorname{diag}(-h_{22}, h_{11})$, $v = \operatorname{diag}(1, \mu)$. А матрица $t_{21}(\lambda)$ получается транспонированием этого соотношения, причем h можно не транспонировать, поскольку λ зависит только от ее диагональных элементов. Отметим полезную в этих вычислениях формулу

$$x^d = \begin{pmatrix} x_{11} & \frac{\beta}{\alpha} x_{12} \\ \frac{\alpha}{\beta} x_{21} & x_{22} \end{pmatrix} \text{ при } d = \operatorname{diag}(\alpha, \beta).$$

в) Существует такое $m \geqslant 1$, что H содержит все трансвекции $t_{12}(2^m \varkappa)$, $t_{21}(2^m \varkappa)$, $\varkappa \in k$. Это сразу вытекает из а) и б).

г) Подгруппа H содержит произвольную матрицу

$$x = \begin{pmatrix} 1 + 2^{2m}\alpha & 2^{2m}\beta \\ 2^{2m}\gamma & 1 + 2^{2m}\delta \end{pmatrix}, \quad \alpha, \beta, \gamma, \delta \in k, \quad \det x = 1.$$

Действительно, непосредственно проверяется, что

$$x = t_{12}(2^m \xi)\, t_{21}(2^m \delta)\, t_{12}(2^m)\, t_{21}(2^m \eta), \tag{2}$$

где

$$\xi = \frac{2^m \beta - 1}{x_{22}}, \quad \eta = \frac{2^m \gamma - \delta}{x_{22}}.$$

На этом вытягивание элементов заканчивается.

Попутно получается положительное решение конгруэнц-проблемы для группы $SL_2(k)$. В самом деле, пусть H — нормальная подгруппа в $SL_2(k)$ конечного индекса n. Так как n-е степени трансвекций из $SL_2(k)$ лежат в H, то выполняется в). Так как в) $\Rightarrow$ г), то H — конгруэнц-подгруппа.

Отметим, что двойка не играла в наших рассуждениях особой роли. Аналогично устанавливается, например, следующий факт. Пусть π — множество, получаемое из множества всех простых чисел удалением конечного подмножества (назовем его π'), $\mathbb{Q}_\pi$ — кольцо π-ичных дробей, т. е. рациональных чисел, знаменатели которых делятся только на простые числа из π. Каждая подгруппа H конечного индекса n в $SL_2(\mathbb{Q}_\pi)$ является конгрузнц-подгруппой. В самом деле, пусть H нормальна и q — произведение всех чисел из π'. Возьмем какую-нибудь верхнюю границу $m \geqslant 1$ для показателей, с которыми делители из π' входят в n. Так как H содержит все трансвекции $t_{ij}(q^m\varkappa)$, $\varkappa \in \mathbb{Q}_\pi$, то наше утверждение вытекает из следующего аналога разложения (2) при $\mu = \mu' = q^m$.

$$x \equiv \begin{pmatrix} 1+\mu\mu'\alpha & \mu\mu'\beta \\ \mu\mu'\gamma & 1+\mu\mu'\delta \end{pmatrix} = t_{12}(\mu\xi)\, t_{21}(\mu'\delta)\, t_{12}(\mu)\, t_{21}(\mu'\eta), \qquad (2')$$

где

$$\det x = 1, \quad \xi = \frac{\mu'\beta - 1}{x_{22}}, \quad \eta = \frac{\mu\gamma - \delta}{x_{22}}.$$

Из примера 22.2.2 видно, что свойства $\overline{RI}$ и $\overline{Z}$ не переносятся на подгруппы, так как свободные нециклические группы этими свойствами не обладают (см. 22.1.4).

Продолжая изложенную здесь работу, Г. А. Носков показал (Сиб. матем. ж., 1973, 14, № 3, с. 680—683), что группа G_1 обладает и свойством $\overline{RN}$, так что оно тоже не переносится на подгруппы.

В топологических группах условия конечности и обобщенной разрешимости исследовали В. М. Глушков, В. С. Чарин и другие авторы.

22.3. Локальная теорема. Система M_i, $i \in I$, подмножеств множества M называется его *локальным покрытием*, если любой элемент из M содержится в некотором M_i и любые два множества M_i, M_j содержатся в некотором третьем множестве M_k. Примеры локальных покрытий —

система всех конечных подмножеств данного множества и система всех конечно порожденных подгрупп данной группы. Говорят, что *группа G локально обладает свойством* σ, если существует локальное покрытие группы G, состоящее из подгрупп со свойством σ. Ясно, что если σ переносится на подгруппы, то G тогда и только тогда локально обладает свойством σ, когда любая конечно порожденная подгруппа из G обладает этим свойством. Примерами локальных свойств могут служить локальная нильпотентность и локальная конечность, встречавшиеся нам в предыдущей главе.

Говорят, что для свойства групп (и соответствующего класса групп) справедлива *локальная теорема*, если всякая группа, локально обладающая этим свойством, сама обладает им. Так, локальная теорема справедлива в классе абелевых групп и не справедлива в классе конечных групп.

Почему для одних свойств локальная теорема справедлива, а для других нет? Задавшись этим вопросом, А. И. Мальцев (Уч. зап. Ивановского пед. ин-та, 1941, 1, № 1, с. 3—9) обратил внимание на то, что локальные теоремы не специфичны для теории групп, а столь же естественны для колец, луп и других алгебраических систем, поэтому ключ к ним надо искать не в теории групп или других частных теориях, а в основаниях математики. И действительно, идейным источником самых разнообразных локальных теорем оказалось следующее замечание формальной логики: если теорема выводится из некоторого списка аксиом, то она выводится из конечной части этого списка. Развивая это замечание, А. И. Мальцев пришел к своей теореме компактности узкого исчисления предикатов, а от нее — к локальной теореме для любого свойства, записываемого так называемыми квазиуниверсальными формулами. Тем самым вопрос о справедливости локальной теоремы для данного свойства σ, который до А. И. Мальцева решался кустарно для каждого σ, был сведен к общему и чисто «грамматическому» вопросу: нельзя ли записать σ квазиуниверсальными аксиомами?

С помощью остроумного приема, который мы здесь изложим, А. И. Мальцев еще в упомянутой выше работе 1941 года записал квазиуниверсальными формулами специального вида свойства RN, RI, Z и этим способом дока-

зал для них локальную теорему. Позднее он вернулся к своему методу, придал ему современную общность и в работе «Модельные соответствия» (Изв. АН СССР, сер. матем., 1959, **23**, № 3, с. 313—336) единообразно получил практически все интересные локальные теоремы теории групп. Можно сказать, что работа 1941 года впервые поставила «и» между локальными теоремами алгебры и логикой, а работа 1959 года в известном смысле поставила точку над «и». Вместе с тем первая работа явилась исходным пунктом теории моделей.

Мы докажем здесь методом А. И. Мальцева локальную теорему для классов Куроша — Черникова. Замкнутое изложение логической части метода дается в § 27 Дополнения. Читатель, незнакомый с этим методом, должен обратиться сейчас к Дополнению, а затем продолжать чтение.

22.3.1. Теорема (А. И. Мальцев). *Для свойств* RN, RI, Z, $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\bar{N}$ *справедлива локальная теорема.*

Доказательство. Используя упоминавшийся прием А. И. Мальцева, перейдем от языка субнормальных матрёшек к языку предикатов. Для этого с каждой субнормальной матрёшкой $\mathcal{M}$ подгрупп группы G свяжем предикат P на G, полагая $P(x, y) =$ И тогда и только тогда, когда в матрёшке $\mathcal{M}$ существует подгруппа, содержащая x и не содержащая y. Ясно, что P удовлетворяет следующим универсальным аксиомам (кванторы опущены):

1) $\neg P(x, x)$,
2) $P(x, y) \wedge P(y, z) \to P(x, z)$,
3) $P(x, z) \wedge \neg P(y, z) \to P(x, y)$,
4) $P(x, z) \wedge P(y, z) \to P(xy^{-1}, z)$,
5) $x \neq 1 \to P(1, x)$,
6) $P(x, y) \to P(y^{-1}xy, y)$.

Обозначим $A_y = \{x \mid x \in G, P(x, y) = \text{И}\}$, $y \neq 1$. Нетрудно проверить, что

$$A_y = \bigcup_{y \notin A \in \mathcal{M}} A, \qquad A = \bigcap_{y \notin A} A_y \qquad (A \in \mathcal{M}, A \neq G),$$

т. е. $A_y \notin \mathcal{M}$ и каждое $A \in \mathcal{M}$, $A \neq G$, представимо в виде пересечения подгрупп A_y.

Обратно, пусть на G задан предикат P со свойствами 1) — 6). Множества A_y составляют систему подгрупп, линейно упорядоченную по вложению. Если мы добавим к этой системе G, а также объединения и пересечения любых подсистем, то получится субнормальная матрёшка подгрупп в группе G. Из 1) — 3) легко следует, что указанные переходы от $\mathcal{M}$ к P и от P к $\mathcal{M}$ взаимно обратны, а потому осуществляют искомый перевод на язык ИП.

Основные понятия теории классов Куроша — Черникова после перевода на язык ИП будут выглядеть следующим образом:

7) разрешимость матрёшки: $x \neq 1 \wedge \neg P(x, y) \wedge \wedge \neg P(y, x) \to P([x, y], x)$,

8) нормальность матрёшки: $P(x, y) \to P(z^{-1}xz, y)$,

9) центральность матрёшки: $x \neq 1 \to P([x, y], x)$.

Охарактеризуем еще трехчленные матрёшки $1 \leqslant A \leqslant G$ на языке ИП. Очевидно, для этого к аксиомам 1) — 5) надо добавить аксиому

10) трехчленность матрёшки: $x \neq 1 \wedge P(x, y) \to \to \neg P(y, z)$.

Теперь ясно, что свойства RN, RI, Z записываются формулами

$$RN\colon (\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (7)),$$

$$RI\colon (\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge \wedge (4) \wedge (5) \wedge (7) \wedge (8)),$$

$$Z\colon (\exists P)(\forall x)(\forall y)(\forall z)((1) \wedge (2) \wedge (3) \wedge (4) \wedge (5) \wedge (9)),$$

где (1), (2), . . . — выражения из 1), 2), . . ., а свойства $\overline{RN}$, $\overline{RI}$, $\overline{Z}$, $\overline{N}$, говорящие об уплотняемости, записываются формулами

$$\overline{RN}\colon (\forall P)((P \text{ — субн.}) \to (\exists Q)((Q \text{ — разр. субн.}) \wedge \wedge (\forall u)(\forall v)(P(u, v) \to Q(u, v)))),$$

$$\overline{RI}\colon (\forall P)\ ((P \text{ — норм.}) \to (\exists Q)((Q \text{ — разр. норм.}) \wedge \wedge (\forall u)(\forall v)[(P(u, v) \to Q(u, v)))),$$

$$\overline{Z}\colon (\forall P)\ ((P \text{ — норм.}) \to (\exists Q)((Q \text{ — центр.}) \wedge \wedge (\forall u)(\forall v)(P(u, v) \to Q(u, v)))),$$

$$\overline{N}\colon (\forall P)((P \text{ — трехчл.}) \to (\exists Q)((Q \text{ — субн.}) \wedge \wedge (\forall u)(\forall v)(P(u, v) \to Q(u, v)))),$$

где сокращенные записи должны быть заменены очевидными комбинациями формул 1) — 10). Поскольку все семь свойств оказались квазиуниверсальными, остается сослаться на теорему 27.3.3 из Дополнения. Теорема доказана.

Для свойств RN^*, RI^*, ZA, ZD, N, не охваченных теоремой Мальцева, локальная теорема не справедлива,— см., в частности, пример 18.2.2.

Заметим, что формулы для RN, RI, Z предметно-универсальны, поэтому по теореме 27.3.1 из Дополнения эти свойства переносятся на подгруппы (что нетрудно доказать и непосредственно).

22.3.2. У п р а ж н е н и е. Свойства RN^*, RI^*, ZA, ZD, N, $\bar{N}$ тоже переносятся на подгруппы.

Глава 8

УСЛОВИЯ КОНЕЧНОСТИ

§ 23. Периодичность и локальная конечность

23.1. Совпадают ли эти понятия? Напомним, что группа называется *периодической*, если каждый ее элемент имеет конечный порядок. Группа называется *локально конечной*, если каждая ее конечно порожденная подгруппа конечна. Ясно, что всякая локально конечная группа является периодической. Верно ли обратное?— в этом состоит проблема Бернсайда, поставленная еще в начале века. Более точно, известны следующие ее варианты:

I. Общая проблема Бернсайда $\mathfrak{B}$: всякая ли периодическая группа локально конечна?

II. Ограниченная проблема Бернсайда $\mathfrak{B}(r, m)$: всякая ли группа данного периода m, т. е. с тождественным соотношением $x^m = 1$, и с данным числом порождающих элементов r конечна?

III. Ослабленная проблема Бернсайда $\mathfrak{B}'(r, m)$: конечно ли число к о н е ч н ы х групп данного периода m с данным числом порождающих элементов r?

Понятно, что из отрицательного решения проблемы $\mathfrak{B}(r, m)$ для каких-либо r, m следует отрицательное решение проблемы $\mathfrak{B}$, а из положительного решения $\mathfrak{B}(r, m)$ следует положительное решение $\mathfrak{B}'(r, m)$.

Состояние трех этих вопросов на сегодня таково:

I. Е. С. Голод (Изв. АН СССР: Сер. матем., 1964, 28, № 2, с. 273—276) и С. В. Алёшин (Матем. заметки, 1972, 11, № 3, с. 319—328) построили примеры бесконечных конечно порожденных периодических групп, что отрицательно решает общую проблему Бернсайда. Разумеется, решает ее — попутно — и недавний пример А. Ю. Ольшанского, о котором мы говорили в § 2 в связи с проблемой О. Ю. Шмидта.

II. П. С. Новиков и С. И. Адян (Изв. АН СССР: Сер. матем., 1968, 32, с. 212—244, с. 251—524, с. 709—731) доказали бесконечность свободной группы $B_r(m)$ в много-

образии групп с тождеством $x^m = 1$ и r свободными порождающими, где $r \geqslant 2$, m — нечетное число $\geqslant 4381$. Позднее эта граница была понижена до $m \geqslant 665$ — см. [2]. С другой стороны, известна конечность свободных бернсайдовых групп малых периодов: $B_r(2)$ (упражнение), $B_r(3)$ (Burnside, 1902), $B_r(4)$ (И. Н. Санов, 1940) и $B_r(6)$ (M. Hall, 1957). Конечна ли пропущенная в этом списке группа $B_r(5)$ — неизвестно.

III. А. И. Кострикин (Изв. АН СССР: Сер. матем., 1959, **23**, № 1, с. 3—34; см. также: Матем. сб., 1979, **110**, № 1, с. 3—12) положительно решил ослабленную проблему Бернсайда $\mathfrak{B}'(r, m)$ в случае, когда m — простое число.

Итак, общая проблема Бернсайда решена, однако до сих пор известно всего лишь несколько отдельных периодических не локально конечных групп или, лучше сказать, конструктивных типов таких групп. Как пойдет дело дальше — судить трудно, но сейчас эти примеры производят приблизительно такое же впечатление, как первые образцы лунного грунта. Каждый из них, несомненно, заслуживает самого пристального внимания, и мы посвятим этот параграф изложению замечательной конструкции С. В. Алёшина. (Пример Е. С. Голода был изложен выше — см. 18.3.2 и § 26 Дополнения,— а остальные из упомянутых конструкций, к сожалению, слишком громоздки для изложения их в учебнике.)

Пользуясь случаем, отметим, что для линейных групп — в отличие от общего случая — результаты по проблеме Бернсайда были получены еще в начале века и имеют положительный характер — см. [20], стр. 409.

Мы закончим эти предварительные замечания следующим важным свойством локально конечных групп (его аналог для периодических групп — легкое упражнение):

23.1.1. Т е о р е м а (О. Ю. Шмидт). *Расширение G локально конечной группы A посредством локально конечной группы G/A — само локально конечная группа.*

Д о к а з а т е л ь с т в о. Проверим, что каждое конечное множество M из G порождает конечную подгруппу. По условию фактор-группа $\mathrm{гр}(M, A)/A$ конечна. Увеличив, если нужно, множество M, будем считать, что оно замкнуто относительно взятия обратных элементов и содержит представители всех смежных классов $\mathrm{гр}(M, A)$

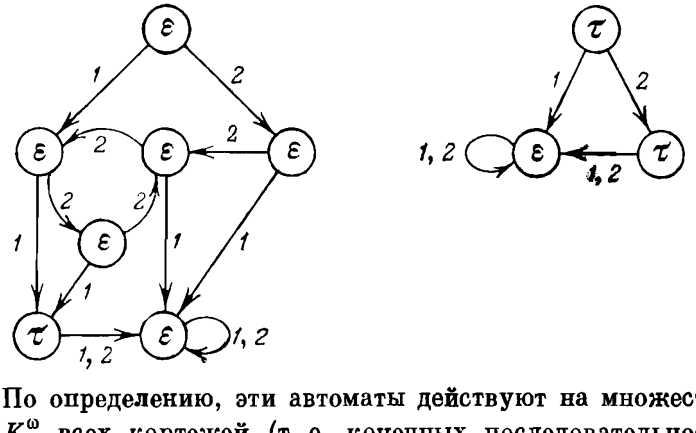
по A. Тогда для любых x, y из M выполняется равенство

$$xy = \overline{xy} \cdot a_{x,y}, \text{ где } \overline{xy} \in M, \ a_{x,y} \in A.$$

Отсюда следует, что любое произведение элементов из M можно записать как произведение некоторого элемента из M на произведение некоторых $a_{x,y}$. Так как всевозможные $a_{x,y}$ порождают конечную подгруппу, то всё доказано.

23.2. Бесконечная 2-порожденная 2-группа автоматных преобразований. В упомянутой выше работе С. В. Алёшина для каждого простого числа p построена бесконечная 2-порожденная финитно аппроксимируемая p-группа автоматных преобразований. Идея конструкции хорошо видна уже в простейшем случае, когда $p = 2$, которым мы и ограничимся.

Что такое автомат и как он работает? Не вдаваясь в общую теорию, ограничимся примерами следующих двух нужных нам автоматов a и b:



По определению, эти автоматы действуют на множестве K_2^ω всех кортежей (т. е. конечных последовательностей) цифр 1, 2. Автомат a имеет 7 состояний, изображенных на рисунке кружками, одно из которых — начальное — помечено буквой a. В кружках написаны подстановки множества $I = \{1, 2\}$: ε — тождественная, τ — транспозиция. Работает автомат a так: если дан кортеж $\gamma = i_1 i_2 \ldots i_m$, то a действует на его первую цифру i_1 подстановкой ε, соответствующей начальному состоянию, и переходит в новое состояние по стрелке i_1, затем действует на i_2 под-

становкой, соответствующей этому новому состоянию, а сам переходит из него по стрелке i_2, и т. д. Здесь удобно ввести следующее обозначение: если после переработки кортежа γ автомат a переходит в состояние, которому соответствует подстановка π, то будем писать

$$a/\gamma \sim \pi.$$

Например, пусть $\gamma = 121221$. Путешествуя по стрелкам автомата a (как в детских настольных играх), мы находим, что

$$\begin{aligned} a/1 &\sim \varepsilon, \\ a/12 &\sim \varepsilon, \\ a/121 &\sim \tau, \\ a/1212 &\sim \varepsilon, \\ a/12122 &\sim \varepsilon, \\ a/121221 &\sim \varepsilon, \end{aligned}$$

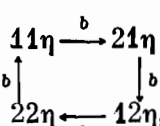
поэтому $\gamma a = 1^{\varepsilon}2^{\varepsilon}1^{\varepsilon}2^{\tau}2^{\varepsilon}1^{\varepsilon} = 121121$ и $a/\gamma \sim \varepsilon$.

Аналогично работает автомат b.

23.2.1. Упражнение. В любом кортеже автомат a меняет не более одной цифры, причем отрезок, предшествующий этой цифре, должен иметь вид $i2\ldots21$. Применив a еще раз, мы вернемся к исходному кортежу, каким бы он ни был, так что $a^2 = 1$ (мы будем отождествлять автоматы и определяемые ими преобразования множества кортежей K_2^{ω}). В частности, a — взаимно однозначное преобразование, обратное самому себе. Вот полный перечень случаев, когда автомат a переходит в (единственное) состояние с подстановкой τ: если дл. $\gamma \geqslant 3$, то $a/\gamma \sim \tau$ тогда и только тогда, когда

$$\gamma = \begin{cases} 12\ldots21 & \text{при дл. } \gamma \equiv 0 \pmod 3, \\ 22\ldots21 & \text{при дл. } \gamma \equiv 1 \pmod 3, \\ i2\ldots21 & \text{при дл. } \gamma \equiv 2 \pmod 3. \end{cases}$$

23.2.2. Упражнение. Автомат b действует совсем просто:



где η — произвольный кортеж. В частности, b меняет только первые две цифры кортежа, причем любую их пару можно переделать в любую другую пару, применив b несколько раз. Далее, $b^4 = 1$, так что b — тоже взаимно однозначное преобразование множества K_2^ω (с обратным преобразованием b^3).

23.2.3. Теорема (С. В. Алёшин). *Группа автоматных преобразований $G = \text{гр}(a, b)$ является бесконечной финитно аппроксимируемой 2-группой.*

Доказательство.; а) Группа G бесконечна. В самом деле, достаточно найти в ней такие элементы x_1, x_2, . . ., что

$$\underbrace{1\ldots1}_{k-1}2\eta \xrightarrow{x_k} \underbrace{1\ldots1}_{k}\eta$$

для всякого кортежа η, потому что взяв $y_k = x_1 \ldots x_k$, мы будем иметь

$$\underbrace{2\ldots2}_{k}2\ldots \xrightarrow{y_k} \underbrace{1\ldots1}_{k}2\ldots,$$

т. е. найдем в G бесконечно много различных элементов $y_1, y_2, \ldots$

Ясно, что можно взять $x_1 = b^3$, $x_2 = b^2$ (см. упражнение 23.2.2). Предположим теперь, что элементы $x_1, \ldots, x_{k-1}$, $k \geqslant 3$, уже построены, и построим x_k. Имеем

$$\underbrace{1\ldots1}_{k-1}2\eta \xrightarrow{x_{k-2}^{-1}} \underbrace{1\ldots1}_{k-3}1212\eta \xrightarrow{x_{k-3}^{-1}} \ldots \xrightarrow{x_1^{-1}} \underbrace{2\ldots2}_{k-2}12\eta. \qquad (1)$$

Из определения автомата a видно (см. также упражнение 23.2.1), что

$$\underbrace{12\ldots2}_{m}12\eta \xrightarrow{a} \underbrace{12\ldots2}_{m}11\eta \quad \text{при} \quad m \equiv 0,\ 1 \pmod 3,$$

$$\underbrace{22\ldots2}_{m}12\eta \xrightarrow{a} \underbrace{22\ldots2}_{m}11\eta \quad \text{при} \quad m \equiv 2 \pmod 3.$$

Следовательно, изменив, если необходимо, в последнем кортеже цепочки (1) первую цифру (с помощью подходящей степени преобразования b) и применив затем a и,

возможно, еще раз подходящую — обратную — степень b, получим

$$\underbrace{2\ldots2}_{k-2}11\eta.$$

Применив, наконец, $x_1 \ldots x_{k-2}$, получим требуемый кортеж $\underbrace{1\ldots1}_{k}\eta$. Таким образом, можно взять

$$x_k = x_{k-2}^{-1} \ldots x_1^{-1} b^{-m} a b^m x_1 \ldots x_{k-2}$$

при подходящем $m = 0, 1$.

б) Группа G аппроксимируется конечными 2-группами. В самом деле, пусть I^n — множество кортежей длины n в алфавите $I = \{1, 2\}$, G_n — группа подстановок множества I^n, индуцируемых (путем сужения на I^n) преобразованиями из G, $n = 1, 2, \ldots$. Ясно, что ядра всех гомоморфизмов-сужений $G \to G_n$ пересекаются по единице, поэтому остается заметить, что каждая G_n является 2-группой. Для этого мы покажем индукцией по n, что G_n имеет период 2^n.

Пусть сначала $n = 1$. Всякий элемент $g \in G$ имеет вид $g = b^{\beta_1} a b^{\beta_2} a \ldots b^{\beta_s}$ и на произвольную цифру $i \in \{1, 2\}$ действует как подстановка $\tau^{\beta_1+\ldots+\beta_s}$. Понятно, что $ig^2 = i$. Пусть уже доказано, что $\gamma g^{2^{n-1}} = \gamma$ для всякого $\gamma \in I^{n-1}$, и пусть $j \in \{1, 2\}$. Очевидно, $(\gamma j)g^{2^{n-1}} = \gamma j^{\tau^m}$, где $m = 0$ или 1. Действуя еще раз преобразованием $g^{2^{n-1}}$, получим $(\gamma j)g^{2^n} = \gamma j$.

в) Осталось последнее — но и самое сложное: доказать, что G является 2-группой. Ввиду б) никакого кручения, кроме 2-кручения, в группе G быть не может, поэтому достаточно доказать только, что она периодическая. Нам понадобится несколько вспомогательных понятий, и в этом пункте мы объясним одно из них — гибкость кортежа относительно автоматного преобразования.

Пусть γ — кортеж в алфавите $\{1, 2\}$, g — элемент группы G, взятый в фиксированной записи через порождающие

$$g = z_1 \ldots z_s, \quad \text{где каждое } z_k = a \text{ или } b.$$

Пусть, далее, d — наименьшее натуральное число с условием $\gamma g^d = \gamma$. Последовательность $\Gamma_g(\gamma)$ всех промежу-

точных результатов применения слова $(z_1 \ldots z_s)^d$ к кортежу γ запишем в таблицу:

$$\begin{array}{c|c|c|c|c} & z_1 & & z_2 \; z_{s-1} & \\ \gamma = \gamma_1^1 & \gamma_2^1 & & \gamma_s^1 & \\ \gamma_1^2 & \gamma_2 & \cdots & \gamma_s^2 & \\ \vdots & \vdots & & \vdots & \\ \gamma_1^d & \gamma_2^d & & \gamma_s^d & \end{array}$$

Таким образом,

$$\gamma_{k+1}^l = \gamma_k^l z_k \quad \text{при} \quad 1 \leqslant k \leqslant s-1, \; 1 \leqslant l \leqslant d,$$
$$\gamma_1^{l+1} = \gamma_s^l z_s \quad \text{при} \quad 1 \leqslant l \leqslant d-1,$$

а сама последовательность $\Gamma_g(\gamma)$ получается чтением этой таблицы строка за строкой. Пусть, далее, $\widetilde{\Gamma}_g(\gamma)$ — подпоследовательность последовательности $\Gamma_g(\gamma)$, составленная из всех γ_k^l вида $i2 \ldots 2j$, к которым применяется $z_k = a$ (напомним, что только после таких кортежей автомат a может изменить следующую цифру, см. упражнение 23.2.1). Если Γ — конечная последовательность, то пусть Γ° обозначает круговую последовательность, получаемую из Γ записыванием последнего члена перед первым. Пусть наконец, $\mathrm{sgm}_g(\gamma)$ (соответственно $\mathrm{sgm}_g^\circ(\gamma)$) — число связных «2-отрезков» вида

$$i'2 \ldots 22, \quad \ldots, \quad i''2 \ldots 22,$$

чередующихся в последовательности $\widetilde{\Gamma}_g(\gamma)$ (соответственно в круговой последовательности $\widetilde{\Gamma}_g^\circ(\gamma)$) со связными «1-отрезками» вида

$$2 \ldots 21, \quad \ldots, \quad i''2 \ldots 21$$

(понятно, что если имеются и те и другие отрезки, то в $\widetilde{\Gamma}_g^\circ(\gamma)$ их количества одинаковы, а в $\widetilde{\Gamma}_g(\gamma)$ отличаются самое большее на единицу). Мы назовем число

$$\mathrm{fl}_g(\gamma) = \left[\frac{1}{2}\,\mathrm{sgm}_g^\circ(\gamma)\right]$$

гибкостью[1]) кортежа γ относительно преобразования g (точнее, относительно фиксированной записи элемента g через порождающие a, b). Например, если «хвостовые»

[1]) fl — от flexibility.

цифры кортежей из $\widetilde{\Gamma}_g(\gamma)$ имеют вид 2122122112, то $\mathrm{sgm}_g(\gamma) = 4$, $\mathrm{sgm}^{\circ}_g(\gamma) = 3$, $\mathrm{fl}_g(\gamma) = 1$. Говоря неформально, гибкость кортежа отражает число виляний хвостом в последовательности $\widetilde{\Gamma}^{\bullet}_g(\gamma)$.

23.2.4. Упражнение. Если $\gamma g = \delta$, то $\mathrm{sgm}^{\circ}_g(\gamma) = \mathrm{sgm}^{\circ}_g(\delta)$ и $\mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\delta)$. Заметим, что именно ради этого свойства мы перешли от sgm к sgm°. Что же касается деления пополам и перехода к целой части, то они были сделаны исключительно ради того, чтобы выполнялось утверждение следующего пункта.

г) Покажем, что с увеличением длины кортежа его гибкость, вообще говоря, уменьшается. Говоря точно, для всякого $g \in G$, всякого кортежа γ длины $\geqslant 3$ и всякой цифры $j \in \{1, 2\}$ выполняется неравенство

$$\mathrm{fl}_g(\gamma j) \leqslant \mathrm{fl}_g(\gamma). \tag{2}$$

Более того, если $\mathrm{fl}_g(\gamma) > 0$, d — наименьшее число с условием $\gamma g^d = \gamma$ и автомат g^d после переработки кортежа γ переходит в состояние, которому соответствует тождественная подстановка, т. е. $g^d/\gamma \sim \varepsilon$, то

$$\mathrm{fl}_g(\gamma j) < \mathrm{fl}_g(\gamma). \tag{3}$$

Заметим сначала, что если $i'2\ldots2$, $i''2\ldots2$ — два соседних кортежа в последовательности $\widetilde{\Gamma}^{\circ}_g(\gamma)$, то в $\widetilde{\Gamma}^{\bullet}_g(\gamma j)$ к ним будет приписана одна и та же цифра. В самом деле, если бы дописанные кортежи имели вид

$$i'2\ldots2j', \quad i''2\ldots2j'' \tag{4}$$

с различными j', j'', то в последовательности $\Gamma^{\bullet}_g(\gamma j)$ (без тильды) первое изменение цифры j' в процессе переработки кортежа $i'2\ldots2j'$ имело бы вид

$$i'''2\ldots21j' \xrightarrow{a} i'''2\ldots21j''$$

(учесть механизм действия автоматов a и b, см. упражнения 23.2.1 и 23.2.2), а потому в $\widetilde{\Gamma}^{\bullet}_g(\gamma)$ между кортежами (4) стоял бы кортеж $i'''2\ldots21$, что неверно. Таким образом, пока в последовательности $\widetilde{\Gamma}^{\circ}_g(\gamma)$ хвостовая цифра 2 не меняется, в последовательности $\widetilde{\Gamma}^{\circ}_g(\gamma j)$ у соответствую-

щих членов новая — дописанная — хвостовая цифра тоже не меняется.

Заметив это, рассмотрим вначале случай, когда $g^d/\gamma \sim \varepsilon$. Тогда $(\gamma j)g^d = \gamma j$, а потому $\widetilde{\Gamma}_g(\gamma j)$ имеет ту же самую длину, что и последовательность $\widetilde{\Gamma}_g(\gamma)$, и получается из нее приписыванием к членам вида $i2\ldots2$ цифры 1 или 2. Из прерыдущего замечания и простых комбинаторных соображений следует, что если $\operatorname{sgm}_g^\circ(\gamma) \geqslant 2$, то $\operatorname{sgm}_g^\circ(\gamma j) \leqslant \left[\frac{1}{2}\operatorname{sgm}_g^\circ(\gamma)\right]$. Так как при $m = 1, 2, \ldots$ выполняется очевидное неравенство $\left[\frac{m}{2}\right] < m$, то при $\operatorname{fl}_g(\gamma) > 0$ выполняется неравенство (3).

Пусть теперь $g^d/\gamma \sim \tau$. Тогда $(\gamma j)g^d = \gamma j^\tau$, $(\gamma j)g^{2d} = \gamma j$, т. е. $\widetilde{\Gamma}_g(\gamma j)$ вдвое длиннее последовательности $\widetilde{\Gamma}_g(\gamma)$. Так как связным 1-отрезкам в первой половине последовательности $\widetilde{\Gamma}_g(\gamma j)$ соответствуют связные 2-отрезки и наоборот, то для вычисления гибкости кортежа γ относительно g получаем следующую таблицу:

тип виляний хвостом в половинах $\widetilde{\Gamma}_g(\gamma j)$		m—общее число отрезков в каждой половине	$\varepsilon\operatorname{sgm}_g^\circ(\gamma j)$
в первой	во второй		
$1 \sim 1$	$2 \sim 2$	нечетное	m
$1 \sim 2$	$2 \sim 1$	четное	$m-1$
$2 \sim 1$	$1 \sim 2$	четное	$m-1$
$2 \sim 2$	$1 \sim 1$	нечетное	m

Мы видим, что во всех случаях

$$\operatorname{fl}_g(\gamma j) = \left[\frac{1}{2}\operatorname{sgm}_g^\circ(\gamma j)\right] = \left[\frac{m-1}{2}\right].$$

Так как

$$m \leqslant \operatorname{sgm}_g(\gamma) \leqslant \operatorname{sgm}_g^\circ(\gamma) + 1,$$

то во всех случаях выполняется неравенство (2).

д) Для всякого $g \in G$ существует такое натуральное число n_g, что гибкость любого кортежа длины n_g относительно g не изменится, как бы этот кортеж ни

дописывать, т. е.

$$\mathrm{fl}_g(\gamma\eta) = \mathrm{fl}_g(\gamma)$$

для всякого γ длины n_g и всякого кортежа η.

В самом деле, множество I^n всех кортежей длины n в алфавите $I = \{1, 2\}$ распадается на орбиты относительно циклической группы (g); назовем их *n-орбитами*. Ясно, что начальные отрезки длины $n' < n$ кортежей какой-нибудь n-орбиты N сами лежат в одной орбите и, более того, составляют в точности некоторую n'-орбиту N'; мы будем говорить, что n-орбита N *продолжает* n'-орбиту N'. Ввиду упражнения 23.2.4 каждой n-орбите N можно приписать *гибкость* $\mathrm{fl}(N) = \mathrm{fl}_g(\gamma)$, $\gamma \in N$.

Пусть множество I^3 распадается на 3-орбиты $I^3_1, \ldots, I^3_r$ и $\mathrm{fl}(I^3_k) = f^3_k$. Пусть $\gamma_1 \in I^3_1$, d_1 — наименьшее число с условием $\gamma_1 g^{d_1} = \gamma_1$. Если $g^{d_1}/\gamma_1 \sim \varepsilon$, то

$$(\gamma_1 j)\, g^{d_1} = \gamma_1 j, \quad \mathrm{fl}_g(\gamma_1 j) < \mathrm{fl}_g(\gamma_1)$$

для любого $j \in \{1, 2\}$ (см. г)), поэтому в множестве I^4 будут две 4-орбиты I^4_1, I^4_2, продолжающих I^3_1 и имеющих гибкость $< \mathrm{fl}(I^3_1)$. Если же $g^{d_1}/\gamma_1 \sim \tau$, то в I^4 будет лишь одна 4-орбита I^4_1, продолжающая I^3_1, причем $\mathrm{fl}(I^4_1) \leqslant \mathrm{fl}(I^3_1)$. Продолжая этот процесс индуктивно, мы видим, что для всякого $n = 4, 5, \ldots$ либо существует единственная n-орбита, продолжающая данную $(n-1)$-орбиту, либо существуют две такие n-орбиты, но тогда их гибкость строго меньше, чем у данной $(n-1)$-орбиты. Ввиду конечности чисел $f^3_1, \ldots, f^3_r$ найдется такое n_g, что каждая $(n_g - 1)$-орбита покрывается точно одной n_g-орбитой и гибкость уже не убывает. Отсюда и следует наше утверждение.

Проведенное рассуждение можно пояснить рисунком — см. стр. 224, где орбиты обозначены точками, а их продолжение — отрезками, идущими вниз.

В дальнейшем мы увидим, что стабилизация гибкости, описанная в д), происходит обязательно на нуле, но для этого нам потребуется еще одно вспомогательное понятие — понятие типа последовательности $\tilde{\Gamma}_g(\gamma)$.

е) Пусть снова $\gamma g^d = \gamma$, дл. $\gamma \geqslant 3$. Какой должна быть подстановка g^d/γ? Оказывается, что при некоторых условиях на дл. γ можно дать вполне определенный ответ.

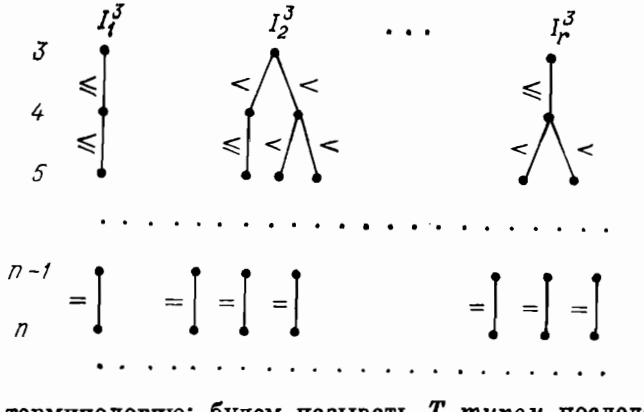
Именно, пусть $T = \{1\}, \{2\}$ или $\{1, 2\}$. Ввиду формулы из упражнения 23.2.1 можно указать сколь угодно большое число n_T, такое, что для всякого кортежа δ длины n_T:

$$a/\delta \sim \tau \Leftrightarrow \delta = i2\ldots.21, \quad i \in T.$$

Значит, если дл. $\gamma = n_T$ и N_T — число всех кортежей вида $i2\ldots.21$, $i \in T$, в последовательности $\widetilde{\Gamma}_g(\gamma)$, то

$$g^d/\gamma \sim \tau^{N_T}.$$

В частности, $g^d/\gamma \sim \varepsilon$ тогда и только тогда, когда N_T четно. Ввиду важности этой ситуации введем специаль-



ную терминологию: будем называть T *типом* последовательности $\widetilde{\Gamma}_g(\gamma)$, если число N_T четно.

23.2.5. У п р а ж н е н и е. При любых g, γ последовательность $\widetilde{\Gamma}_g(\gamma)$ обладает хотя бы одним типом (а, возможно, и несколькими). [Учесть, что хотя бы одно из чисел N_1, N_2, $N_1 + N_2$ должно быть четным.]

ж) Покажем, что если бы гибкость при дописывании кортежей относительно какого-то g стабилизировалась не на нуле, то не позднее чем через шаг после стабилизации гибкости наступала бы и стабилизация типов. Более точно, если

$$0 < \mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\gamma j_1) = \mathrm{fl}_g(\gamma j_1 j_2)$$

для некоторого кортежа γ и цифр j_1, j_2, то типы последовательностей $\widetilde{\Gamma}_g(\gamma j_1)$ и $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ одинаковы.

В самом деле, пусть d — наименьшее число с условием $\gamma g^d = \gamma$. В силу первого равенства и замечания г) $g^d/\gamma \sim \tau$, поэтому в последовательности $\widetilde{\Gamma}_g(\gamma j_1)$ вместе с каждым кортежем вида $\delta 1$ должен быть кортеж $\delta 2$ и наоборот (см. третий абзац пункта г)). По той же причине в $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ вместе со всяким кортежем $\delta 1$ должен быть $\delta 2$ и наоборот. Следовательно, множество кортежей из $\widetilde{\Gamma}_g(\gamma j_1 j_2)$ с хвостовой цифрой 1 можно получить из таких же кортежей в $\widetilde{\Gamma}_g(\gamma j_1)$ следующим приемом: меняем хвостовую цифру 1 на 2 и приписываем новую хвостовую цифру 1. Теперь наше утверждение прямо следует из определения типа (см. е)).

з) Покажем, что стабилизация гибкости, описанная в д), на самом деле всегда происходит на нуле, т. е. $\mathrm{fl}_g(\gamma) = 0$ для всех γ длины $\geqslant n_g$.

Действительно, ввиду д)

$$\mathrm{fl}_g(\gamma) = \mathrm{fl}_g(\gamma\eta)$$

для всех γ длины n_g и всех η. Допустим, что $\mathrm{fl}_g(\gamma) > 0$. Ввиду ж) типы всех последовательностей

$$\widetilde{\Gamma}_g(\gamma j_1 \ldots j_k), \quad k = 1, 2, \ldots,$$

при произвольных $j_1, j_2, \ldots$ из $\{1, 2\}$ одинаковы; пусть T — один из этих типов. Согласно е) найдется такое число $n'_g > n_g$, что для всякого кортежа δ длины n'_g

$$a/\delta \sim \tau \Leftrightarrow \delta = i2\ldots21, \quad i \in T.$$

Положим $k = n'_g - n_g$, тогда дл. $\gamma j_1 \ldots j_k = n'_g$. Пусть d таково, что $(\gamma j_1 \ldots j_k) g^d = \gamma j_1 \ldots j_k$. Так как число N_T всех кортежей вида $i2\ldots21$, $i \in T$, в последовательности $\widetilde{\Gamma}_g(\gamma j_1 \ldots j_k)$ четно (по определению типа), то $g^d/\gamma j_1 \ldots j_k \sim \varepsilon$ (см. е)). Но тогда ввиду г) должно выполняться строгое неравенство

$$\mathrm{fl}_g(\gamma j_1 \ldots j_{k+1}) < \mathrm{fl}_g(\gamma j_1 \ldots j_k),$$

что явно противоречит условию.

и) Докажем, наконец, что группа G периодическая. Более точно, если $g \in G$, то $g^{2^{n_g+2}} = 1$, где $n_g \geqslant 3$ — число, определенное в д) (см. также предыдущий пункт). Прежде всего, мы уже отмечали (см. б)), что если $d = 2^{n_g}$, то $\gamma g^d = \gamma$ для любого кортежа γ длины n_g. Остается

доказать, что

$$(\gamma\eta)\, g^{4d} = \gamma\eta \text{ для любого } \eta.$$

Так как $\mathrm{fl}_g(\gamma) = 0$, то возможны такие четыре случая:

и.1) Последовательность $\widetilde{\Gamma}_g^\circ(\gamma)$ пустая. Тогда, в частности, в ней нет кортежей вида $i2\ldots.21$. Так как автомат a меняет только цифру, идущую за таким кортежем, а b вообще не меняет цифр, начиная с третьего места, то $(\gamma j)\, g^d = \gamma j$ для любого $j \in \{1, 2\}$. Так как в $\widetilde{\Gamma}_g^\circ(\gamma)$ нет и кортежей вида $i2\ldots.2$, то последовательность $\widetilde{\Gamma}_g^\circ(\gamma j)$ тоже пустая. Следовательно, рассуждение можно повторить, и $(\gamma\eta)\, g^d = \gamma\eta$ для любого кортежа η.

и.2) Последовательность $\widetilde{\Gamma}_g^\circ(\gamma)$ целиком состоит из кортежей вида $i2\ldots21$. Пусть $j \in \{1, 2\}$. Так как в $\widetilde{\Gamma}_g^\circ(\gamma j)$ могут войти лишь кортежи, начала которых являются элементами из $\widetilde{\Gamma}_g(\gamma)$, то последовательность $\widetilde{\Gamma}_g^\circ(\gamma j)$ пуста. Так как $\gamma g^d = \gamma$, то $(\gamma j)\, g^{2d} = \gamma j$, и мы приходим к случаю и.1) для кортежа γj.

и.3) Последовательность $\widetilde{\Gamma}_g^\circ(\gamma)$ целиком состоит из кортежей вида $i2\ldots.2$. Отсюда, как и в и.1), следует, что $(\gamma j)\, g^d = \gamma j$ для всякой цифры $j \in \{1, 2\}$. Более того, последовательность $\widetilde{\Gamma}_g^\circ(\gamma j)$ получается приписыванием к $\widetilde{\Gamma}_g^\circ(\gamma)$ одной и той же цифры j. Если $j = 1$, то мы приходим к случаю и.2) для кортежа γj, и всё заканчивается. Если же $j = 2$, то мы возвращаемся к рассматриваемому случаю и.3), но уже для γj. Снова будем иметь:

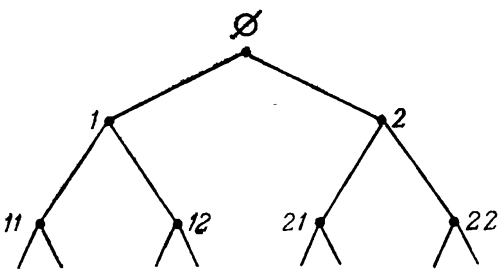
$$(\gamma 21\eta)\, g^{2d} = \gamma 21\eta, \quad (\gamma 22)\, g^d = \gamma 22$$

и т. д.

и.4) Последовательность $\widetilde{\Gamma}_g^\circ(\gamma)$ состоит из одного 1-отрезка и одного 2-отрезка. Тогда при любом $j \in \{1, 2\}$ последовательность $\widetilde{\Gamma}_g^\circ(\gamma j)$ подпадает под и.2) или и.3). Так как $(\gamma j)\, g^{2d} = \gamma j$, то $(\gamma j\eta)\, g^{4d} = \gamma j\eta$ для всякого кортежа η. Теорема доказана.

23.3. Другое доказательство. Определим на множестве K_2^ω всех кортежей в алфавите $\{1, 2\}$ частичное упорядочение $\leqslant$, полагая $\gamma \leqslant \delta$, если γ — начальный отрезок кортежа δ. Изображая кортежи одной длины точками на одной горизонтали, кортежи большей длины — точками на более низкой горизонтали, и соединяя γ с δ отрезком,

если $\gamma \leqslant \delta$, получим следующее **стандартное** представление множества K_2^ω в виде дерева:



Понятно, что автоматные преобразования сохраняют отношение $\leqslant$, поэтому группа Алёшина $G = \text{гр}\,(a, b)$ естественным образом вкладывается в группу $\text{Aut}\,K_2^\omega$ автоморфизмов дерева K_2^ω.

23.3.1. Упражнение. Пусть p — простое число, K_p^n — множество кортежей длины $\leqslant n$ в алфавите $\{1, 2, \ldots, p\}$ с определенным выше частичным упорядочением (т. е., как говорят, дерево *кратности* p и *высоты* n). Тогда

$$\text{Aut}\,K_p^n \simeq \underbrace{\mathbb{Z}_p \wr (\ldots \wr (\mathbb{Z}_p \wr \mathbb{Z}_p)\ldots)}_{n \text{ раз}}$$

Если $K_p^\omega = \bigcup_{n=1}^{\infty} K_p^n$ (дерево всех кортежей), то $\text{Aut}\,K_p^\omega$ — объединение последовательности групп $G_p^n = \text{Aut}\,K_p^n$ с естественными вложениями $G_p^n \to G_p^{n+1} = \mathbb{Z}_p \wr G_p^n$, что позволяет рассматривать группы автоматных преобразований как подгруппы этого объединения G_p^ω. Изложенные на таком языке конструкции, параллельные конструкции С. В. Алёшина, включая доказательство, можно найти в публикациях В. И. Сущанского (см., например, ДАН СССР, 1979, **247**, № 3, с. 557—561).

Как действует автомат a на дереве K_2^ω? Вспомним, что если дл. $\gamma \geqslant 3$, то $a/\gamma \sim \tau$ тогда и только тогда, когда

$$\gamma = 12\ldots.21 \quad \text{и} \quad \text{дл. } \gamma \equiv 0 \text{ или } 2 \pmod 3$$

или

$$\gamma = 22\ldots.21 \quad \text{и} \quad \text{дл. } \gamma \equiv 1 \text{ или } 2 \pmod 3$$

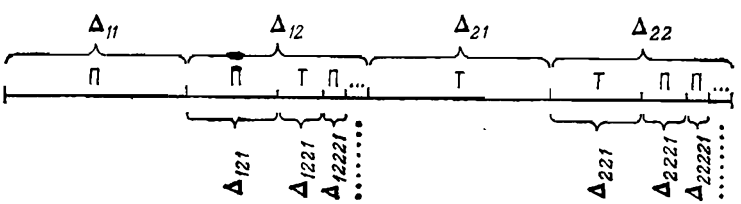
(см. упражнение 23.2.1). Значит, на поддеревьях $[\gamma]$ с «корнями» γ указанного вида автомат a совершает преобразование

$$\text{П: } \gamma 1\eta \leftrightarrow \gamma 2\eta$$

(*перестановку половин*), а на всех остальных поддеревьях $[\delta]$ — тождественное преобразование

$$\text{Т: } \delta\eta \leftrightarrow \delta\eta.$$

Перейдем еще к одной естественной интерпретации множества K_2^ω: пусть Δ — отрезок прямой линии, Δ_1, Δ_2 — его половины, Δ_{11}, Δ_{12}, Δ_{21}, Δ_{22} — их половины и т. д., тогда кортеж γ будем изображать отрезком Δ_γ. Пусть теперь П обозначает перестановку половинок (левая сдвигается вправо, правая — влево), а Т — тождественное преобразование отрезка. Легко сообразить, что на этом языке автомату a соответствует такое преобразование множества отрезков Δ_γ:



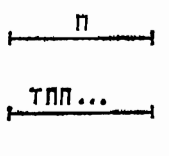
Более точно, на первой четверти Δ_{11} отрезка Δ преобразование a действует как П, а на второй четверти Δ_{12} так: делим Δ_{12} пополам, вторую половину — снова пополам, ее вторую половину — снова пополам и т. д., после чего на полученных отрезках расставляем преобразования ПТПППТП... На третьей четверти Δ_{21} преобразование a действует как Т, а четвертую четверть Δ_{22} снова разбиваем как вторую и на полученных отрезках расставляем преобразования ТППТППП...

Пусть G_0 — подгруппа группы G, состоящая из элементов, допускающих запись через порождающие a, b с нулевой суммой показателей при b. Ясно, что $|G: G_0| = 4$ (представители в смежных классах — 1, b, b^2, b^3) и

$$G_0 = \text{гр}\,(a,\quad b^{-1}ab,\quad b^{-2}ab^2,\quad b^{-3}ab^3).$$

23.3.2. Упражнение. Проверить, что порождающие элементы группы G_0 действуют на четвертях отрезка Δ следующим образом:

Пусть теперь Γ — какой-нибудь другой отрезок прямой линии, t, u, v — преобразования множества его 2-ичных долей, определяемые рисунками:



(для u, v имеется в виду описанное выше разбиение отрезка по правилу «вторая половина — пополам»). Пусть

$$H = \text{гр}\,(t,\ u,\ v).$$

Ясно, что G_0 — подпрямое произведение четырех экземпляров группы H (см. упражнение 23.3.2), а потому группа G тогда и только тогда будет бесконечной 2-группой, когда такова H. Таким образом, мы получим новое доказательство теоремы С. В. Алёшина 23.2.3 (впрочем, без легко доказываемого там свойства финитной аппроксимируемости), если будет доказана следующая

23.3.3. Теорема (Р. И. Григорчук). *Группа H — бесконечная 2-группа.*

Замечательно то, что попутно мы получим еще один экземпляр периодической, но не локально конечной группы, встроенный в группу Алёшина как секция (не

правда ли, переход от G к H напоминает выламывание адамова ребра?).

Доказательство. Очевидно, $uv = w$, где w определяется рисунком

Непосредственно проверяется, что

$$t^2 = u^2 = v^2 = w^2 = 1,$$
$$uv = vu = w, \quad uw = wu = v, \quad vw = wv = u,$$

поэтому каждый элемент из H имеет вид

$$*t*t*. \ . \ .*t*,$$

где звездочки — элементы вида u, v, w (на концах могут отсутствовать). Пусть H_0 — подгруппа группы H, состоящая из элементов, допускающих запись с четным числом множителей t. Очевидно, $|H : H_0| = 2$,

$$H_0 = \text{гр}\,(tut,\ tvt,\ twt,\ u,\ v,\ w)$$

и H_0 отображает каждую из двух половин Γ_1, Γ_2 отрезка Γ на себя. Пусть φ_i — сужение H_0 на Γ_i. Легко проверить, что гомоморфизмы φ_1, φ_2 действуют на порождающие элементы группы H_0 следующим образом:

x	tut	tvt	twt	u	v	w
x^{φ_1}	$\widetilde{w}$	$\widetilde{u}$	$\widetilde{v}$	1	$\tilde{t}$	$\tilde{t}$
x^{φ_2}	1	$\tilde{t}$	$\tilde{t}$	$\widetilde{w}$	$\widetilde{u}$	$\widetilde{v}$

(5)

(тильда поставлена, чтобы подчеркнуть, что соответствующее преобразование определено уже не на Γ). Сейчас для нас важно то, что под тильдой появляются в с е элементы t, u, v, w, поэтому

$$H_0^{\varphi_1} \simeq H_0^{\varphi_2} \simeq H.$$

Так как $x \mapsto x^{\varphi_1} \times x^{\varphi_2}$ — вложение группы H_0, то группа H оказалась гомоморфным образом своей собственной подгруппы H_0. Значит, H бесконечна!

Покажем теперь, что всякий ее элемент имеет порядок вида 2^m. Для порождающих t, u, v, w это очевидно, поэтому применим индукцию по k = дл. h. Пусть уже доказано, что элементы длины, меньшей k, имеют порядки вида 2^m. Можно считать, что $k \geqslant 2$ и h имеет специальный вид

$$h = t*t*\ldots t*, \tag{6}$$

где звездочки снова обозначают u, v, w (иначе мы сопрягли бы h элементом t или $*$).

Случай 1: $h \in H_0$ и, значит, произведение (6) распадается на четверки $t*t*$. Из таблицы (5) явствует, что под действием φ_1 и φ_2 каждая такая четверка переходит в $\tilde{*}\tilde{t}$, $\tilde{t}\tilde{*}$ или $\tilde{*}$, так что

$$\text{дл. } h^{\varphi_i} \leqslant \frac{k}{2} < k.$$

По индуктивному предположению h^{φ_1}, h^{φ_2} — 2-элементы, поэтому и h — 2-элемент.

Случай 2: $h \notin H_0$ и в записи (6) есть хотя бы один множитель u. Применив, если необходимо, подходящее сопряжение, можно считать, что u — именно первая звездочка. Так как $|H : H_0| = 2$, то $h^2 \in H_0$, причем h^2 начинается с четверки $tut*$ и имеет в середине четверку $t*tu$. Из таблицы (5) видно, что $t*tu$ под действием φ_1 переходит в $\tilde{*}$, а $tut*$ под действием φ_2 переходит в $\tilde{*}$. Следовательно,

$$\text{дл. } (h^2)^{\varphi_1} < k, \quad \text{дл. } (h^2)^{\varphi_2} < k,$$

и остается сослаться на индуктивное предположение.

Случай 3: $h \notin H_0$ и в записи (6) нет множителей u, но есть хотя бы один множитель v. Применив подходящее сопряжение, можно считать, что v — именно первая звездочка. Снова $h^2 \in H_0$, но теперь h^2 начинается четверкой $tvt*$ и имеет в середине четверку $t*tv$. Из таблицы (5) видно, что $tvt*$ под действием φ_1 переходит в $\tilde{u}\tilde{t}$, а $t*tv$ под действием φ_2 переходит в $\tilde{t}\tilde{u}$, поэтому оба слова $(h^2)^{\varphi_i}$ имеют в своей записи множитель u. Так как

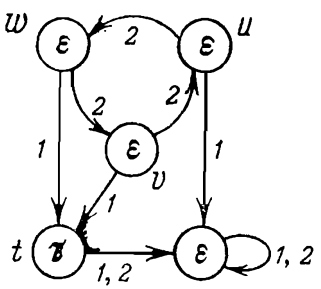
$$\text{дл. } (h^2)^{\varphi_1} \leqslant k, \quad \text{дл. } (h^2)^{\varphi_2} \leqslant k, \tag{7}$$

то мы приходим к уже рассмотренному случаю 2.

Случай 4: $h \notin H_0$ и в записи (6) нет ни u, ни v. Тогда $h^2 \in H_0$ и h^2 начинается с четверки $twtw$. Из таблицы (5

видно, что под действием φ_1 эта четверка переходит в $\tilde{v}\tilde{t}$, а под действием φ_2 — в $\tilde{t}\tilde{v}$, так что оба слова $(h^2)^{\varphi_i}$ имеют в своей записи множитель v. Так как снова выполнено (7), то мы приходим к уже рассмотренному случаю 3. Теорема доказана.

23.3.4. Упражнение. Если трактовать порождающие t, u, v, w группы H как преобразования множества K_2^ω кортежей в алфавите $\{1, 2\}$, то их можно задать следующими автоматами:



Здесь на одном рисунке изображены все четыре автомата, так как они отличаются друг от друга лишь начальными состояниями (помеченными соответствующей буквой). Взглянув теперь на автомат Алёшина a, вы можете почувствовать операцию выламывания ребра почти физически.

§ 24. Условия минимальности и максимальности

24.1. Определения и примеры. Говорят, что группа удовлетворяет *условию минимальности* (*для подгрупп*) или, короче, *условию* min, если всякий убывающий ряд ее подгрупп $H_1 \geqslant H_2 \geqslant \ldots$ обрывается, т. е. $H_n = H_{n+1} = \ldots$ при некотором n. Говорят, что группа удовлетворяет *условию максимальности* (*для подгрупп*) или, короче, *условию* max, если всякий возрастающий ряд ее подгрупп $H_1 \leqslant H_2 \leqslant \ldots$ обрывается, т. е. $H_n = H_{n+1} = \ldots$ при некотором n.

Конечно, всякая группа с условием min должна быть периодической, поскольку бесконечная циклическая группа не удовлетворяет этому условию.

24.1.1. Упражнение. Условие max равносильно условию, что все подгруппы рассматриваемой группы конечно порождены.

24.1.2. Упражнение. Условия min и max сохраняются при переходе к подгруппам, гомоморфным образам и расширениям.

Учитывая это упражнение и очевидное замечание, что квазициклическая группа $\mathbb{C}_{p^\infty}$ удовлетворяет условию min (см. 2.4.10), а бесконечная циклическая группа $\mathbb{Z}$ — условию max, мы получаем следующий основной

24.1.3. Пример. Назовем *черниковской группой* расширение прямого произведения конечного числа квазициклических групп (вообще говоря, по различным простым числам) при помощи конечной группы (под произведением нуля множителей здесь понимается единичная группа). Всякая черниковская группа удовлетворяет условию min. Всякая почти полициклическая группа удовлетворяет условию max.

Может показаться удивительным, но до самого последнего времени не было известно, исчерпываются ли этим каноническим примером вообще все группы с условием min (проблема Черникова) и группы с условием max (проблема Бэра), хотя интерес к этим двум вопросам неуклонно возрастал в течение десятилетий по мере их положительного решения всё в новых и новых классах групп. Окончательный ответ на оба вопроса оказался, однако, отрицательным — это показывает пример А. Ю. Ольшанского, о котором говорилось в § 2. Открытие подобных примеров наложило глянец полной завершенности на полученные ранее положительные результаты, два из которых заслуживают особого упоминания— черниковость локально разрешимых групп с условием минимальности для абелевых подгрупп (Черников С. Н.— Матем. сб., 1951, 28, № 1, с. 119—129) и черниковость локально конечных групп с тем же условием (Шунков В. П.— Алгебра и логика, 1970, 9, § 5, с. 579—615). Первый из этих результатов будет доказан в нашей книге (см. 24.3.4), а доказательство второго, опирающееся на узкоспециальные сведения из теории конечных простых групп, остается, к сожалению, слишком громоздким для изложения его в учебнике.

Разрешимые группы с условием min полностью описывает следующая

24.1.4. Теорема (С. Н. Черников). *Всякая разрешимая группа G с условием минимальности является черниковской* (или, по первоначальной терминологии С. Н. Черникова, *экстремальной*).

Доказательство. Ввиду условия минимальности группа G содержит подгруппу H конечного индекса, не содержащую других подгрупп конечного индекса. Так как пересечение двух подгрупп конечного индекса само имеет конечный индекс, то H единственна, а потому нормальна. Если H абелева, то для всякого простого числа p группа $H/H^p \simeq \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots$ конечна, а потому $H = H^p$, т. е. H — полная абелева группа. По теореме 9.1.6 она разлагается в прямое произведение квазициклических групп. Ввиду условия минимальности их число конечно. Тем самым для абелевой группы G теорема доказана.

Пусть теперь G бесконечна и неабелева. Возьмем в H неединичную абелеву нормальную подгруппу A (например, последний неединичный коммутант). Покажем, что A лежит в центре группы H. В самом деле, A — абелева группа с условием минимальности, а потому по предыдущему содержит лишь конечное число элементов любого данного порядка. Значит, каждый элемент a из A имеет в H лишь конечное число сопряженных элементов, откуда $|H : C_H(a)| < \infty$. Так как H не содержит подгрупп конечного индекса, то

$$C_H(a) = H, \quad A \leqslant Z(H),$$

что и требовалось.

Покажем теперь, что подгруппа H нильпотентна. Мы сделаем это индукцией по ее ступени разрешимости k. Так как, по предыдущему, $H^{(k-1)} \leqslant Z(H)$, то $H/Z(H)$ разрешима ступени $\leqslant k-1$. По индуктивному предположению, примененному к группе $G/Z(H)$, группа $H/Z(H)$ нильпотентна, а потому и сама H нильпотентна.

Покажем, наконец, что H абелева. Пусть B — максимальная абелева нормальная подгруппа в H. По доказанному ранее B лежит в центре группы H, а по теореме 16.2.6 B совпадает с ее централизатором в H. Отсюда $B = H$, т. е. группа H абелева. Теорема доказана.

24.1.5. У п р а ж н е н и е. Класс черниковских групп замкнут относительно взятия подгрупп, гомоморфных образов и расширений.

Так как автоморфизмы групп вида

$$\mathbb{C}_{p^\infty} \times \ldots \times \mathbb{C}_{p^\infty}$$

изображаются матрицами из $GL_n(\mathbb{Z}_{p^\alpha})$ (упражнение 5.1.4), то при изучении черниковских групп оказывается полезным

24.1.6. У п р а ж н е н и е. Группа матриц $GL_n(\mathbb{Z}_{p^\alpha})$ почти вся не имеет кручения. В частности, ее периодические подгруппы конечны.

У к а з а н и е. Конгруэнц-подгруппа по модулю p^i, $i = 1, 2, \ldots$, т. е. группа матриц $e + p^i a$, $a \in M_n(\mathbb{Z}_{p^\alpha})$, имеет конечный индекс в $GL_n(\mathbb{Z}_{p^\alpha})$ и не имеет кручения за исключением случая $p = 2$, $i = 1$ (см. 4.2.7 и 5.1.5).

Что касается разрешимых групп с условием max, то их полное описание дает такая очень простая

24.1.7. Т е о р е м а. *Группа G тогда и только тогда разрешима и удовлетворяет условию максимальности, когда она полициклическая.*

Д о к а з а т е л ь с т в о. Достаточность уже отмечалась (см. 24.1.3). Докажем необходимость. Пусть G удовлетворяет условию max и имеет конечную разрешимую матрёшку

$$1 = G_0 \leqslant G_1 \leqslant \ldots \leqslant G_n = G.$$

Так как ее секции G_{i+1}/G_i тоже удовлетворяют условию max (см. 24.1.2), то они конечно порождены и, значит, разлагаются в прямые произведения циклических групп (теорема 8.1.2). Это позволяет уплотнить данную матрёшку до полициклической матрёшки. Теорема доказана.

Выделим особо — ввиду его важности — описание а б е л е в ы х групп с условиями min и max, полученное в ходе доказательства теорем 24.1.4 и 24.1.7:

24.1.8. У п р а ж н е н и е. Абелева группа тогда и только тогда удовлетворяет условию min, когда она разлагается в прямое произведение конечного числа квазициклических и конечных циклических групп. В частности, для абелевых p-групп условие min равносильно ус-

ловию конечности ранга (см. 10.1.16). Абелева группа тогда и только тогда удовлетворяет условию max, когда она разлагается в прямое произведение конечного числа циклических групп.

24.1.9. Упражнение. Опираясь на локальную теорему А. И. Мальцева 22.3.2 и теорему О. Ю. Шмидта 23.1.1 и повторяя схему доказательства теоремы 24.1.4, получить следующее ее обобщение: *всякая RN-группа с условием* min *является разрешимой черниковской.*

24.2. Перенос с абелевых подгрупп на разрешимую группу. В этом пункте мы докажем, что если в разрешимой группе G условие min или max выполняется для абелевых подгрупп, то оно должно выполняться и для произвольных подгрупп, а потому G опять-таки будет черниковской или полициклической группой соответственно. Конечно, первое, что приходит в голову,— доказывать это утверждение индукцией по ступени разрешимости. Пусть A — последний неединичный коммутант группы G. Если мы докажем, что в G/A все абелевы подгруппы снова удовлетворяют условию min (max), то останется сослаться на то, что свойство группы быть черниковской (полициклической) сохраняется при расширениях (см. 4.4.3 и 24.1.5). Таким образом, нужно научиться доказывать, что некоторое свойство подгрупп группы G сохраняется при переходе к ее фактор-группе по нормальной абелевой подгруппе A. А нельзя ли «пересаживать» подгруппы из G/A в саму G (тогда и их свойства, естественно, наследовались бы)? Идеальным ответом здесь была бы «дополняемость» A в G, т. е. наличие в G подгруппы X, для которой

$$G = XA \text{ и } X \cap A = 1$$

(тогда $X \simeq G/A$). Мы увидим, что хотя идеальный ответ не всегда возможен, некоторую «почти дополняемость» можно гарантировать — она и будет основным нашим орудием.

Пусть A — нормальная подгруппа группы G. Будем говорить, что A min-*неприводима* относительно G, если всякая нормальная подгруппа H группы G, содержащаяся в A и отличная от A, конечна. Двойственным образом, будем говорить, что A max-*неприводима* относительно G, если для всякой нормальной подгруппы H группы G, содержащейся в A и отличной от 1, фактор-группа A/H

периодическая. (Конечно, для полной двойственности лучше было бы требовать, что A/H конечна, однако в приложениях max-неприводимость обычно возникает именно в такой более слабой форме; этим объясняется также, почему в следующей лемме предположений для случая max делается больше и доказательство длиннее.)

24.2.1. Лемма. *Пусть* $A \trianglelefteq G$, *обе группы* A, G/A *абелевы и* A *не центральна в* G.

а) *Если* A min-*неприводима относительно* G, *то существует такая подгруппа* X, *что*

$$G = XA \quad и \quad |X \cap A| < \infty.$$

б) *Если* A — *группа без кручения конечного ранга*, max-*неприводимая относительно* G, *то существует такая подгруппа* X, *что*

$$|G : XA| < \infty \quad и \quad X \cap A = 1.$$

Доказательство. Можно сразу считать, что подгруппа A бесконечна — иначе имели бы случай а) и достаточно было бы взять $X = G$. Возьмем в группе G элемент x, для которого $[A, x] \neq 1$, и покажем, что его централизатор $X = C_G(x)$ — искомая подгруппа в обоих случаях. Очевидно, отображение $\theta\colon a \mapsto [a, x]$ есть эндоморфизм подгруппы A. Более того, он перестановочен со всеми сопряжениями группы G, т. е.

$$[a, x]^g = [a^g, x] \text{ для всех } a \in A,\ g \in G,$$

так как $x^g \equiv x \pmod{A}$ (воспользоваться коммутаторными тождествами из § 3).

а) Поскольку $\operatorname{Ker}\theta < A$ и A min-неприводима относительно G, то $\operatorname{Ker}\theta$ или, что то же самое, пересечение $X \cap A$ конечно. Тогда образ A^θ бесконечен, откуда, снова ввиду min-неприводимости, $A = A^\theta = [A, x]$. Теперь ясно, что для всякого $g \in G$ существует $a \in A$ с условием $[g, x] = [a, x]$, откуда $ga^{-1} \in X$ и, следовательно, $G = AX$.

б) Так как $\operatorname{Ker}\theta < A$, группа $A/\operatorname{Ker}\theta \simeq A^\theta$ не имеет кручения, а A max-неприводима относительно G, то $\operatorname{Ker}\theta = 1$ или, что то же самое, $X \cap A = 1$. Далее, ввиду 7.2.3, фактор-группа A/A^θ конечна; пусть m — ее порядок. Группа G индуцирует в A/A^θ (сопряжениями)

группу автоморфизмов, изоморфную группе G/C, где $C = C_G(A/A^\theta)$, поэтому G/C также конечна. Если $c \in C$, то $[c, x]^m \in A^\theta = [A, x]$. Далее,

$$[c^m, x] \equiv [c, x]^m \pmod{[C, x, C]},$$

$$[C, x, C] \leqslant [A, C] \leqslant [A, x],$$

так что $[c^m, x] = [a, x]$ для некоторого $a \in A$. Отсюда $c^m a^{-1} \in X$, $c^m \in XA$. Следовательно, фактор-группа G/XA периодическая, и остается доказать, что она конечно порождена.

Пусть $a_1, \ldots, a_m$ — представители смежных классов группы A по подгруппе $[A, x]$. Для каждого $j = 1, \ldots, m$ выберем в G элемент g_j с условием $a_j = [g_j, x]$, а если такого элемента не существует, то положим $g_j = 1$. Для каждого $g \in G$ имеем $[g, x] = a_i\,[b_i, x]$ при подходящих i и $b_i \in A$. Следовательно,

$$[gb_i^{-1}, x] = a_i = [g_i, x],$$

откуда

$$gb_i^{-1}g_i^{-1} \in X, \quad g \in \text{гр}\,(g_1, \ldots, g_m, X, A).$$

Теперь ясно, что группа G/XA конечно порождена. Лемма доказана.

24.2.2. Теорема (С. Н. Черников). *Разрешимая группа G, у которой абелевы подгруппы удовлетворяют условию* min, *является черниковской.*

(Заметим, что на самом деле С. Н. Черников доказал сразу значительно более сильную теорему 24.3.4, содержащую 24.2.2 как частный случай. Внутренняя логика позднейшего изложения предмета не всегда совпадает с его историей.)

Доказательство проведем индукцией по ступени разрешимости группы G. Как уже говорилось в начале пункта, достаточно доказать, что если группа G удовлетворяет условию min для абелевых подгрупп и A — ее абелева нормальная подгруппа, то фактор-группа G/A тоже удовлетворяет условию min для абелевых подгрупп. Заметим на будущее, что доказательства подобных утверждений для пары G, A нередко очень облегчаются разложением подгруппы A в G-допустимую матрёшку

$$1 = A_1 \leqslant A_2 \leqslant \ldots \leqslant A_{n+1} = A$$

с последующим рассмотрением пары G, A_1, затем пары $G/A_1, A_2/A_1$ и т. д.

Допустим сначала, что A конечна, и докажем, что каждая абелева подгруппа B/A группы G/A действительно удовлетворяет условию min. Группа $B/C_B(A)$ также конечна (она изоморфна подгруппе из Aut A) и, разумеется, $A \leqslant C_B(A)$. Будем считать поэтому, что $[A, B] = 1$, причем A уже не обязательно конечна. Возьмем в B какую-нибудь максимальную абелеву нормальную подгруппу M. Очевидно, $A \leqslant M$, а так как B нильпотентна, то $M = C_B(M)$ (см. 16.2.6). Легко видеть, что отображение

$$\tau\colon\ B/M \to \mathrm{Hom}\,(M/A,\ A),$$

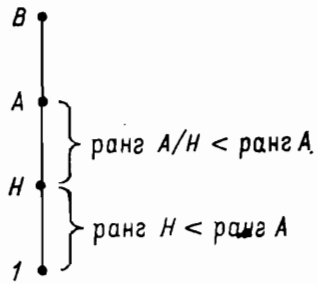
определенное правилом

$$(bM)^{\tau}\colon\ xA \mapsto [x,\ b],$$

является вложением (определение Hom см. в 5.1.6). Так как B (и даже вся G) периодическая, а M удовлетворяет условию min, то достаточно убедиться, что периодическая часть группы Hom $(M/A, A)$ конечна. Ввиду 24.1.8 $M/A = P \oplus Q$, где P — полная, Q — конечная группы, поэтому достаточно проверить, что всякий периодический элемент φ из Hom $(M/A, A)$ действует на P тривиально, т. е. отображает P в нуль. Но это действительно так: если бы φ отображал какой-то элемент $x \in P$ не в нуль, то для всякого $n \geqslant 1$ гомоморфизм $n\varphi$ отображал бы элементы множества $\frac{1}{n}x$ также не в нуль.

Пусть теперь A бесконечна. Разложив ее в G-допустимую матрёшку с примарными секциями, конечными или полными, мы видим, что достаточно изучить случай, когда A — полная абелева p-группа. Докажем, что в этом случае всякая абелева подгруппа B/A группы G/A также удовлетворяет условию min. Так как для $A = 1$ утверждение тривиально, воспользуемся индукцией по рангу группы A. Предположим сначала, что A min-приводима относительно B, т. е. содержит неединичную полную собственную B-допустимую подгруппу H. Так как полная подгруппа абелевой группы выделяется в ней прямым множителем (теорема 9.1.4) и ранг конечного прямого произведения квазициклических p-групп равен числу сомножителей, то

получаем такую картину:



Поднимаясь по матрёшке $1 \leqslant H \leqslant A$, мы видим, что ранг группы B/A конечен. Пусть теперь A min-неприводима относительно B. Можно считать также, что $[A, B] \neq 1$, так как противоположный случай был рассмотрен выше. По лемме 24.2.1. а) B содержит такую подгруппу X, что

$$B = XA \text{ и } |X \cap A| < \infty.$$

Согласно разобранному выше случаю (когда A конечна) подгруппа X удовлетворяет условию min, а потому B и B/A также ему удовлетворяют. Теорема доказана.

24.2.3. Теорема (А. И. Мальцев). *Разрешимая группа, у которой все абелевы подгруппы удовлетворяют условию* max, *является полициклической.*

Доказательство проводится по тому же плану. Пусть G удовлетворяет условию max для абелевых подгрупп, A — ее абелева нормальная подгруппа; докажем, что G/A также удовлетворяет условию max для абелевых подгрупп.

Сначала опять допустим, что $[A, B] = 1$ (этим, в частности, охватывается случай, когда A конечна). Пусть M, τ имеют тот же смысл, что и в предыдущем доказательстве. Так как M/A и A — конечно порожденные абелевы группы, то таковы и аддитивная группа $\mathrm{Hom}\,(M/A, A)$ (см. 8.1.8) и вложенная в нее группа B/M. Следовательно, B и вместе с ней B/A удовлетворяют условию max.

Переходя к общему случаю, можно считать, что A не имеет кручения, так как ее периодическая часть A_0 конечна и, значит, над A_0 можно подняться согласно предыдущему. Докажем опять, что всякая абелева подгруппа B/A группы G/A удовлетворяет условию max. Так как

при $A = 1$ это тривиально, воспользуемся индукцией по рангу группы A. Предположим сначала, что A max-приводима относительно B, т. е. содержит неединичную B-допустимую подгруппу H с непериодической факторгруппой A/H. Пусть T/H — периодическая часть группы A/H. Так как в конечно порожденных абелевых группах без кручения ранг совпадает с размерностью, а при факторизации размерности складываются (см. 7.2.2), то картина такова:

Поднимаясь по матрёшке $1 \leqslant H \leqslant T \leqslant A$, мы видим, что ранг группы B/A конечен. Пусть теперь A max-неприводима относительно B. Можно считать также, что $[A, B] \neq 1$ (противоположный случай был разобран выше). По лемме 24.2.1.б) существует подгруппа X, для которой

$$|B : XA| < \infty \text{ и } X \cap A = 1.$$

Так как подгруппа $X \simeq XA/A$ абелева, то она, а потому и подгруппа XA, удовлетворяет условию max. Следовательно, B и B/A также удовлетворяют этому условию. Теорема доказана.

Полезно отметить для дальнейшего, что на самом деле вместо теорем 24.2.2 и 24.2.3 доказана более общая.

24.2.4. Теорема. *Пусть A — абелева нормальная подгруппа группы G. Если G удовлетворяет условию* min (*соответственно* max) *для абелевых подгрупп, то G/A также удовлетворяет условию* min (*соответственно* max) *для абелевых подгрупп.*

24.2.5. Упражнение. Если в разрешимой группе все абелевы подгруппы конечны, то она сама конечна.

24.3. О локально разрешимых группах. В этом пункте мы распространим теорему 24.2.2 с разрешимых на локально разрешимые группы, придав ей тем самым наибольшую разумную общность. Подчеркнем сразу же, что для параллельной ей теоремы 24.2.3 подобное обобщение невозможно — причины этого мы обсудим в следующем параграфе, когда столкнемся с аналогичным препятствием для групп конечного ранга.

Начнем с такого частного случая:

24.3.1. Л е м м а. *Всякая локально конечная p-группа G с условием* min *для абелевых подгрупп является разрешимой черниковской.*

Д о к а з а т е л ь с т в о. а) Ввиду теоремы 24.2.2 достаточно доказать, что G разрешима. Так как в неразрешимой группе существуют счетные неразрешимые подгруппы, то можно предполагать, что G счетна и отлична от единицы.

б) Центр $Z(G)$ группы G отличен от единицы. В самом деле, так как G счетна, то ее можно представить в виде объединения возрастающей последовательности конечных подгрупп $1 < G_1 < G_2 < \ldots$ Пусть $Z_i = Z(G_i)$, $i = 1, 2, \ldots$ Так как центр конечной p-группы отличен от единицы (см. 17.1.1), то все $Z_i \neq 1$. Порожденная ими подгруппа

$$Z = \text{гр}\,(Z_1, Z_2, \ldots)$$

абелева, а потому удовлетворяет условию min. Учитывая строение абелевых групп с условием min (упражнение 24.1.8), видим, что элементы z из Z с условием $z^p = 1$ составляют конечную подгруппу P. Так как $P \leqslant G_i$ для некоторого i, то $P \cap Z_i \geqslant P \cap Z_{i+1} \geqslant \ldots$ и, значит, $P \cap Z_j = P \cap Z_{j+1} = \ldots$ для некоторого j. Ясно, что $1 < P \cap Z_j \leqslant Z(G)$.

в) Все гиперцентры группы G разрешимы. Пусть, напротив, α-й гиперцентр $\zeta_\alpha G$ группы G неразрешим, причем α — первое порядковое число с этим свойством. Ясно, что оно предельное и больше нуля. Положим для краткости $L = \zeta_\alpha G$ и выберем в L какую-нибудь максимальную абелеву нормальную подгруппу M. Очевидно, L является ZA-группой, поэтому, ввиду 22.1.7, $M = C_L(M)$. Пусть A/M — максимальная абелева нормальная подгруппа группы L/M. По теореме 24.2.4 A/M удовлетворяет условию min. Очевидно, M также удовлетворяет этому усло-

вию и может быть представлена в виде объединения возрастающей последовательности своих конечных подгрупп $M_1 < M_2 < \ldots$, нормальных в L. Так как

$$C_A(M_1) \geqslant C_A(M_2) \geqslant \ldots,$$

то найдется номер i, для которого

$$C_A(M_i) = C_A(M_{i+1}) = \ldots = C_A(M) = M.$$

Группа $A/M \simeq A/C_A(M_i)$ вкладывается в Aut M_i, а потому конечна. Но тогда и (ZA-группа) L/M конечна (см. последнее замечание в 22.1.7). Значит, L разрешима.

г) Группа G разрешима. В самом деле, если $\zeta_\beta G < G$, то из теоремы 24.2.4 следует, что фактор-группа $G/\zeta_\beta G$ удовлетворяет условию min для абелевых подгрупп [учесть, что ввиду в) $\zeta_\beta G$ разрешима]. Ввиду б) центр этой фактор-группы отличен от единицы, а потому $\zeta_\beta G < \zeta_{\beta+1} G$. Таким образом, последовательность гиперцентров $\{\zeta_\beta G\}$ доходит до всей группы G, а потому, снова ввиду в), G должна быть разрешимой. Лемма доказана.

24.3.2. Л е м м а. *Пусть G — локально конечная группа, p — простое число, $S = X/Y$ — секция группы G и $S_1 < S_2 < \ldots$ — бесконечная возрастающая последовательность конечных p-подгрупп группы S. Тогда в X существует такая возрастающая последовательность конечных p-подгрупп $P_1 < P_2 < \ldots$, что*

$$S_i = P_i Y/Y, \quad i = 1, 2, \ldots$$

Д о к а з а т е л ь с т в о. Возьмем в смежных классах по Y, составляющих (конечную) секцию S_i, по представителю и породим ими подгруппу F_i. Так как G локально конечна, то F_i конечна и, очевидно, $S_i = F_i Y/Y$. Можно считать при этом, что $F_1 \leqslant F_2 \leqslant \ldots$ Выберем в каждой подгруппе F_i по силовской p-подгруппе P_i так, чтобы было $P_1 \leqslant P_2 \leqslant \ldots$ Так как при гомоморфизмах конечных групп силовские подгруппы переходят в силовские (см. 11.3.4), а при факторизации F_i по $F_i \cap Y$ получается p-группа (изоморфная S_i), то $P_i(F_i \cap Y) = F_i$. Теперь ясно, что $F_i Y = P_i Y$ и $P_1 < P_2 < \ldots$

24.3.3. Л е м м а. *Пусть G — локально конечная группа. Если G удовлетворяет условию* min *для абелевых подгрупп, то она не имеет бесконечных элементарных абе-*

левых секций. Если в G все силовские подгруппы конечны, то и в любой ее секции тоже.

Доказательство. Допустим, что G удовлетворяет условию min для абелевых подгрупп и обладает счетной элементарной абелевой секцией S. Пусть $S_1 < S_2 < \ldots$ — возрастающая последовательность конечных подгрупп из S, дающая в объединении S, $P_1 < P_2 < \ldots$ — соответствующая ей в силу предыдущей леммы последовательность p-подгрупп группы G. Так как группа $P = \bigcup P_i$ удовлетворяет условию min для абелевых подгрупп, то она черниковская (лемма 24.3.1). Значит, ранги всех P_i ограничены. Это, однако, невозможно, так как ранги группы S_i неограничены. Второе утверждение леммы следует из 24.3.2 совсем очевидным образом.

24.3.4. Теорема (С. Н. Черников). *Всякая локально разрешимая группа с условием минимальности для абелевых подгрупп является разрешимой черниковской.*

Доказательство. Пусть G — локально разрешимая группа с условием min для абелевых подгрупп. По локальной теореме А. И. Мальцева 22.3.2 G обладает некоторой RI-матрёшкой. Пусть $\mathcal{M}$ — неуплотняемая RI-матрёшка группы G. Очевидно, каждая секция S этой матрёшки — периодическая абелева автоморфно простая группа, поэтому S — элементарная абелева группа (см. 5.2.8). По лемме 24.3.3 она к тому же конечна.

Пусть R — подгруппа, порожденная в G всеми квазициклическими подгруппами. Так как R не содержит подгрупп конечного индекса (см. 2.4.10), то она стабилизирует матрёшку $\mathcal{M}$, т. е. индуцирует в каждой ее секции S единичную группу автоморфизмов. Значит, R обладает центральной матрёшкой (см. 22.1.5). Так как R локально конечна, то она локально нильпотентна. Ввиду 18.1.5 и 24.3.1 она черниковская, а так как не содержит собственных подгрупп конечного индекса, то абелева.

Фактор-группа G/R уже не содержит квазициклических подгрупп. В самом деле, допустим, что такая подгруппа H/R существует, т. е. в G найдутся элементы $1 = a_1, a_2, \ldots$ такие, что

$$H = \text{гр}\,(a_1, a_2, \ldots)\cdot R$$

и

$$a_{i+1}^p \equiv a_i \pmod{R}, \quad i = 1, 2, \ldots$$

Группа H, действуя в группе R сопряжениями, индуцирует в ней автоморфизмы. Если хотя бы один из них был бы нетождественным, то, взяв элемент из R, который им передвигается, и добавив все элементы из R того же порядка, мы получили бы конечное множество M, на котором H действует нетождественно. Подгруппа H_0 всех элементов из H, действующих на M тождественно, содержит R и имеет конечный индекс в H. Так как $H/H_0 \simeq \simeq (H/R)/(H_0/R)$ и H/R не содержит собственных подгрупп конечного индекса, то получилось противоречие. Значит, H поэлементно перестановочна с R. Заметив это, мы заменим сейчас элементы $1 = a_1, a_2, \ldots$ на $1 = b_1, b_2, \ldots$ с условием

$$b_i \equiv a_i \pmod{R},\ b_{i+1}^p = b_i, \qquad i = 1, 2, \ldots$$

Действительно, пусть $b_1, \ldots, b_i$ уже построены и $a_{i+1}^p = b_i r_i$, $r_i \in R$. Возьмем в R элемент x_{i+1} с условием $x_{i+1}^p = r_i$ и положим $b_{i+1} = a_{i+1}x_{i+1}^{-1}$. Ясно, что $b_{i+1} \equiv \equiv a_{i+1} \pmod{R}$ и $b_{i+1}^p = b_i$. Построенные таким способом элементы $b_1, b_2, \ldots$, очевидно, порождают в G квазициклическую подгруппу, не лежащую в R, что противоречит выбору подгруппы R.

Так как, по доказанному, группа G/R не содержит квазициклических подгрупп и удовлетворяет условию min для абелевых подгрупп (теорема 24.2.4), то все ее абелевы и все ее силовские подгруппы конечны (см. 24.1.8 и 24.3.1 соответственно). Докажем, что сама G/R конечна.

Итак, пусть G — локально разрешимая группа, у которой все абелевы и все силовские подгруппы конечны. Надо доказать, что G сама конечна. Так как каждая бесконечная группа содержит счетные подгруппы, то достаточно доказать, что G не может быть счетной. Пусть, напротив, она счетна. Так как G локально конечна (см. 24.2.5), то ее можно представить в виде объединения возрастающей последовательности конечных подгрупп $G_1 < G_2 < \ldots$

Так как каждая G_n конечна и разрешима, то она содержит некоторую нормальную элементарную абелеву p_n-подгруппу A_n (см. 19.1.7). Если среди простых чисел $p_1, p_2, \ldots$ имеется лишь конечное число различных, то, перейдя к подходящей подпоследовательности, можно

считать, что все p_n совпадают с некоторым p. Пусть

$$A = \text{гр}\,(A_1,\ A_2,\ \ldots) = A_1A_2\ldots$$

Так как силовские подгруппы в G конечны, то A конечна. Но тогда среди подгрупп A_1, A_2, ... найдется бесконечно много совпадающих, т. е. G обладает конечной нормальной элементарной абелевой подгруппой K_1.

Ввиду 24.2.5 и 24.3.3 в локально разрешимой группе G/K_1 все абелевы и все силовские подгруппы снова конечны. Повторим проведенное выше рассуждение для G/K_1, взятой вместо группы G. Если при этом в G/K_1 найдется конечная нормальная элементарная абелева подгруппа K_2/K_1, то повторим рассуждение для G/K_2, и т. д. В конце концов мы либо построим в G бесконечную возрастающую последовательность конечных нормальных подгрупп $K_1 < K_2 < \ldots$, либо придем к фактор-группе G/K_{i_0}, для которой процесс выделения групп A_n связан с последовательностью простых чисел p_n, содержащей бесконечно много различных членов.

В первом случае рассмотрим группу $K = \bigcup K_i$. Для каждого простого числа p она может иметь лишь конечное число секций K_{i+1}/K_i, порядки которых делятся на p (так как силовские подгруппы в G конечны), а потому множество $\pi(K)$ всех простых делителей порядков элементов из K бесконечно. Далее, для всякого $p \in \pi(K)$ множество элементов из K порядка p конечно, так как все силовские p-подгруппы группы K лежат в некотором K_i. Пусть $p_1 \in \pi(K)$, a_1 — элемент из K порядка p_1 и $C_1 = C_K(a_1)$. Так как

$$|K : C_1| = |a_1^K| < \infty$$

(см. 2.5.6), то множество $\pi_1 = \pi(C_1)$ снова бесконечно. Возьмем в π_1 элемент $p_2 \neq p_1$ и в C_1 элемент a_2 порядка p_2. Так как подгруппа

$$C_2 = C_K(a_1, a_2) = C_K(a_1) \cap C_K(a_2)$$

имеет в K конечный индекс, то множество $\pi_2 = \pi(C_2)$ бесконечно. Возьмем в π_2 элемент $p_3 \neq p_1, p_2$ и в C_2 элемент a_3 порядка p_3. Продолжая эти рассуждения, получим попарно перестановочные элементы $a_1, a_2, \ldots$ порядков $p_1, p_2, \ldots$ соответственно. Так как порожденная

ими подгруппа бесконечна, то первый случай на самом деле невозможен.

Переходя ко второму случаю, будем считать, что уже для самой группы G последовательность $p_1, p_2, \ldots$ содержит бесконечно много различных чисел. Более того, можно считать, что уже сами числа $p_1, p_2, \ldots$ различны — иначе мы просто опустили бы те группы G_n, которым отвечают повторяющиеся p_n.

Последовательность групп $A_1, A_2, \ldots$ не может содержать бесконечной подпоследовательности циклических групп. В самом деле, пусть, напротив, $A_{k_1}, A_{k_2}, \ldots$ — такая подпоследовательность. Положим

$$B_j = \text{гр}\,(A_{k_j}, A_{k_{j+1}}, \ldots), \quad j = 1, 2, \ldots$$

Так как группа B_1 обладает нормальной матрёшкой $B_1 > B_2 > \ldots$ с циклическими секциями, то ее коммутант B_1' обладает центральной матрёшкой (см. 22.1.6). Так как группа B_1' локально конечна, то она локально нильпотентна, а потому разлагается в прямое произведение своих силовских подгрупп (см. 18.1.5). Но ее силовские являются циклическими, поэтому B_1' абелева. Таким образом, группа B_1 разрешима, а потому конечна (см. 24.2.5). Это, однако, невозможно по самому определению группы B_1.

Итак, среди групп $A_1, A_2, \ldots$ число циклических групп не более чем конечно; можно считать поэтому, что их нет совсем. Так как A_i и A_j при $i \neq j$ — нециклические элементарные абелевы группы различных периодов, то в силу 6.1.6 в произведении A_iA_j существует элемент порядка p_ip_j, а потому в группах A_i и A_j существуют перестановочные между собой неединичные элементы a_i и a_j. Рассмотрим всевозможные пары

$$(x_1, x_i), \text{ где } x_1 \in A_1, \ x_i \in A_i, \ x_1x_i = x_ix_1,$$

$i = 2, 3, \ldots$ Так как группа A_1 конечна, то существует бесконечное множество пар

$$(b_1, x_{i_1}), (b_1, x_{i_2}), \ldots$$

с одинаковым первым элементом. Значит, в A_1 существует неединичный элемент b_1, централизатор которого в G содержит бесконечную подгруппу N_1, не содержащую b_1. Так как N_1 удовлетворяет тем же условиям, что и G, то

в N_1 существует неединичный элемент b_2, централизатор которого в G содержит бесконечную подгруппу N_2, не содержащую b_2, и т. д. Очевидно, что элементы b_1, b_2, ... попарно перестановочны и порождают бесконечную подгруппу. Это, однако, невозможно, так как все абелевы подгруппы группы G конечны. Теорема доказана.

Общую теорию групп с заданными свойствами системы их подгрупп, развиваемую с 40-х годов одним из основоположников современной теории групп С. Н. Черниковым и его учениками, можно найти в монографии [31].

§ 25. Конечность ранга

25.1. Примеры. Рассмотрим для начала некоторые интересные конкретные группы и вычислим или хотя бы оценим сверху их ранги.

25.1.1. Пример. Пусть p — простое число, m, n — натуральные числа, $m \geqslant 2$. За исключением случая $p = 2$, $k = 1$, все главные конгруэнц-подгруппы

$$P_k = GL_n(\mathbb{Z}_{p^m}, p^k\mathbb{Z}_{p^m}), \qquad k = 1, 2, \ldots,$$

группы $GL_n(\mathbb{Z}_{p^m})$ имеют ранг n^2 (не зависящий, стало быть, ни от p, ни от m, ни от k).

В самом деле, из описания групп P_k, данного в 4.2.8, видно, что P_{m-1}^{i} — векторное пространство размерности n^2 над полем из p элементов, поэтому достаточно убедиться, что при $p > 2$ ранг группы P_1 не выше n^2, а при $p = 2$ ранг группы P_2 не выше n^2. Оба эти случая разбираются аналогично, и мы ограничимся рассмотрением только первого из них ($p > 2$).

Пусть H — произвольная подгруппа группы P_1; нужно показать, что она порождается не более чем n^2 элементами. Пусть φ_k — гомоморфизмы, описанные в 4.2.8. Очевидно,

$$H^{\varphi_1} \leqslant (H \cap P_2)^{\varphi_2} \leqslant \ldots \leqslant (H \cap P_{m-1})^{\varphi_{m-1}} = H \cap P_{m-1}.$$

Выберем в векторном пространстве $H \cap P_{m-1}$ такую базу $a_1, \ldots, a_s$, в которой первые s_1 элементов являются базисными для H^{φ_1}, первые s_2 элементов — базисными для $(H \cap P_2)^{\varphi_2}$ и т. д., $0 \leqslant s_1 \leqslant \ldots \leqslant s \leqslant n^2$. Пусть m_i — наибольшее число, при котором уравнение $x^{p^{m_i}} = a_i$

имеет решение в H, b_i — одно из таких решений. Покажем, что H порождается элементами $b_1, \ldots, b_s$. Пусть уже доказано, что

$$H \cap P_{k+1} \leqslant \text{гр}(b_1, \ldots, b_s),$$

и пусть $x \in H \cap P_k$. Тогда $x^{\varphi_k} = v(\ldots, a_i, \ldots)$, где v — некоторое слово, $i \leqslant s_k$. Ясно, что

$$x = v(\ldots, b_i^{p^{m_i+k+1-m}}, \ldots) \cdot y, \qquad y \in H \cap P_{k+1},$$

и, следовательно, $H \cap P_k \leqslant$ гр $(b_1, \ldots, b_s)$. Индуктивные соображения позволяют теперь заключить, что H содержится в группе гр $(b_1, \ldots, b_s)$, а потому совпадает с ней (обратное включение очевидно).

25.1.2. Упражнение. Провести доказательство в случае $p = 2$, $k > 1$.

25.1.3. Пример. Ранг силовской p-подгруппы группы $GL_n(\mathbb{Z}_{p^m})$ не превосходит числа $\theta(n) = \frac{1}{2}(5n-1)n$ (не зависящего от m).

Действительно, эта силовская p-подгруппа P описана — с точностью до сопряженности — в упражнении 11.3.3. Пусть P_k имеют тот же смысл, что и выше (в упражнении 25.1.1). Рассмотрим цепочку подгрупп $P \geqslant P_1 \geqslant P_2$. Фактор-группа P/P_1 изоморфна группе $UT_n(p)$, поэтому обладает нормальным матрёшкой с абелевыми секциями рангов $n-1, n-2, \ldots, 1$ (см. 16.1.2). Фактор-группа P_1/P_2 либо тривиальна, либо элементарная абелева ранга n^2. Наконец, группа P_2 либо тривиальна, либо ввиду 25.1.1 имеет ранг n^2. Отсюда и из 4.1.7 следует, что ранг P не выше $2n^2 + (n-1) + (n-2) + \ldots + 1 = \theta(n)$.

25.1.4. Пример. Как сказывается конечность ранга на локальных свойствах групп — скажем, на локальной нильпотентности или локальной разрешимости? Напомним для сравнения, что, например, при условии линейности группы локальная разрешимость превращается в разрешимость (упражнение 21.1.6), хотя, с другой стороны, существуют линейные локально нильпотентные группы, не являющиеся нильпотентными (приведите примеры!). Мы покажем сейчас, что при условии конечности ранга ни локально нильпотентная группа не

обязана быть нильпотентной, ни локально разрешимая группа — разрешимой.

В самом деле, пусть n — натуральное число $\geqslant 3$. Рассмотрим прямое произведение конгруэнц-групп

$$G = \prod_p GL_n(\mathbb{Z}_{m(p)}, p\mathbb{Z}_{m(p)}),$$

где p пробегает все простые числа, $m(p) = p^{l(p)}$ и числа $l(p)$ не ограничены в совокупности. Так как множители этого произведения — конечные p-группы (см. доказательство 14.2.2), то G локально нильпотентна. С другой стороны, согласно формуле (9) из § 3

$$[t_{ik}(p^{2^l}), t_{kj}(p^{2^l})] = t_{ij}(p^{2^{l+1}})$$

при различных i, j, k, поэтому ступени разрешимости множителей не ограничены в совокупности и, значит, G не может быть разрешимой. Наконец, ввиду 2.3.4 и 25.1.1 ранг группы G конечен — равен n^2.

25.1.5. Пример. Если A — абелева p-группа конечного ранга r, то всякая p-подгруппа Φ ее группы автоморфизмов конечна и ранг Φ не превосходит числа $\theta(r)$ из примера 25.1.3.

Ясно, что пример 25.1.3 появляется здесь не случайно — это в точности частный случай нашего утверждения, когда A — прямая сумма $r = n$ циклических групп одного и того же порядка p^m. Общее утверждение достаточно свести к этому частному, что мы сейчас и сделаем.

Прежде всего, ввиду 10.1.16 $A = B \oplus C$ (в аддитивной записи), где группа B конечна, а C — прямая сумма не более чем r квазициклических групп. Пусть p^l — наибольший порядок элементов из B, A_0 — подгруппа элементов из A, удовлетворяющих уравнению

$$p^{l'}x = 0, \text{ где } l' = \max(l, 2).$$

Очевидно, A_0 конечна и автоморфно (даже эндоморфно) допустима в A. Покажем, что если $\varphi \in \Phi$ и φ действует на A_0 тождественно, то $\varphi = 1$. В самом деле, так как $B \leqslant A_0$, то φ оставляет элементы из B неподвижными, и остается доказать, что $\varphi|_C = 1$.

Ввиду 5.1.4 автоморфизму $\varphi|_C$ соответствует некоторая матрица α над кольцом целых p-адических чисел

причем

$$\alpha \equiv \varepsilon \pmod{p^2},$$

так как φ оставляет на месте все решения уравнения $p^2x = 0$ (здесь ε — единичная матрица). Если $\alpha \neq \varepsilon$, то матрица α должна быть элементом бесконечного порядка (см. указание к 24.1.6), что противоречит периодичности группы Φ. Значит, $\varphi = 1$.

Из сказанного следует, что сопоставление каждому автоморфизму $\varphi \in \Phi$ его сужения φ_0 на (конечную автоморфно допустимую) подгруппу A_0 является изоморфизмом, т. е. $\Phi \simeq \Phi_0$, где Φ_0 — группа всех таких φ_0. Таким образом, можно сразу считать, что группа A к о н е ч н а.

Пусть A — прямая сумма циклических групп порядков $p^{m_1}, \ldots, p^{m_r}$ и $m = \max(m_1, \ldots, m_r)$. Погрузим A в «однородную» сумму

$$A^* = (a_1) \oplus \ldots \oplus (a_r),$$

где все слагаемые одного и того же порядка p^m, полагая

$$A = (p^{k_1}a_1) \oplus \ldots \oplus (p^{k_r}a_r),$$

где $k_i = m - m_i$, $i = 1, \ldots, r$. Для каждого автоморфизма φ группы A имеем

$$(p^{k_i}a_i)\,\varphi = \sum_j \alpha_{ij}(\varphi)\,(p^{k_j}a_j), \tag{1}$$

где $\alpha_{ij}(\varphi)$ — подходящие целые числа. Понятно, что

$$\alpha_{ij}(\varphi) = \beta_{ij}(\varphi)\,p^{\max(k_i,k_j)-k_j},$$

где $\beta_{ij}(\varphi)$ — тоже целые числа. Пусть

$$\alpha^*_{ij}(\varphi) = \beta_{ij}(\varphi)\,p^{\max(k_i,k_j)-k_i}.$$

Простое матричное вычисление показывает, что $\alpha^* = \delta^{-1}\alpha\delta$, где

$$\alpha = (\alpha_{ij}(\varphi)), \quad \alpha^* = (\alpha^*_{ij}(\varphi)), \quad \delta = \operatorname{diag}(p^{k_1}, \ldots, p^{k_r}).$$

Если теперь $\varphi \in \Phi$ и $\varphi^{p^s} = 1$, то $\alpha^{p^s} \equiv \varepsilon$ по модулю

ковра идеалов

$$\begin{pmatrix} (p^{m_1}) & \dots & (p^{m_r}) \\ \dots & \dots & \dots \\ (p^{m_1}) & \dots & (p^{m_r}) \end{pmatrix}.$$

Сопрягая это соотношение матрицей δ, видим, что $(\alpha^*)^{p^s} \equiv \equiv \varepsilon$ по модулю транспонированного ковра

$$\begin{pmatrix} (p^{m_1}) & \dots & (p^{m_1}) \\ \dots & \dots & \dots \\ (p^{m_r}) & \dots & (p^{m_r}) \end{pmatrix}.$$

Следовательно, возводя матрицу $(\alpha^*)^{p^s}$ в p^m-ю степень, мы получим единичную матрицу по модулю p^m (ср. с доказательством 14.2.2). Это означает, что α^* — матрица конечного порядка; в частности, она обратима. Матрица α^* определяет автоморфизм φ^* «однородной» группы A^* по формуле

$$a_i\varphi^* = \sum_j \alpha_{ij}^*(\varphi)\, a_j.$$

Из (1) видно, что φ^* продолжает φ с подгруппы A на всю группу A^*. Более того, если φ^*, ψ^* — какие-нибудь продолжения автоморфизмов φ, ψ из Φ, то $\varphi^*\psi^*$ — продолжение автоморфизма $\varphi\psi$, а потому, по тем же соображениям, что и выше, оно является p-элементом. Значит, совокупность Φ^* всех φ^*, взятых по всем $\varphi \in \Phi$,— p-группа автоморфизмов группы A^*. Ввиду 25.1.3 ранг группы Φ^* не превосходит $\theta(r)$, а потому и ранг ее гомоморфного образа Φ не может превосходить этого числа.

25.2. Перенос с абелевых подгрупп на разрешимую группу. Здесь будет доказана следующая основная

25.2.1. Теорема (М. И. Каргаполов). *Всякая разрешимая группа, у которой ранги абелевых подгрупп конечны, сама имеет конечный ранг.*

Доказывать теорему мы будем в такой форме (учитывая индуктивные соображения, изложенные в предыдущем параграфе в связи с теоремами 24.2.2 и 24.2.3):

25.2.2. Теорема. *Пусть A — абелева нормальная подгруппа группы G. Если ранги абелевых подгрупп группы*

G конечны, то ранги абелевых подгрупп группы G/A тоже конечны.

Начнем с лемм.

25.2.3. Л е м м а. *Пусть A — периодическая абелева нормальная подгруппа группы G. Если A имеет конечный ранг, а G/A содержит свободную абелеву подгруппу счетной степени, то и G содержит свободную абелеву подгруппу счетной степени.*

Д о к а з а т е л ь с т в о. Пусть x_1A, x_2A, . . . — счетная база свободной абелевой подгруппы группы G/A и $A_{ij} = \text{гр}\,(x_i,\ x_j)$. Согласно 3.2.2 коммутант A'_{ij} группы A_{ij} порождается всевозможными элементами, сопряженными с коммутатором $[x_i,\ x_j]$. Так как все они лежат в A, а абелева группа конечного ранга и конечного периода конечна (учесть 10.1.16), то A'_{ij} конечен. Согласно 3.1.4 индекс его централизатора в A_{ij} должен быть конечен, поэтому A'_{ij} централизуется некоторым элементом $x_j^{n_{ij}}$, $n_{ij} > 0$. В частности,

$$[x_i,\ x_j^{n_{ij}},\ x_j^{n_{ij}}] = 1,$$

откуда индукцией по m (с использованием коммутаторных соотношений из § 3) получается, что

$$[x_i,\ x_j^{n_{ij}m}] = [x_i,\ x_j^{n_{ij}}]^m, \quad m = 1, 2, \ldots$$

В частности, при $m = |A'_{ij}|$ имеем $[x_i,\ x_j^{n_{ij}m}] = 1$. Положим

$$m_{ij} = n_{ij}\,|A'_{ij}|, \quad m_1 = 1 \text{ и } m_j = m_{1j}m_{2j}\ldots m_{j-1,\,j}$$

при $j > 1$. Ясно, что $\text{гр}\,(x_1^{m_1},\ x_2^{m_2},\ \ldots)$ — свободная абелева группа счетной степени. Лемма доказана.

Обратимся теперь к локально конечным группам. Прежде всего, нам понадобится лемма 24.3.1, которую удобно переформулировать так:

25.2.4. Л е м м а. *Локально конечная p-группа, у которой ранги всех абелевых подгрупп конечны, является разрешимой черниковской группой.*

Действительно, для абелевых p-групп условие конечности ранга и условие min совпадают (см. 24.1.8).

25.2.5. Л е м м а. *Пусть G — локально конечная группа, у которой ранги абелевых подгрупп конечны, p — простое число. Тогда:*

а) *ранги силовских p-подгрупп группы G конечны и ограничены в совокупности,*

б) *ранги p-секций группы G не превосходят s_p, где s_p — максимум рангов силовских p-подгрупп группы G,*

в) $s_p \leqslant \frac{1}{2}(5a_p + 1)a_p$, *где a_p — максимум рангов абелевых p-подгрупп группы G.*

Доказательство. а) По лемме 25.2.4 ранги всех силовских p-подгрупп группы G конечны; покажем, что они ограничены в совокупности. Пусть, напротив, существует последовательность конечных p-подгрупп P_1, P_2, ... неограниченных рангов. Тогда найдется аналогичная последовательность, для которой каждое $Q_i = \text{гр}(P_1, \ldots, P_i)$ — p-группа. В самом деле, если $P_1, \ldots, P_i$ уже подобраны так, что Q_i — p-группа, то некоторая сопряженная с P_{i+1} подгруппа лежит в той же силовской p-подгруппе группы Q_{i+1}, что и Q_i (по теореме Силова 11.1.1, примененной к конечной группе Q_{i+1}). Если теперь заменить P_{i+1} на эту сопряженную с ней подгруппу, то Q_{i+1} также будет p-группой. Подправленные таким способом $P_1, P_2, \ldots$ порождают p-подгруппу. По лемме 25.2.4 ее ранг конечен, однако ранги подгрупп P_1, P_2, ... не ограничены,— противоречие.

б) Ясно, что достаточно ограничиться рассмотрением конечных p-секций группы G. Если L/M — такая секция, то $L = XM$, где X — конечная подгруппа. Пусть P — ее силовская p-подгруппа. Так как при гомоморфизме $X \to XM/M$ силовская p-подгруппа отображается на силовскую p-подгруппу (см. 11.3.4), то

$$L = XM = PM, \tag{2}$$

откуда

$$\text{ранг } L/M \leqslant \text{ранг } P \leqslant s_p.$$

в) Пусть P — силовская p-подгруппа группы G ранга s_p. Так как P черниковская (см. 25.2.4), то она содержит такую максимальную абелеву нормальную подгруппу M, что P/M — конечная p-группа. Далее, P является ZA-группой (см. доказательство леммы 24.3.1), поэтому, ввиду 22.1.7, P/M изоморфно вкладывается в $\mathrm{Aut}\, M$. Так как ранг M не превосходит a_p, то ввиду 25.1.5

$$\text{ранг } P/M \leqslant \theta(a_p) = \frac{1}{2}(5a_p - 1)a_p.$$

Наконец, ввиду 4.1.7

$$s_p \leqslant a_p + \theta(a_p) = \frac{1}{2}(5a_p + 1)\, a_p.$$

Лемма доказана.

25.2.6. Упражнение. В условиях леммы 25.2.5 каждая p-секция группы G — черниковская группа.

25.2.7. Лемма. *Пусть G — локально конечная группа, A — ее нормальная подгруппа, являющаяся прямым произведением своих силовских подгрупп, а G/A абелева. Если ранги абелевых подгрупп группы G конечны, то G сама имеет конечный ранг.*

Доказательство. а) Можно считать, что силовские подгруппы S_p/A группы G/A по каждому простому числу p конечны. В самом деле, согласно 25.2.6 каждая группа S_p/A черниковская, а потому ее ранг совпадает с рангом нижнего слоя S_p^*/A, т. е. максимальной подгруппы периода p. Если мы докажем, что ранг группы

$$G^* = \text{гр}\,(S_p^* |\ p \text{ — простое число})$$

конечен, то это будет означать конечность рангов групп A и G^*/A, а потому и G/A (см. 2.3.4) и, значит, всей группы G.

б) Силовские подгруппы группы G (а также любой ее подгруппы) сопряжены. В самом деле, каждая силовская p-подгруппа G_{pi} группы G должна содержать (единственную) силовскую p-подгруппу A_p группы A. Так как G_{pi}/A_p конечна, то $G_{pi} = X_{pi}A_p$, где X_{pi} — конечная p-группа (см. выше доказательство формулы (2)). Если Y_{pi}, Y_{pj} — силовские p-подгруппы конечной группы $\text{гр}\,(X_{pi}, X_{pj})$, содержащие X_{pi}, X_{pj} соответственно, то

$$G_{pi} = Y_{pi}A_p, \quad G_{pj} = Y_{pj}A_p,$$

поэтому, по теореме Силова 11.1.1, G_{pi} и G_{pj} сопряжены в G.

в) Достаточно доказать, что $G = TA$ для некоторой подгруппы T, являющейся прямым произведением своих силовских подгрупп T_p. Действительно, если H_p — абелева подгруппа наибольшего ранга группы T_p, то все такие H_p порождают абелеву подгруппу, которая должна иметь конечный ранг, скажем, r. По лемме 25.2.5.в) ранг каждой T_p не превосходит $\frac{1}{2}(5r + 1)\, r$, а потому ранг T

конечен (см. 2.3.4). По тем же соображениям ранг A и, значит, ранг всей группы G также конечен.

г) Построение требуемой T.

Пусть $p_1 = 2$, $p_2 = 3, \ldots$ — последовательность простых чисел, S_i/A — силовская p_i-подгруппа группы G/A. Рассмотрим две последовательности подгрупп

$$G = N_0 \geqslant N_1 \geqslant \ldots$$

и

$$P_1, P_2, \ldots,$$

где P_{i+1} — силовская p_{i+1}-подгруппа группы N_i,

$$N_{i+1} = N_{N_i}(P_{i+1}),$$

и покажем, что $G = N_iA$ для всех $i = 0, 1, 2, \ldots$ Для $i = 0$ это тривиально; перейдем от i к $i + 1$. Очевидно, P_{i+1} — силовская p_{i+1}-подгруппа пересечения $N_i \cap S_{i+1}$, нормального в N_i, поэтому, по обобщенной лемме Фраттини 17.1.9,

$$N_i = N_{i+1}(N_i \cap S_{i+1}).$$

Но

$$N_i \cap S_{i+1} = P_{i+1}(N_i \cap A),$$

поскольку секция $(N_i \cap S_{i+1})/(N_i \cap A)$ — конечная p-группа (см. вывод формулы (2)). Отсюда

$$N_i = N_{i+1}(N_i \cap A)$$

и $G = N_iA = N_{i+1}A$, как и требовалось.

Согласно 25.2.6 группа P_i удовлетворяет условию min, поэтому ряд ее подгрупп

$$N_1 \cap P_i \geqslant N_2 \cap P_i \geqslant \ldots$$

обрывается, т. е.

$$N_{k(i)} \cap P_i = N_{k(i)+1} \cap P_i = \ldots$$

для некоторого $k(i) \geqslant i$; обозначим эти пересечения T_i. Если $k \geqslant k(i)$ и P — произвольная p_i-подгруппа группы N_k, то P нормализует подгруппу P_i (так как $N_k \leqslant N_{k(i)} \leqslant N_i$), поэтому

$$P \leqslant N_k \cap P_i = T_i$$

и, значит, T_i — единственная силовская p_i-подгруппа

группы N_k. Отсюда следует, что $[T_i, T_j] = 1$ при $i \neq j$ и, значит, подгруппа

$$T = \text{гр}\,(T_1, T_2, \ldots)$$

— прямое произведение ее силовских подгрупп $T_1, T_2, \ldots$

Группа T — искомая. В самом деле, осталось убедиться только, что $G = TA$. Так как $G = \text{гр}\,(S_1, S_2, \ldots)\,A$, то для этого достаточно установить равенства $S_i = T_iA$. Но

$$S_i = (N_kA) \cap S_i = (N_k \cap S_i)\,A,$$

и если $k \geqslant k\,(i)$, то

$$N_k \cap S_i = T_i\,(N_k \cap A)$$

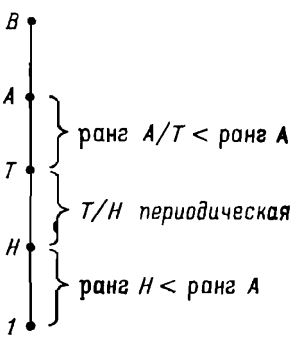
(см. вывод формулы (2)). Следовательно, $S_i = T_iA$. Лемма доказана.

Доказательство теоремы 25.2.2. Очевидно, достаточно дать доказательство только в двух крайних случаях, когда A — периодическая подгруппа и когда A не имеет кручения, так как в общем случае можно подняться по матрёшке $1 \leqslant A_0 \leqslant A$, где A_0 — периодическая часть группы A.

Предположим сначала, что A периодическая, и покажем, что ранги абелевых подгрупп группы G/A конечны. Пусть, напротив, G/A содержит абелеву подгруппу B/A бесконечного ранга. По лемме 25.2.7 ее периодическая часть B_0/A должна иметь конечный ранг, а потому группа без кручения B/B_0 должна быть бесконечного ранга. Тогда B/B_0 имеет и бесконечную размерность над $\mathbb{Z}$ (иначе она вкладывалась бы в конечную прямую сумму $\mathbb{Q} \oplus \ldots \ldots \oplus \mathbb{Q}$, ранг которой конечен), а потому содержит свободную абелеву подгруппу счетной степени. По лемме 25.2.3, примененной последовательно к парам B/A, B_0/A и B, A, такую подгруппу должна содержать сама B. Но это противоречит конечности рангов абелевых подгрупп группы G.

Теперь разберем второй случай: подгруппа A не имеет кручения. Покажем, что в этом случае всякая абелева подгруппа B/A группы G/A также имеет конечный ранг Мы будем следовать той схеме и тем обозначениям, какие применялись выше для доказательства теорем 24.2.2 и 24.2.3 (см. стр. 239). Если $[A, B] = 1$, то, согласно этой

схеме, достаточно убедиться, что ранг группы $\mathrm{Hom}\,(M/A, A)$ конечен. Так как M/A и A — абелевы группы конечного ранга, причем A без кручения, то группа $\mathrm{Hom}\,(M/A, A)$ изоморфна подгруппе аддитивной группы (прямоугольных) матриц над полем $\mathbb{Q}$, а потому действительно имеет конечный ранг. В общем случае воспользуемся индукцией по рангу группы A (при $A = 1$ утверждение тривиально). Предположим сначала, что A max-приводима относительно B, т. е. содержит неединичную B-допустимую подгруппу H с непериодической фактор-группой A/H. Пусть T/H — периодическая часть группы A/H. Так как в абелевых группах конечного ранга без кручения ранг совпадает с размерностью, а при факторизации размерности складываются (см. 7.2.2), то картина такова:



Поднимаясь по матрёшке $1 \leqslant H \leqslant T \leqslant A$, мы видим, что ранг группы B/A конечен. Пусть теперь A max-неприводима относительно B. Можно считать, далее, что $[A, B] \neq 1$, так как противоположный случай уже разобран. Тогда по лемме 24.2.1.б) существует такая подгруппа X, что

$$|B : XA| < \infty \quad \text{и} \quad X \cap A = 1.$$

Так как подгруппа $X \simeq XA/A$ абелева, то она, а потому и подгруппы XA и B имеют конечные ранги. Но тогда и B/A должна иметь конечный ранг. Теорема доказана.

25.3. О локально разрешимых группах. Как уже отмечалось в начале п. 24.3, в отличие от теоремы 24.2.2 ни теорема 24.2.3, ни теорема 25.2.1 на локально разрешимые группы не переносятся — это показывает пример, который мы сейчас изложим.

25.3.1. Пример (Ю. И. Мерзляков). Существуют локально полициклические группы без кручения, у которых ранги всех абелевых секций конечны, но уже ранги абелевых подгрупп не ограничены в совокупности.

Для построения таких групп введем понятие $\varkappa$-деформации. Мы будем рассматривать тройки (G, A, a), где G — группа, A — ее нормальная подгруппа конечного индекса, являющаяся свободной абелевой группой конечной положительной степени (так что в данном случае степень свободы совпадает с рангом группы), a — отмеченная в ней база. Пусть $\varkappa$ — кортеж попарно взаимно простых натуральных чисел, длина которого совпадает с рангом группы A, k — произведение чисел из $\varkappa$. Обозначим через $A^{\varkappa}$ подгруппу, порожденную элементами из a, возведенными в соответствующие степени из $\varkappa$, а через A^k — подгруппу k-х степеней элементов из A.

Пусть Φ_k — круговой многочлен порядка k,

$$\Phi_k(x) = x^n - c_1 x^{n-1} - \ldots - c_n.$$

Здесь $n = \varphi(k)$, φ — функция Эйлера. Матрица

$$\zeta_k = \begin{pmatrix} c_1 & c_2 & c_3 & \ldots & c_{n-1} & c_n \\ 1 & 0 & & & & \\ & 1 & 0 & & & \\ & & \ddots & & & \\ & & & & 0 & \\ & & & & 1 & 0 \end{pmatrix}$$

имеет своим характеристическим многочленом Φ_k, поэтому порождает в группе $GL_n(\mathbb{Z})$ циклическую подгруппу порядка k.

Так как $A/A^{\varkappa}$ — тоже циклическая группа порядка k, то существует ее точное представление степенями матрицы ζ_k. Пусть σ — композиция этого представления с естественным гомоморфизмом $A \to A/A^{\varkappa}$. Так как индекс $m = |G : A|$ конечен, то представление $\sigma\colon A \to GL_n(\mathbb{Z})$ индуцирует представление $\bar{\sigma}\colon G \to GL_{mn}(\mathbb{Z})$ по следующему правилу (см. конец п. 17.2): берем какие-нибудь представители $u_1, \ldots, u_m$ в смежных классах G по A и полагаем $g^{\bar{\sigma}} = ((u_i^{-1} g u_j)^{\sigma})$ для $g \in G$; здесь $x^{\sigma} = 0$ при $x \notin A$.

Возьмем теперь свободную абелеву группу $B \simeq \mathbb{Z}^{mn}$ и будем считать, что $\bar{\sigma}\colon G \to \operatorname{Aut} B$. Пусть $G^* = GB$ —

расширение группы B посредством группы G, действующей на B в силу $\overline{\sigma}$. Очевидно, подгруппа $A^* = A^k B$ нормальна в G^*, имеет в ней конечный индекс и является свободной абелевой группой конечного ранга. Отметим в ней базу a^*, начинающуюся с k-х степеней соответствующих элементов из a. Тройка (G^*, A^*, a^*) называется *$\varkappa$-деформацией* тройки (G, A, a); символическая запись

$$(G, A, a) \overset{\varkappa}{\rightsquigarrow} (G^*, A^*, a^*). \tag{3}$$

25.3.2. Упражнение. Доказать, что если $a \in A$ и $a^g \notin A^\varkappa$ для всех $g \in G$, то $C_B(a) = 1$.

25.3.3. Лемма. *Если составное натуральное число k делится на некоторое простое число, но не делится на его квадрат, то* $\det(1 - \zeta_k) = 1$.

Доказательство. Прибавив в матрице $1 - \zeta_k$ к первому столбцу остальные и разложив определитель полученной матрицы по ее первому столбцу, мы видим, что $\det(1 - \zeta_k) = \Phi_k(1)$ (при произвольном k). Воспользуемся теперь формулой

$$x^k - 1 = \prod_{d|k} \Phi_d(x)$$

(см., например, [6], стр. 154). Пусть $k = pl$, где p — простое число, не делящее l. Тогда

$$x^k - 1 = (x^l - 1) \cdot \prod_{d|l} \Phi_{pd}(x).$$

В частности, если число l простое, то

$$x^{l(p-1)} + x^{l(p-2)} + \ldots + x^l + 1 = \Phi_p(x)\,\Phi_k(x).$$

Положив здесь $x = 1$, получим $\Phi_k(1) = 1$. В общем случае рассуждаем точно так же, но с применением индукции по числу делителей числа l.

25.3.4. Лемма. *Пусть k — натуральное число, свободное от квадратов, t — произвольное натуральное число. Матрица ζ_k^t сопряжена в группе $GL_{\varphi(k)}(\mathbb{C})$ с тензорным произведением $\zeta_{k/d} \otimes 1_{\varphi(d)}$, где $d = (k, t)$, 1_m — единичная матрица степени m. Если при этом число k/d составное, то* $\det(1 - \zeta_k^t) = 1$.

Доказательство. Прежде всего,

$$\zeta_k \sim \operatorname{diag}(\varepsilon_1, \ldots, \varepsilon_{\varphi(k)}),$$

где $\sim$ обозначает сопряженность в $GL_{\varphi(k)}(\mathbb{C})$, а по диагонали выписаны все примитивные корни k-й степени из 1. Ясно, что если $d = 1$, то $\zeta_k^t \sim \zeta_k$. Пусть теперь $d > 1$ и $k = dk_1$, $t = dt_1$. Легко видеть, что

$$\zeta_k^d \sim \zeta_{k_1} \otimes 1_{\varphi(d)}.$$

Возводя обе части этого соотношения в i_1-ю степень и учитывая предыдущее замечание, получаем первое из доказываемых утверждений. Второе утверждение легко вытекает из первого, если учесть лемму 25.3.3.

Приступим к построению групп, о которых говорится в примере 25.3.1.

а) Построение требуемых групп. Прежде всего, занумеруем в последовательность $\nu_1, \nu_2, \ldots$ все последовательности целых чисел, стабилизирующие на нуле. Пусть G_1 — произвольная полициклическая почти абелева группа без кручения, A_1 — ее свободная абелева подгруппа конечного индекса, $\mathfrak{a}_1$ — какая-нибудь база группы A_1. Отправляясь от тройки $(G_1, A_1, \mathfrak{a}_1)$, мы построим последовательность деформаций

$$(G_1, A_1, \mathfrak{a}_1) \overset{\varkappa_1}{\rightsquigarrow} \cdots \rightsquigarrow (G_n, A_n, \mathfrak{a}_n) \overset{\varkappa_n}{\rightsquigarrow} \cdots,$$

а затем перейдем к ее «пределу». Именно, пусть тройка $(G_n, A_n, \mathfrak{a}_n)$ уже построена, и пусть $\mathfrak{a}_n^{\nu_i}$ обозначает произведение элементов базы $\mathfrak{a}_n$, возведенных в соответствующие степени из ν_i (компоненты с номерами, большими длины $\mathfrak{a}_n$, не используются). Легко сообразить, что множество элементов

$$(\mathfrak{a}_n^{\nu_i})^g,\ g \in G_n,\ i = 1, 2, \ldots, n, \tag{4}$$

конечно. Возьмем в качестве $\varkappa_n$ кортеж попарно взаимно простых чисел, свободных от квадратов, с условием, что группа $A_n^{\varkappa_n}$ не содержит ни элементов (4), отличных от единицы, ни их степеней с простыми показателями (для выполнения этого условия достаточно потребовать, например, чтобы все числа из $\varkappa_n$ были составными, а их простые делители были больше, чем модули координат элементов (4) в базе $\mathfrak{a}_n$). Теперь построение $(n+1)$-й тройки производится на основе определения $\varkappa_n$-деформации,

т. е.

$$G_{n+1} = G_n B_n, \quad A_{n+1} = A_n^{k_n} B_n \tag{5}$$

и $\mathfrak{a}_{n+1}$ — какая-нибудь база группы A_{n+1}, начинающаяся с k_n-х степеней соответствующих элементов из $\mathfrak{a}_n$. Здесь k_n, B_n имеют тот же смысл, какой имели k, B при определении деформации (3).

Пусть G_∞ — *предельная деформация* тройки $(G_1, A_1, \mathfrak{a}_1)$ относительно последовательности кортежей $\varkappa_1, \varkappa_2, \ldots$, т. е. объединение последовательности вложенных друг в друга групп $G_1 \leqslant G_2 \leqslant \ldots$ Мы покажем, что группа G_∞ искомая. Действительно, учитывая (5), легко убеждаемся индукцией по n, что все группы G_n полициклические, без кручения и имеют конечные ранги. Таким образом, группа G_∞ локально полициклическая, не имеет кручения и содержит абелевы подгруппы A_n неограниченно растущих рангов. Остается проверить, что ранги абелевых секций группы G_∞ конечны.

б) Для всякого неединичного элемента h группы G_∞ существует такое натуральное число $n(h)$, что для всякого $n \geqslant n(h)$ найдется элемент $a_n \in \text{гр}\,(h) \cap A_n$, ни в какой простой степени не попадающий в подгруппы $(A_n^{\varkappa_n})^g$, $g \in G_n$. Именно, если $h \in G_s$ и $h^{|G_s : A_s|} = \mathfrak{a}_s^{\nu_t}$, причем ν_t содержит нули на всех местах, начиная с $(|\mathfrak{a}_s| + 1)$-го, то можно взять $n(h) = \max(s, t)$. В самом деле, пусть $n \geqslant s, t$ и

$$a_n = h^{|G_s : A_s| \cdot k_s k_{s+1} \ldots k_{n-1}}.$$

Очевидно, $a_n = \mathfrak{a}_n^{\nu_t} \in A_n$. С другой стороны, так как $t \leqslant n$ то по построению кортежа $\varkappa_n$ для всякого простого числа p выполняется соотношение

$$a_n^p = (\mathfrak{a}_n^{\nu_t})^p \notin (A_n^{\varkappa_n})^g, \qquad g \in G_n.$$

в) Приступим непосредственно к доказательству конечности рангов абелевых секций группы G_∞. Пусть H — неединичная подгруппа группы G_∞, H' — ее коммутант. Достаточно убедиться, что

$$\text{ранг}\, H/H' \leqslant \text{ранг}\, G_{n(H)},$$

где $n(H) = \min n(h)$ по всем $h \in H$, $h \neq 1$. Пусть $n(H) = l$. Достаточно доказать, что ранг любой конечно порож-

денной подгруппы группы H/H' не превосходит ранга группы G_l, поэтому, не ограничивая общности, можно считать, что сама H конечно порождена и по-прежнему содержит h_0, для которого $n(h_0) = 1$. В частности, $H \leqslant G_s$ при достаточно большом $s \geqslant 2$.

Так как $G_s = G_l B_l B_{l+1} \ldots B_{s-1}$, то G_s обладает конечной нормальной матрёшкой

$$G_s = D_{l-1} > D_l > \ldots > D_s = 1,$$

где

$$D_n = B_n B_{n+1} \ldots B_{s-1}, \quad n = l, l+1, \ldots, s-1.$$

Эта матрёшка индуцирует в H матрёшку

$$H = H_{l-1} \geqslant H_l \geqslant \ldots \geqslant H_s = 1, \text{ где } H_n = H \cap D_n,$$

а в H/H' — матрёшку

$$H/H' = \overline{H}_{l-1} \geqslant \overline{H}_l \geqslant \ldots \geqslant \overline{H}_s = 1, \text{ где } \overline{H}_n = H_n H'/H'.$$

Мы покажем, что на самом деле $\overline{H}_n/\overline{H}_{n+1} = 1$ при $n = l, l+1, \ldots, s-1$, т. е. $\overline{H}_l = 1$ и $H/H' \simeq \overline{H}_{l-1}/\overline{H}_l$. Так как $\overline{H}_{l-1}/\overline{H}_l$ — секция группы $D_{l-1}/D_l \simeq G_l$, то это и даст требуемую оценку: ранг $H/H' \leqslant$ ранг G_l.

г) Итак, пусть $l \leqslant n < s$. Применив дважды теорему 4.2.4, получим

$$\begin{aligned}\overline{H}_n/\overline{H}_{n+1} &\simeq H_n H'/H_{n+1}H' \simeq H_n/H_{n+1}(H_n \cap H') = \\ &= (H \cap D_n)/(H' \cap D_n)(H \cap D_{n+1}) \simeq \\ &\simeq (H \cap D_n) D_{n+1}/(H' \cap D_n) D_{n+1} \simeq \\ &\simeq (H \cap D_n)^{\pi_n}/(H' \cap D_n)^{\pi_n},\end{aligned}$$

где π_n — естественная проекция $D_n \to B_n$. Обозначим для краткости

$$L = (H \cap D_n)^{\pi_n}, \quad M = (H' \cap D_n)^{\pi_n};$$

осталось доказать, что $L = M$. При $L = 1$ утверждение очевидно, поэтому предположим, что $L \neq 1$.

Пусть $b \in L$, $b = h^{\pi_n}$, $h \in H \cap D_n$, т. е.

$$h \equiv b \pmod{D_{n+1}}, \quad b \in B_n.$$

Так как $n(h_0) = l$ (см. начало пункта в)), то существует такой элемент $h_n \in \text{гр}(h_0) \cap A_n$, что

$$h_n^p \notin (A_n^{\varkappa_n})^g$$

для любого простого числа p и любого $g \in G_n$.

Заметим, что

$$(h_n^{-1}hh_n)^{-1}h = [h_n, h] \in H' \cap D_n \tag{6}$$

и

$$h_n^{-1}hh_n \equiv h_n^{-1}bh_n \pmod{D_{n+1}}.$$

Если $u_1, \ldots, u_m$ — представители смежных классов группы G_n по подгруппе A_n, то, согласно построению группы G_{n+1},

$$h_n^{-1}bh_n = b\hat{h}_n,$$

где элемент b записан строкой из $\mathbb{Z}^{m\cdot\varphi(k_n)}$, линейное преобразование $\hat{h}_n$ — матрицей

$$\operatorname{diag}((u_1^{-1}h_nu_1)^\sigma, \ldots, (u_m^{-1}h_nu_m)^\sigma)$$

и σ — композиция естественного гомоморфизма $A_n \to$ $\to A_n/A_n^{k_n}$ с последующим изоморфизмом на группу (ζ_{k_n}). Ввиду (6)

$$[h_n, h] \equiv b(1 - \hat{h}_n) \pmod{D_{n+1}}. \tag{7}$$

По лемме 25.3.4 определители клеток $1 - (u_i^{-1}h_nu_i)^\sigma$ равны 1, поэтому

$$\det(1 - \hat{h}_n) = 1.$$

По теореме 8.1.1 свободные абелевы группы B_n, L обладают согласованными базами

$$b_1, \ldots, b_r, b_{r+1}, \ldots, b_t, \tag{8}$$

$$m_1b_1, \ldots, m_rb_r, \tag{9}$$

где m_j — целые числа, отличные от нуля. Так как L $\hat{h}_n$-допустима, то преобразование $1 - \hat{h}_n$ переводит базу (9) в ее линейную $\mathbb{Z}$-оболочку, а потому группу $L^* =$ $=$ гр $(b_1, \ldots, b_r)$ — в себя. Мы видим, что оно записывается в базе (8) полураспавшейся целочисленной матрицей, поэтому

$$\det(1 - \hat{h}_n)|_L = \det(1 - \hat{h}_n)|_{L^*} = \pm 1.$$

Значит,

$$L\hat{h}_n(1 - \hat{h}_n) = L.$$

Отсюда и из (6), (7) вытекает, что $L = M$. Доказательство закончено.

Отметим, что группы G_∞ обладают и другими любопытными свойствами:

25.3.5. *Каждая из групп G_∞ локально разрешима, но не обладает свойством RN^*, поскольку каждая ее RN^*-подгруппа (в частности, каждая абелева подгруппа) содержится в некоторой G_n.*

Доказательство. а) Нормализаторы и централизаторы в G_∞. Покажем прежде всего, что

$$N_{G_{n+1}}(M) = N_{G_n}(M)\, C_{B_n}(M) \text{ для } M \leqslant G_n. \qquad (10)$$

Действительно, пусть элементы $g \in G_n$, $b \in B_n$ таковы, что $M^{gb} = M$. Так как $[M, b^{-1}] \leqslant B_n$, а с другой стороны

$$[M, b^{-1}] \leqslant M^{-1}M^{b^{-1}} = M^{-1}M^g \leqslant G_n,$$

то $[M, b^{-1}] = 1$. Отсюда $b \in C_{B_n}(M)$, $g \in N_{G_n}(M)$, что и требовалось.

Далее, ввиду 25.3.2 и выбора кортежа $\varkappa_n$

$$C_{B_n}(a_n^{\nu_i}) = 1 \text{ при } a_n^{\nu_i} \neq 1, \quad i \leqslant n. \qquad (11)$$

б) Пусть H — неединичная подгруппа группы G_∞, через которую проведена трансфинитно возрастающая субнормальная последовательность

$$H = H_0 < H_1 < \ldots < H_\alpha < \ldots < H_\gamma,$$

т. е. $H_\alpha \lhd H_{\alpha+1}$ для всех трансфинитных чисел $\alpha < \gamma$ и $H_\alpha = \bigcup\limits_{\beta<\alpha} H_\beta$ для предельных $\alpha \leqslant \gamma$. Если H содержится в некотором G_s, то существует такой номер $n = n_H$, что $H_\gamma \leqslant G_n$.

Действительно, пусть a — неединичный элемент пересечения $H_s \cap A_s$. Пусть он имеет в базе $\mathfrak{a}_s$ координаты $u_1, \ldots, u_r$, а последовательность $\nu = (u_1, \ldots, u_r, 0, \ldots)$ имеет номер t, т. е. $\nu = \nu_t$. Покажем, что число $n = \max(s, t)$ искомое, т. е. $H_\gamma \leqslant G_n$. Пусть уже доказано, что $H_\beta \leqslant G_n$ для всех $\beta < \alpha \leqslant \gamma$, и докажем, что $H_\alpha \leqslant G_n$. Для предельного α это очевидно. Пусть α — непредельное трансфинитное число. Достаточно проверить, что

$$N_{G_{l+1}}(H_{\alpha-1}) = N_{G_l}(H_{\alpha-1}) \text{ при } l \geqslant n$$

или, ввиду (10), что

$$C_{B_l}(H_{\alpha-1}) = 1 \text{ при } l \geqslant n. \tag{12}$$

Но

$$C_{B_l}(H_{\alpha-1}) \leqslant C_{B_l}(a) \leqslant C_{B_l}(a^{k_s \ldots k_{l-1}}). \tag{13}$$

Ввиду выбора отмеченных баз $a^{k_s \ldots k_{l-1}} = a_l^v$, поэтому из (13) и (11) вытекает (12).

Все утверждения предложения 25.3.5 теперь очевидны.

Примеры примерами, но некоторое недоумение все же остается: почему из трех параллельных по формулировке и схеме доказательства теорем 24.2.2, 24.2.3 и 25.2.1 первая допускает обобщение на локально разрешимые группы, а две другие нет? Это недоумение полностью рассеивается, если учесть следующую важную теорему Ю. М. Горчакова (ДАН СССР, 1964, **156**, № 1, с. 17—20): *всякая периодическая локально разрешимая группа, у которой ранги абелевых подгрупп конечны, сама имеет конечный ранг.* Таким образом, параллелизм — и с ним душевный покой — восстанавливается очень просто: на п е р и о д и ч е с к и е локально разрешимые группы переносятся все три обсуждаемые теоремы (разберите сами несложный оставшийся случай теоремы 24.2.3), а на группы без кручения не переносится ни одна из них. Правда, вы можете возразить, что семейство групп с условием min для абелевых подгрупп содержит одни лишь периодические группы, а групп без кручения и даже смешанных групп в нем нет, но тут уж ничего не поделаешь — таковы его суровые семейные нравы, заложенные в самом определении.

ВСПОМОГАТЕЛЬНЫЕ СВЕДЕНИЯ ИЗ АЛГЕБРЫ, ЛОГИКИ И ТЕОРИИ ЧИСЕЛ

§ 26. О нильпотентных алгебрах

Упомянутая в основном тексте вскользь связь между нильпотентностью в группах и кольцах играет в действительности важную роль, обогащая как теорию групп, так и теорию колец. Мы приведем здесь некоторые сведения о нильпотентных алгебрах, необходимые при изучении энгелевых групп в п. 18.3. В первом пункте будут даны основные определения и изучено поведение нильпотентности при стандартном переходе от ассоциативных алгебр к лиевым и обратно. Второй пункт посвящен построению ненильпотентных нильалгебр.

26.1. Нильпотентность ассоциативных и лиевых алгебр. Пусть k — поле, A — кольцо (ни коммутативность, ни ассоциативность умножения в A не предполагаются). Кольцо A называется (*линейной*) *алгеброй над* k, если для всяких $\alpha \in k$, $a \in A$ определен элемент $\alpha a \in A$, причем это «умножение на скаляр» связано с операциями в k и A следующими соотношениями:

$$\begin{aligned}(\alpha + \beta)a &= \alpha a + \beta a,\\ (\alpha\beta)a &= \alpha(\beta a),\\ 1a &= a,\\ \alpha(a + b) &= \alpha a + \alpha b,\\ \alpha(ab) &= (\alpha a)b = a(\alpha b).\end{aligned}$$

Здесь α, β — любые элементы из k, 1 — единица поля k, a, b — любые элементы из A. Алгебра A называется *ассоциативной*, если

$$(ab)c = a(bc) \text{ для всех } a, b, c \in A.$$

Алгебра A называется *лиевой* (или *алгеброй Ли*), если

$$\begin{aligned}ab + ba &= 0,\\ (ab)c + (bc)a + (ca)b &= 0\end{aligned}$$

для всех $a, b, c \in A$.

Роль ассоциативности читателю объяснять не надо, а вот лиевы алгебры могут на первый взгляд показаться искусственным объектом. В действительности они столь же естественны как и ассоциативные: каждая ассоциативная алгебра имеет лиеву спутницу, получаемую следующим стандартным способом. Пусть A — ассоциативная алгебра. Если a, b — ее элементы, то элемент $(a, b) = ab - ba$ называется их (*кольцевым*) *коммутатором*. Как и в случае групп, можно сказать, что коммутатор измеряет отклонение от коммутативности, ср. с п. 3.2. Легко проверить, что множество A с от-

меченными на нем операциями сложения, коммутирования и умножения на скаляры из k будет лиевой алгеброй. Она называется лиевой алгеброй, *присоединенной* к ассоциативной алгебре A. Другой источник алгебр Ли — группы Ли — упоминался в основном тексте.

Пусть теперь в ассоциативной алгебре A выделено подпространство L, замкнутое относительно коммутирования (так что в присоединенной лиевой алгебре L будет лиевой подалгеброй). Ассоциативная подалгебра $\overline{L}$, порожденная в ассоциативной алгебре A множеством L, называется ассоциативной алгеброй, *обертывающей* лиеву алгебру L.

Элемент a линейной алгебры A называется *нильпотентным* (так сказать, «потенциально нулевым»), если $a^n = 0$ при некотором n, вообще говоря, зависящем от a, и произвольной расстановке скобок в a^n. Алгебра A называется *нильпотентной*, если существует такое n, что $a_1 \ldots a_n = 0$ для всех $a_1, \ldots, a_n \in A$ и произвольной расстановки скобок в левой части. Наименьшее n с этим свойством называется *ступенью нильпотентности*. Как упоминалось в основном тексте, примером нильпотентной ассоциативной алгебры служит алгебра треугольных матриц с нулевой диагональю.

26.1.1. Упражнение. Конечно порожденная нильпотентная алгебра конечномерна.

26.1.2. Упражнение. Лиева алгебра L тогда и только тогда нильпотентна, когда существует такое n, что $(\ldots((a_1a_2)a_3)\ldots \ldots)a_n = 0$ для всех $a_1, \ldots, a_n \in L$.

Как ведет себя нильпотентность при переходе от ассоциативных алгебр к лиевым и обратно, точнее, при операциях присоединения и обертывания? В одну сторону вопрос решается легко: понятно, что если ассоциативная алгебра A нильпотентна ступени n, то присоединенная к ней лиева алгебра нильпотентна ступени $\leqslant n$ (неравенство снять нельзя). А вот при обертывании рассчитывать на сохранение нильпотентности уже не приходится, поскольку существуют ненильпотентные ассоциативные алгебры, для которых присоединенные лиевы алгебры нильпотентны: такова, например, алгебра A всех треугольных матриц некоторой степени n с постоянными диагоналями. Другой пример — прямая сумма B однопорожденных нильпотентных алгебр неограниченно растущих ступеней нильпотентности.

Причина того, почему алгебра A не нильпотентна, бросается в глаза: даже отдельные элементы алгебры A не все нильпотентны в ассоциативном смысле. Оказывается, если потребовать ассоциативную нильпотентность элементов да еще конечную порождаемость «обертываемой» лиевой алгебры, то нильпотентность уже будет сохраняться при обертывании:

26.1.3. Теорема. *Пусть A — ассоциативная алгебра, L — ее подпространство, замкнутое относительно коммутирования. Если лиева алгебра L конечно порождена и нильпотентна, а каждый ее элемент нильпотентен в ассоциативном смысле, то обертывающая ассоциативная алгебра $\overline{L}$ нильпотентна.*

Доказательство. Пусть $e_1, \ldots, e_s$ — порождающие элементы лиевой алгебры L. Назовем их порождающими коммутаторами веса 1, а если порождающие коммутаторы c, d весов u, v

уже определены, то назовем коммутатор (c, d) порождающим коммутатором веса $u + v$ (таким образом, вес определяется не только самим элементом, но и выбранной для него записью). Пусть n — ступень нильпотентности лиевой алгебры L. Это означает, что коммутаторы веса $\geqslant n$ равны нулю, поэтому множество ненулевых порождающих коммутаторов конечно. Упорядочим их по возрастанию весов, а при одном весе — произвольным способом: $c_1, c_2, \ldots, c_r$. По условию $c_i^{n_i} = 0$ при некотором n_i. Покажем, что ассоциативная алгебра $\bar{L}$ нильпотентна ступени не более $N = n(n_1 + \ldots + n_r)$. Очевидно, для этого достаточно проверить, что все $c_{i_1} \ldots c_{i_N} = 0$.

Длиной произведения $c_{i_1} \ldots c_{i_m}$ назовем число m, *весом* — сумму весов множителей, *беспорядком* — любое вхождение $\ldots c_i \ldots c_j \ldots$ при $i > j$, *характеристикой* — пару (m, t), где t — число беспорядков. Упорядочим характеристики словарно, т. е. положим $(m, t) < (m', t')$, если $m < m'$ или $m = m'$, $t < t'$. Очевидно, любая убывающая цепочка характеристик обрывается.

Если в произведении $c_{i_1} \ldots c_{i_N}$ веса w имеется беспорядок $c_i c_j$, то после его замены на $c_j c_i + (c_i, c_j)$ мы получим сумму двух произведений того же веса, но с меньшими характеристиками. Значит, через конечное число таких замен мы придем к сумме произведений

$$c_{j_1}^{m_1} \ldots c_{j_l}^{m_l}, \text{ где } j_1 < \ldots < j_l, \text{ все } m_\alpha \geqslant 1.$$

Остается заметить, что при $w \geqslant N$ указанные произведения равны нулю. Действительно, при $w \geqslant N$ некоторое $m_\alpha \geqslant n_{j_\alpha}$, а тогда $c_{j_\alpha}^{m_\alpha} = 0$. Теорема доказана.

В заключение пункта приведем один результат о конечной порождаемости в кольцах, напоминающий упражнение 14.3.2 для групп. Хотя в его формулировке нильпотентность явно не фигурирует, этот результат служит важным вспомогательным средством при ее изучении, что оправдывает его изложение именно здесь. Впрочем, нам он понадобится для других целей (см. § 21).

Напомним, что абелева группа A по сложению называется *левым модулем* над кольцом k, если для всяких $\alpha \in k$, $a \in A$ определено $\alpha a \in A$ и выполняются первые четыре аксиомы из списка в самом начале параграфа. Аналогично определяется *правый модуль*. Если на A определено строение левого и правого модуля над k, причем $(\alpha a)\beta = \alpha(a\beta)$ для всех $\alpha, \beta \in k$, $a \in A$, то говорят о *бимодуле* над k. *Аннулятором* бимодуля A над k называется совокупность всех $\alpha \in k$ с условием

$$\alpha a = 0, \quad a\alpha = 0 \quad \text{для любого } a \in A.$$

Пусть K — ассоциативное кольцо (не обязательно коммутативное), M — его подмножество, s — натуральное число. Тогда M^s обозначает подгруппу аддитивной группы кольца K, порожденную всевозможными произведениями s элементов из M.

26.1.4. Теорема. *Пусть I — идеал конечно порожденного ассоциативного кольца K. Если аддитивная группа K/I конечно порождена, то идеал I конечно порожден и все аддитивные группы K/I^s, $s = 1, 2, \ldots$, также конечно порождены.*

Доказательство. а) Возьмем в аддитивной группе кольца K конечно порожденную подгруппу A с условием:

$$K = A + I, \text{ кольцо } K \text{ порождается множеством } A. \qquad (1)$$

Пусть I' — идеал, порожденный в K пересечением $I \cap (A + A^2)$. Сумма $A + I'$ — подкольцо. Действительно, если $a_1, a_2 \in A$, то ввиду (1) $a_1a_2 = a + i$, $a \in A$, $i \in I$. Очевидно, $i \in I'$, так что $a_1a_2 \in A + I'$.

Отсюда $K = A + I'$ (см. (1)). Так как A конечно порождена, то и аддитивная группа K/I' конечно порождена. Значит, ее подгруппа I/I' тоже конечно порождена. Из определения идеала I' видно, что он конечно порожден, так как $A + A^2$ — конечно порожденная аддитивная группа. Следовательно, идеал I конечно порожден.

б) Кольцо K действует на аддитивной группе I/I^2 левыми и правыми умножениями, превращая эту группу в бимодуль над K. Ясно, что I содержится в его аннуляторе, так что I/I^2 можно рассматривать как бимодуль над K/I, причем ввиду а) он конечно порожден. Так как аддитивная группа K/I конечно порождена, то и аддитивная группа I/I^2 конечно порождена. Индукцией по n убеждаемся, что все аддитивные группы K/I^{2^n} конечно порождены. Наконец, при произвольном s можно выбрать такое n, что $2^n > s$, поэтому и все аддитивные группы K/I^s конечно порождены. Теорема доказана.

26.2. **Ненильпотентные нильалгебры.** В этом пункте рассматриваются только ассоциативные алгебры. Если все элементы алгебры нильпотентны, она называется *нильалгеброй*. Один из центральных вопросов теории нильпотентных алгебр состоит в следующем: будет ли конечно порожденная ассоциативная нильалгебра нильпотентной? Для конечномерных алгебр давно был получен утвердительный ответ, но если не предполагать конечномерность заранее, то ответ, как показал Е. С. Голод, будет отрицательным. Более точно, Е. С. Голод для каждого поля k и каждого $d \geqslant 2$ построил ненильпотентную алгебру над полем k с d порождающими, у которой все подалгебры с $d - 1$ порождающими нильпотентны (Изв. АН СССР: Сер. матем., 1964, 28, № 2, с. 273—276). Его конструкция позволяет ответить и на ряд важных вопросов теории групп. Цель настоящего пункта — изложить эту конструкцию.

Пусть $F = k\{x_1, \ldots, x_d\}$ — кольцо многочленов над каким-нибудь полем k от неперестановочных переменных $x_1, \ldots, x_d$. Очевидно, F разлагается в прямую сумму $F_0 \oplus F_1 \oplus \ldots$, где $F_0 \simeq k$, F_n — векторное пространство над k, порожденное d^n одночленами $x_{i_1}x_{i_2}\ldots x_{i_n}$. Многочлены из F_n называются *однородными* степени n. Идеал I кольца F называется *однородным*, если он порождается однородными многочленами (вообще говоря, различных степеней).

26.2.1. Упражнение. Идеал I тогда и только тогда однороден, когда он вместе с каждым своим элементом содержит и все

его однородные компоненты, т. е. из

$$a \in I,\ a = a_{n_1} + \ldots + a_{n_s}, \qquad a_{n_i} \in F_{n_i},\ n_1 < \ldots < n_s,$$

следует, что все $a_{n_i} \in I$.

Пусть $f_1, f_2, \ldots$ — ненулевые однородные многочлены из F неубывающих степеней $\geqslant 2$, причем число r_n многочленов каждой степени n конечно. Пусть I — идеал, порожденный элементами $f_1, f_2, \ldots$, $A = F/I$. Очевидно, $A = A_0 \oplus A_1 \oplus \ldots$, где $A_n = (F_n + I)/I$. В частности, $A_0 \simeq F_0 \simeq k$, $A_1 \simeq F_1$, так как многочлены f_i имеют степени $\geqslant 2$. Основную роль в излагаемой конструкции играет фактор-алгебра F/I по некоторому идеалу I. В качестве подготовительного шага мы установим сейчас один признак ее бесконечномерности.

Рассмотрим формальный степенной ряд

$$\mathfrak{s} = 1 - dt + \sum_{n=2}^{\infty} s_n t^n,$$

где s_n — целые числа. Легко понять, что обратным к нему будет ряд $\mathfrak{s}^{-1} = \sum_{n=0}^{\infty} y_n t^n$, где

$$y_0 = 1, \quad y_1 = d,$$

$$y_n = dy_{n-1} - \sum_{i=2}^{n} s_i y_{n-i}, \qquad n = 2, 3, \ldots$$

26.2.2. Теорема (Е. С. Голод). *Пусть $F = k\{x_1, \ldots, x_d\}$ — кольцо многочленов над полем k от неперестановочных переменных $x_1, \ldots, x_d$. Пусть $f_1, f_2, \ldots$ — однородные многочлены из F неубывающих степеней $\geqslant 2$, I — порожденный ими идеал. Если число r_n многочленов степени n из $f_1, f_2, \ldots$ не превосходит числа s_n и все коэффициенты ряда $\mathfrak{s}^{-1}$ неотрицательны, то алгебра F/I бесконечномерна.*

Доказательство. а$_1$) Пусть a_n — размерность факторалгебры $A_n = (F_n + I)/I$ как векторного пространства над k. Для доказательства теоремы достаточно убедиться, что ряд

$$\mathfrak{a} = \sum_{n=0}^{\infty} a_n t^n$$

не есть многочлен. Пусть

$$\mathfrak{r} = 1 - dt + \sum_{n=2}^{\infty} r_n t^n,$$

и пусть уже доказано, что ряды $\mathfrak{r}^{-1}$ и $\mathfrak{r}\mathfrak{a}$ имеют неотрицательные

коэффициенты (мы сделаем это ниже). Так как $\mathfrak{r}^{-1}\mathfrak{r} = 1$, то

$$\mathfrak{r}^{-1}\left(1 + \sum_{n=2}^{\infty} r_n t^n\right) = 1 + \mathfrak{r}^{-1}\,dt.$$

Отсюда видно, что $\mathfrak{r}^{-1}$ не многочлен. Но тогда и $a = \mathfrak{r}^{-1}\cdot \mathfrak{r}a$ не может быть многочленом.

б) Ряд $\mathfrak{r}^{-1}$ имеет неотрицательные коэффициенты. Действительно, в силу очевидных свойств действий над формальными рядами

$$\mathfrak{r} = \mathfrak{s} - \mathfrak{q} = \mathfrak{s}\,(1 - \mathfrak{s}^{-1}\mathfrak{q}), \text{ где } \mathfrak{q} = \sum_{n=2}^{\infty} (s_n - r_n)\, t^n,$$

и, значит,

$$\mathfrak{r}^{-1} = \mathfrak{s}^{-1}\,(1 - \mathfrak{s}^{-1}\mathfrak{q})^{-1} = \mathfrak{s}^{-1}\left(1 + \sum_{m=1}^{\infty} (\mathfrak{s}^{-1}\mathfrak{q})^m\right).$$

Остается учесть, что ряды $\mathfrak{s}^{-1}$ и $\mathfrak{q}$ имеют неотрицательные коэффициенты.

в) Убедимся, что ряд $\mathfrak{r}a$ тоже имеет неотрицательные коэффициенты, т. е.

$$a_n \geqslant d a_{n-1} - \sum_{i=2}^{n} r_i a_{n-i}, \qquad n \geqslant 2. \tag{2}$$

Пусть I_n — множество всех однородных многочленов степени n из I, A_n^* — прямое дополнение подпространства I_n в пространстве F_n, т. е. $F_n = I_n \oplus A_n^*$. Сравнение размерностей дает

$$d^n = \dim I_n + a_n.$$

Пусть еще H_m — подпространство, порожденное многочленами степени m из $f_1, f_2, \ldots$, а XY обозначает подпространство, натянутое на элементы xy, $x \in X$, $y \in Y$. Мы покажем, что

$$I_n \subseteq I_{n-1}F_1 + \sum_{m=2}^{n} A_{n-m}^* H_m, \qquad n \geqslant 2. \tag{3}$$

Тогда подсчет размерностей в (3) и даст (2).

Пусть $u \in I_n$. По построению u есть сумма произведений вида vf_jw, где v, w — однородные многочлены. Будем считать, что $u = vf_jw$. Если w имеет степень $\geqslant 1$, то ясно, что $u \in I_{n-1}F_1$. Если же f имеет степень 0, то можно считать, что $u = vf_j$. Пусть f_j имеет степень m и, значит, принадлежит подпространству H_m. Тогда $v \in F_{n-m}$,

$$v = v' + v'', \quad v' \in I_{n-m}, \quad v'' \in A_{n-m}^*.$$

Отсюда $u \in I_{n-1}F_1 + A_{n-m}^* H_m$. Теорема доказана.

26.2.3. Пример. Если в условии теоремы 26.2.2

$$r_n \leqslant \varepsilon^2 (d - 2\varepsilon)^{n-2}, \quad \varepsilon > 0, \tag{4}$$

то алгебра A бесконечномерна. Действительно, достаточно проверить, что ряд $\mathfrak{s}^{-1}$ имеет неотрицательные коэффициенты, где

$$\mathfrak{s} = 1 - dt + \sum_{n=2}^{\infty} \varepsilon^2 (d - 2\varepsilon)^{n-2} t^n.$$

Мы воспользуемся следующими формулами для формальных рядов:

$$\frac{1}{1-a} = \sum_{n=0}^{\infty} a^n, \qquad \frac{1}{(1-a)^2} = \sum_{n=0}^{\infty} (n+1)\, a^n.$$

Имеем

$$\mathfrak{s} = 1 - dt + \varepsilon^2 t^2 \sum_{n=0}^{\infty} (d - 2\varepsilon)^n t^n =$$

$$= 1 - dt + \frac{\varepsilon^2 t^2}{1 - (d - 2\varepsilon)\, t} = \frac{(1 - (d - \varepsilon)\, t)^2}{1 - (d - 2\varepsilon)\, t},$$

откуда

$$\mathfrak{s}^{-1} = \frac{1 - (d - 2\varepsilon)\, t}{(1 - (d - \varepsilon)\, t)^2} = (1 - (d - 2\varepsilon)\, t) \sum_{n=0}^{\infty} (n+1)\, (d - \varepsilon)^n t^n =$$

$$= 1 + \sum_{n=1}^{\infty} (d - \varepsilon)^{n-1} (d + (n-1)\, \varepsilon)\, t^n.$$

Так как $d - 2\varepsilon \geqslant 0$, то $d - \varepsilon \geqslant \varepsilon > 0$, и всё доказано.

Теперь мы готовы к изложению конструкции Е. С. Голода. Ее идею хорошо поясняет следующий частный

26.2.4. Пример. Пусть k — не более чем счетное поле, $F = k\{x, y\}$ — алгебра многочленов над полем k от неперестановочных переменных x, y, F' — подалгебра многочленов без свободных членов. Покажем, что в алгебре F существует такой идеал I, содержащийся в F', что алгебра $A' = F'/I$ не нильпотентна, но все ее элементы (и, значит, все подалгебры с одним порождающим) нильпотентны.

Занумеруем элементы из F': $u_1, u_2, \ldots$. Пусть $N_1 = 9$. Возведем u_1 в N_1-ю степень и разложим $u_1^{N_1}$ на однородные слагаемые $f_1, f_2, \ldots, f_{m_1}$ возрастающих степеней. Пусть число N_2 превосходит любую из них. Возведем u_2 в N_2-ю степень и разложим $u_2^{N_2}$ на однородные слагаемые $f_{m_1+1}, f_{m_1+2}, \ldots$ возрастающих степеней. Продолжая этот процесс, мы построим многочлены $f_1, f_2, \ldots$ возрастающих степеней $\geqslant 9$. Пусть I — идеал, порожденный этими многочленами. Ясно, что $A' = F'/I$ — нильалгебра с порождаю-

щими $\bar{x} = x + I$, $\bar{y} = y + I$. Остается проверить, что A' не нильпотентна, а для этого достаточно убедиться, что $A = F/I$ бесконечномерна (тогда $A' = A_1 \oplus A_2 \oplus \ldots$ тоже будет бесконечномерна, а потому не нильпотентна — см. 26.1.1). В обозначениях теоремы Голода имеем $d = 2$, $r_n \leqslant 1$, причем $r_2 = r_3 = \ldots = r_8 = 0$. Прямое вычисление показывает, что при $\varepsilon = 1/4$ выполняется условие примера 26.2.3, поэтому все доказано.

Изложим теперь результат Е. С. Голода в полном объеме.

26.2.5. Пример. Для всякого $d \geqslant 2$ и всякого поля k существует ненильпотентная алгебра над k с d порождающими, каждая подалгебра которой с $d - 1$ порождающими нильпотентна. В самом деле, пусть $F = k\{x_1, \ldots, x_d\}$ — алгебра многочленов над k от неперестановочных переменных $x_1, \ldots, x_d$, F' — подалгебра многочленов без свободного члена. Построим в F такой идеал I, лежащий в F', что F'/I — искомая алгебра.

Пусть ε — фиксированное число, $0 < \varepsilon < 1/2$. Ввиду примера 26.2.3 в качестве I можно взять идеал, порожденный однородными многочленами $f_1, \ldots, f_{s_1}, f_{s_1+1}, \ldots, f_{s_2}, \ldots$ степени $\geqslant 2$ с условием (4) и следующим дополнительным условием: для любых $d - 1$ элементов из F' степени $\leqslant n$ существует такое натуральное число N, что произведение любых N множителей из данных элементов принадлежит идеалу I_n, порожденному элементами $f_1, \ldots, f_{s_n}$. Допустим, что отрезок $f_1, \ldots, f_s$, $s = s_{n-1}$, уже построен, и покажем, как дополнить его до отрезка $f_1, \ldots, f_t$, $t = s_n$.

Рассмотрим $d - 1$ многочленов степени $\leqslant n$ без свободного члена с неопределенными (буквенными) коэффициентами $c_{i\alpha}$:

$$g_i = \sum_\alpha c_{i\alpha} M_\alpha (x_1, \ldots, x_d), \quad 1 \leqslant i \leqslant d-1, \quad M_\alpha \text{ — одночлены.}$$

Пусть N — натуральное число. Существует $(d-1)^N$ различных произведений по N элементов g_i. Записав их как многочлены от $\{c_{i\alpha}\}$, мы получим в качестве коэффициентов некоторые линейные комбинации $f_{s+1}, \ldots, f_t$ одночленов от $\{x_j\}$ степени $N, N+1, \ldots, nN$. Покажем, что при достаточно большом N многочлены $f_{s+1}, \ldots, f_t$ — искомые. Ясно, что в проверке нуждается только свойство (4). Оно будет выполнено, если возьмем число N больше, чем степени $f_1, \ldots, f_s$, и такое, что количество многочленов $f_{s+1}, \ldots, f_t$ будет $\leqslant \varepsilon^2 (d - 2\varepsilon)^{N-2}$. Докажем существование такого N, для чего оценим количество многочленов $f_{s+1}, \ldots, f_t$ в зависимости от N.

Пусть $g = g_{i_1} \ldots g_{i_N}$, причем g_i входит в это произведение m_i раз. Так как $c_{i\alpha}$ между собой перестановочны (это буквенные обозначения для элементов поля k), то g, как многочлен от $\{c_{i\alpha}\}$, содержит

$$\prod_{i=1}^{d-1} \binom{m_i + q - 1}{q - 1}, \qquad q = d + d^2 + \ldots + d^n,$$

слагаемых. Значит, столько и многочленов добавится от произведе-

ния g в отрезок $f_{s+1}, \ldots, f_t$. Так как $\binom{u}{v} \leqslant u^v$ и различных g имеется $(d-1)^N$, то общее число многочленов $f_{s+1}, \ldots, f_t$ не превосходит числа

$$(d-1)^N (N+q-1)^{(q-1)(d-1)}.$$

Так как $d - 1 < d - 2\varepsilon$, то это число $\leqslant \varepsilon^2 (d-2\varepsilon)^{N-2}$ при достаточно большом N. Доказательство закончено.

§ 27. Локальные теоремы логики

Здесь будет установлена локальная теорема Мальцева для квазиуниверсальных классов. Предполагая, что читатель знает основные определения формальной логики из общего курса, мы даем беглое, но вполне замкнутое изложение.

27.1. **Алгебраические системы.** Пусть A — множество. Функция n переменных, определенная на A и принимающая значения из множества {истина, ложь} (соответственно из A), называется *n-арным предикатом* (соответственно *n-арной операцией*) на A. Множество A с отмеченными на нем предикатами $P_\alpha^{n_\alpha}$ и операциями $f_\beta^{m_\beta}$ (n_α, m_β — их арности) называется *алгебраической системой*, а перечень символов $P_\alpha^{n_\alpha}$, $f_\beta^{m_\beta}$ — ее *сигнатурой*. Две алгебраические системы одной и той же сигнатуры называются *изоморфными*, если существует взаимно однозначное соответствие между ними, сохраняющее предикаты и операции. Примеры алгебраических систем — группы, кольца, поля, векторные пространства, упорядоченные множества и т. п.

Подмножество алгебраической системы, замкнутое относительно всех сигнатурных операций, называется *подсистемой*, если оно рассматривается вместе с индуцированными на нем предикатами и операциями, которые получаются сужением сигнатурных предикатов и операций самой системы.

Как отмечалось в основном тексте, совокупность подмножеств A_i, $i \in I$, множества A называется его *локальным покрытием*, если любой элемент из A содержится в некотором A_i и любые два множества A_i, A_j содержатся в некотором третьем множестве A_k. С локальными покрытиями тесно связано следующее понятие фильтра.

Пусть I — множество. Система F его непустых подмножеств называется *центрированной*, если она замкнута относительно конечных пересечений: $X \in F$, $Y \in F \Rightarrow X \cap Y \in F$. Центрированная система F называется *фильтром* над I, если она вместе с каждым своим множеством содержит все его надмножества: $X \in F$, $Y \supseteq X \Rightarrow Y \in F$. Фильтр, не содержащийся ни в каком большем, называется *максимальным*. Легко проверяется, что условие максимальности равносильно следующему: для каждого подмножества из I либо оно само, либо его дополнение принадлежит F. Очевидно, всякую центрированную систему можно дополнить до фильтра (добавляя к ней надмножества всех ее множеств), а вся-

кий фильтр — до максимального (лемма Цорна). Заметим, кстати, что до сих пор не известно ни одного максимального фильтра, построенного без леммы Цорна, за исключением малоинтересного фильтра, состоящего из всех надмножеств одной точки.

Пусть A_i, $i \in I$,— локальное покрытие множества A. Для каждого $\alpha \in I$ положим

$$I_\alpha = \{i \mid i \in I, \quad A_i \supseteq A_\alpha\}.$$

Легко видеть, что пересечение $I_\alpha \cap I_\beta$ содержит некоторое I_γ. Поэтому система всех I_α центрируема и, значит, существует максимальный фильтр F, содержащий эту систему. Если на каждом A_i отмечен предикат P_i, то обозначим через $P = \lim P_i$ предикат на A, определяемый следующим правилом:

$$P(x, y, \ldots) = \text{И на } A \Leftrightarrow$$
$$\Leftrightarrow \{i \mid x, y, \ldots \in A_i,\ P_i(x, y, \ldots) = \text{И на } A_i\} \in F.$$

Вообще говоря, сужение P на A_i не обязано совпадать с P_i. Однако если взять предикат, заданный на A, сузить его на каждое A_i и затем перейти к пределу по фильтру F в указанном смысле, то, конечно, получится исходный предикат.

27.2. **Язык исчисления предикатов.** Алфавит языка ИП состоит из предметных и предикатных переменных, скобок и следующих логических символов (первые четыре называются *связками*, а последние два — *кванторами*):

$\wedge$	и
$\vee$	или
$\neg$	не
$\rightarrow$	влечет
$=$	равно
$\forall$	для всякого
$\exists$	существует

Формулы ИП, не содержащие кванторов, относящихся к предикатам, называются *формулами узкого исчисления предикатов* (УИП) Несмотря на бедность словаря, язык ИП весьма содержателен Например, класс абелевых групп без кручения можно задать следующими аксиомами ИП — даже аксиомами УИП — в обычной сигнатуре $\cdot$, $^{-1}$, e теории групп:

1) ассоциативность: $(\forall x)(\forall y)(\forall z)((xy)\,z = x\,(yz))$,
2) определение единицы: $(\forall x)\,(xe = x \wedge ex = x)$,
3) определение обратных элементов:

$$(\forall x)(x^{-1}x = e \wedge xx^{-1} = e),$$

4) коммутативность: $(\forall x)(\forall y)(xy = yx)$,
5) отсутствие кручения:

$$(\forall x)\,(x = e \vee \neg(\underbrace{x \ldots x}_{n} = e)), \qquad n = 1, 2, \ldots$$

Приведем еще несколько примеров. Бинарный предикат называется *частичным порядком*, если для него имеют место

6) рефлексивность: $(\forall x)(x \leqslant x)$,

7) антисимметричность: $(\forall x)(\forall y)(x \leqslant y \wedge y \leqslant x \to x = y)$,

8) транзитивность: $(\forall x)(\forall y)(\forall z)(x \leqslant y \wedge y \leqslant z \to x \leqslant z)$,

и *линейным порядком*, если еще выполняется

9) линейность: $(\forall x)(\forall y)(x \leqslant y \vee y \leqslant x)$.

Предикат $\leqslant$, определенный на группе, называется *устойчивым относительно умножения*, если

10) $(\forall x)(\forall y)(\forall z)(x \leqslant y \to xz \leqslant yz \wedge zx \leqslant zy)$.

Группа называется *упорядочиваемой*, если на ней можно определить линейный порядок, устойчивый относительно умножения. Группа называется *доупорядочиваемой*, если любой ее частичный порядок, устойчивый относительно умножения, можно продолжить до линейного порядка, устойчивого относительно умножения. Легко понять, что классы упорядочиваемых и доупорядочиваемых групп выделяются в классе всех групп следующими аксиомами ИП (но уже не УИП):

11) упорядочиваемость:

$$(\exists P)(\forall x)(\forall y)(\forall z)(P(x, x) \wedge (P(x,y) \wedge P(y,x) \to x = y) \wedge$$
$$\wedge (P(x, y) \wedge P(y,z) \to P(x, z)) \wedge (P(x, y) \vee P(y, x)) \wedge$$
$$\wedge (P(x, y) \to P(xz, yz) \wedge P(zx, zy))),$$

12) доупорядочиваемость:

$$(\forall P)((P \text{ — у. ч. п.}) \to$$
$$\to (\exists Q)((Q \text{ — у.л.п.}) \wedge (\forall u)(\forall v)(P(u, v) \to Q(u, v))))$$

В последней формуле ради экономии места мы не выписываем явный вид аксиом устойчивого частичного порядка и аксиом устойчивого линейного порядка — они легко комбинируются из 6) — 10).

Напомним, что любую формулу ИП можно канонически переделать в равносильную ей *предваренную формулу*, в которой кванторы предшествуют всем другим логическим символам. Предваренная формула называется *универсальной*, если она совсем не содержит кванторов $\exists$, и *предметно-универсальной*, если она не содержит кванторов $\exists$, относящихся к предметным переменным. Формула ИП называется *квазиуниверсальной*, если она получается из предметно-универсальных формул без свободных предметных переменных применением только связок с последующим навешиванием кванторов $\forall$ на свободные предикатные переменные (это определение несколько отличается от первоначального определения А. И. Мальцева (1959) и было предложено Кливом (Cleave J. P. — J. London Math. Soc. (1), 1969, 44, № 1, p. 121—130; Addendum. — J. London Math. Soc.(2), 1969, 1, № 2, p. 384), назвавшим такие формулы булево-универсальными). Примером универсальных формул могут служить формулы 1) — 10). Формула 11) предметно-универсальна, а формула 12) равносильна квазиуниверсальной формуле, получающейся перенесением кванторных приставок из области действия приставки $(\exists Q)$ непосредственно за $(\exists Q)$.

27.2.1. Упражнение. Простые группы выделяются в классе всех групп квазиуниверсальной аксиомой.

27.3. Локальные теоремы. Рассмотрим сначала предметно-универсальные формулы.

37.3.1. Теорема. *Пусть* Ф — *предметно-универсальная формула. Если* Ф *истинна на некоторой алгебраической системе, то она истинна и на любой ее подсистеме. Если* Ф *истинна на подсистемах* A_i, *локально покрывающих алгебраическую систему* A, *то* Ф *истинна и на* A.

Доказательство. Чтобы избежать нудных «всеобщих» обозначений, ограничимся случаем, когда сигнатура содержит один символ бинарной операции и один символ S бинарного предиката.

а) Пусть A — алгебраическая система данной сигнатуры, удовлетворяющая предметно-универсальной аксиоме Ф, A' — подсистема системы A, т. е. подмножество, замкнутое относительно операции с индуцированной операцией и индуцированным предикатом. Покажем, что Ф истинна на A'. Предположим сначала, что Ф не содержит кванторов. Тогда утверждение непосредственно следует из определения истинности (напомним, что согласно определению формула ИП тогда и только тогда истинна на алгебраической системе, если она истинна при любых значениях предметных и предикатных переменных, не связанных кванторами). Предположим теперь, что Ф содержит кванторы, и проведем индукцию по их числу. В зависимости от того, какой квантор последний, возможны три случая: 1) $\Phi = (\forall t)\,\Psi$, 2) $\Phi = (\forall T)\,\Psi$, 3) $\Phi = (\exists T)\,\Psi$, где t — предметное, а T — предикатное переменные. Доопределяя предикаты с A' на всё A или, наоборот, сужая с A на A' и во всех трех случаях применяя индуктивное предположение, мы получаем, что Ф истинна на A'.

б) Пусть подсистемы A_i, $i \in I$, локально покрывают алгебраическую систему A и удовлетворяют формуле Ф. Требуется доказать, что Ф истинна на A. Пусть Ф содержит свободные предметные переменные $x, y, \ldots$ и свободные предикатные переменные $P, Q, \ldots$

$$\Phi = \Phi(x, y, \ldots, P, Q \ldots).$$

Пусть F — какой-нибудь максимальный фильтр над I, построенный по локальному покрытию A_i, $i \in I$, как указано в конце п. 27.1. Отметим на каждом A_i предикаты P_i, $Q_i, \ldots$ и положим $P_0 = \lim P_i$, $Q_0 = \lim Q_i, \ldots$ Для доказательства теоремы достаточно установить, что при любых значениях $x, y, \ldots$ из A

$$\{i \mid x, y, \ldots \in A_i,\ \Phi(x, y, \ldots, P_i, Q_i, \ldots) = \text{И на } A_i\} \in F \Rightarrow \Rightarrow \Phi(x, y, \ldots, P_0, Q_0, \ldots) = \text{И на } A. \qquad (1)$$

Собираясь вести индукцию по числу кванторов, допустим сначала, что Ф совсем их не содержит, и докажем, что тогда верно (1) и обратная импликация. Пусть (1′) обозначает объединение этих импликаций. Если формула Ф не содержит связок, то возможны три случая: 1) $\Phi = (u(x, y, \ldots) = v(x, y, \ldots))$, 2) $\Phi = S(u, v)$, 3) $\Phi = P(u, v, \ldots)$, где $u, v, \ldots$ — произведения с некоторой расстановкой скобок. В первых двух случаях (1′) очевидно, а в третьем случае вытекает из определения lim. Пусть теперь Ф по-прежнему не содержит кванторов, но содержит связки. Так как $\Psi \to \Omega$ рав-

носительно $\neg\Psi \vee \Omega$, то будем считать, что Φ содержит только связки $\wedge$, $\vee$, $\neg$, и докажем (1′) индукцией по их числу. В зависимости от того, какая связка последняя, возможны три случая: 4) $\Phi = \Psi \wedge \Omega$, 5) $\Phi = \Psi \vee \Omega$, 6) $\Phi = \neg\Psi$. В каждом из них (1′) легко вытекает из индуктивного предположения и определения фильтра F.

Предположим, наконец, что Φ содержит кванторы, и докажем утверждение (1) индукцией по их числу. В зависимости от того, какой квантор последний, возможны три случая: 7) $\Phi = (\forall t)\Psi$, 8) $\Phi = (\forall T)\Psi$, 9) $\Phi = (\exists T)\Psi$, где t — предметное, а T — предикатное переменные. Разберем случай 7). Придадим t произвольное значение на A. Надо показать, что $\Psi(t, x, y, \ldots, P_0, Q_0, \ldots) =$ И на A. В силу индуктивного предположения для этого достаточно проверить, что множество

$$\{i \mid t,\ x,\ y, \ldots \in A_i,\ \Psi(t, x, y, \ldots, P_i, Q_i, \ldots) = \text{И на } A_i\}$$

принадлежит F. Но это множество содержит пересечение множестиа $\{\ldots\}$ из (1) с множеством $\{i \mid t \in A_i\}$, поэтому всё доказано. Теперь разберем случай 8). Пусть T_0 — произвольный предикат на A, T_i — его сужение на A_i. Как отмечалось в конце п. 27.1, $T_0 = \lim T_i$. Надо показать, что

$$\Psi(x, y, \ldots, T_0, P_0, Q_0, \ldots) = \text{И на } A.$$

В силу индуктивного предположения достаточно проверить, что множество

$$\{i \mid x, y, \ldots \in A_i, \Psi(x, y, \ldots, T_i, P_i, Q_i, \ldots) = \text{И на } A_i\}$$

принадлежит F. Но это множество содержит $\{\ldots\}$ из (1), поэтому все доказано. Разберем последний случай 9). Пусть посылка в (1) выполнена. Тогда на каждой системе A_i существует такой предикат T_i, что множество

$$\{i \mid x, y, \ldots \in A_i,\ \Psi(x, y, \ldots, T_i, P_i, Q_i, \ldots) = \text{И на } A_i\}$$

принадлежит F. Пусть $T_0 = \lim T_i$. В силу индуктивного предположения $\Psi(x, y, \ldots, T_0, P_0, Q_0, \ldots) =$ И на A. Но это означает, что выполнено заключение в (1). Теорема доказана.

В качестве иллюстрации к этой теореме отметим справедливость локальной теоремы для класса упорядочиваемых групп — достаточно учесть, что этот класс определяется предметно-универсальной аксиомой 11) из п. 27.2.

27.3.2. Упражнение. Если в группе G каждая конечно порожденная подгруппа содержит абелеву нормальную подгруппу конечного индекса $\leqslant n$, то и вся G содержит абелеву нормальную подгруппу индекса $\leqslant n$.

Рассмотрим теперь произвольные квазиуниверсальные формулы.

27.3.3. Теорема (А. И. Мальцев). *Если квазиуниверсальная формула* Φ *истинна на подсистемах* A_i, *локально покрывающих алгебраическую систему* A, *то* Φ *истинна и на* A.

Доказательство. Согласно определению квазиуниверсальной формулы

$$\Phi = (\forall P_1)\ldots(\forall P_n)\,\Phi',$$

где Φ' составлена при помощи связок $\wedge$, $\vee$, $\neg$, $\to$ из предметно-универсальных формул без свободных предметных переменных, но со свободными предикатными переменными из списка $P_1, \ldots, P_n$. Допустим, что Φ истинна на каждом A_i, и докажем, что Φ истинна на A. Придадим предикатным переменным $P_1, \ldots, P_n$ какие-нибудь значения на A. Надо показать, что Φ' истинна на A при такой интерпретации $P_1, \ldots, P_n$, причем известно, что Φ' истинна на каждом A_i при индуцированных значениях $P_1, \ldots, P_n$. Другими словами, надо доказать теорему для формулы Φ', когда $P_1, \ldots, P_n$ считаются сигнатурными предикатами. Из начального курса логики известно, что Φ' можно привести к равносильному виду $\Phi' = \bigwedge \Phi_\alpha$, $\Phi_\alpha = \bigvee \Phi_{\alpha\beta}$, где $\Phi_{\alpha\beta}$ — предметно-универсальная формула, занрытая по предметным переменным, или отрицание такой формулы. Ясно, что если для всех Φ_α теорема верна, то она верна и для Φ'. Все это позволяет ограничиться рассмотрением следующих случаев:

1) $\Phi = \Psi_1 \vee \ldots \vee \Psi_r$,
2) $\Phi = \neg \Omega_1 \vee \ldots \vee \neg \Omega_s$,
3) $\Phi = \Psi_1 \vee \ldots \vee \Psi_r \vee \neg \Omega_1 \vee \ldots \vee \neg \Omega_s$,

где Ψ_α, Ω_β — предметно-универсальные формулы, закрытые по предметным переменным, $r, s \geqslant 1$.

Разберем только случай 3). Пусть Φ истинна на каждой A_i, но ложна на A. Тогда все Ψ_α ложны на A, все Ω_β истинны на A. По второй части теоремы 27.3.1 каждая Ψ_α ложна на некотором $A_{i(\alpha)}$. Пусть A_i содержит все $A_{i(\alpha)}$. По первой части теоремы 27.3.1 каждая Ψ_α ложна на A_i, каждая Ω_β истинна на A_i. Значит, Φ ложна на A_i, что противоречит условию. Случаи 1), 2) разбираются аналогично с очевидными упрощениями. Теорема доказана.

В качестве иллюстрации к ней отметим справедливость локальной теоремы для класса доупорядочиваемых групп и класса простых групп — см. формулу 12) в п. 27.2 и упражнение 27.2.1.

§ 28. О целых алгебраических числах

Мы предполагаем здесь, что начальные сведения и терминология теории полей известны читателю из общего курса алгебры.

Пусть $\overline{\mathbb{Q}}$ — алгебраическое замыкание поля $\mathbb{Q}$ рациональных чисел. Элементы из $\overline{\mathbb{Q}}$ называются *алгебраическими числами*. Элемент из $\overline{\mathbb{Q}}$ называется *целым* алгебраическим числом, если он является корнем многочлена с целыми коэффициентами и старшим коэффициентом 1.

Пусть k — произвольное поле алгебраических чисел, имеющее конечную степень (т. е. размерность как векторное пространство) над полем $\mathbb{Q}$, k_0 — множество всех целых алгебраических чисел из k.

28.1.1. Упражнение. Для всякого $\alpha \in k$ существует такое $m \in \mathbb{Z}$, что $m\alpha \in k_0$.

28.1.2. Упражнение. $\mathbb{Q}_0 = \mathbb{Z}$.

28.1.3. Лемма. *k_0 — подкольцо в k.*

Доказательство. Пусть $\alpha, \beta \in k_0$, γ — произвольный из элементов $\alpha \pm \beta$, $\alpha\beta$. Надо показать, что $\gamma \in k_0$.

Пусть

$$\alpha^l = \sum_{i=0}^{l-1} a_i \alpha^i, \quad a_i \in \mathbb{Z}, \quad \beta^m = \sum_{j=0}^{m-1} b_j \beta^j, \quad b_j \in \mathbb{Z}.$$

Легко понять, что совокупность o всевозможных элементов вида

$$\sum_{i=0}^{l-1} \sum_{j=0}^{m-1} c_{ij} \alpha^i \beta^j, \qquad c_{ij} \in \mathbb{Z},$$

является подкольцом в k. Пусть $\gamma_1, \ldots, \gamma_t$ — база аддитивной группы o и $\gamma_r \gamma = \sum_s d_{rs} \gamma_s$, $d_{rs} \in \mathbb{Z}$. Характеристический многочлен матрицы (d_{rs}) обращается в нуль в точке γ, поэтому γ — целое алгебраическое число. Лемма доказана.

Очевидно, для всякого $\alpha \in k$ сдвиг $x \mapsto x\alpha$, $x \in k$, является линейным преобразованием пространства k над полем $\mathbb{Q}$. Пусть χ_α — характеристический многочлен этого преобразования, $\operatorname{tr} \alpha$ — его след. Более общо, если K — подполе из $\mathbb{C}$, L — его расширение конечной степени, то для всякого $\alpha \in L$ преобразование $x \mapsto x\alpha$, $x \in L$, линейно над K и его след обозначается через $\operatorname{tr}_{L/K}(\alpha)$ (он принадлежит, конечно, полю K).

28.1.4. Лемма. *Если $\alpha \in k_0$, то χ_α — многочлен над $\mathbb{Z}$.*

Доказательство. Пусть n — степень k над $\mathbb{Q}$. Зафиксируем какую-нибудь базу k над $\mathbb{Q}$ и сопоставим каждому $\gamma \in k$ матрицу $\tilde{\gamma}$ сдвига $x \mapsto x\gamma$ в этой базе. Очевидно, получится изоморфное вложение $k \to M_n(\mathbb{Q})$. Так как α — корень уравнения над $\mathbb{Z}$ со старшим коэффициентом 1, то таковы и характеристические корни матрицы $\tilde{\alpha}$. Ввиду 28.1.3 коэффициенты многочлена χ_α — целые алгебраические числа. Ввиду 28.1.2 они лежат в $\mathbb{Z}$. Лемма доказана.

28.1.5. Лемма. *Пусть $\omega_1, \ldots, \omega_n$ — база k над $\mathbb{Q}$. Матрица $(\operatorname{tr}(\omega_i \omega_j))$ невырождена. Существует база $\{\omega_j^*\}$ поля k над $\mathbb{Q}$, двойственная к $\{\omega_i\}$, т. е. с условием*

$$\operatorname{tr}(\omega_i \omega_j^*) = \delta_{ij}.$$

Доказательство. а) Пусть, напротив, между столбцами матрицы $(\operatorname{tr}(\omega_i \omega_j))$ существует нетривиальная зависимость с коэффициентами $\alpha_j \in \mathbb{Q}$. Тогда

$$\omega = \sum \alpha_j \omega_j \neq 0, \ \operatorname{tr}(\omega_i \omega) = 0 \text{ для всех } 1 \leqslant i \leqslant n.$$

Так как $\{\omega_i \omega\}$ — тоже база k над $\mathbb{Q}$, то $1 = \sum \beta_i \omega_i \omega$ при подходящих $\beta_i \in \mathbb{Q}$. Вычисляя след от обеих частей, получим $n = 0$, что неверно.

б) Ищем ω_j^* в виде

$$\omega_j^* = \sum_l \xi_{jl}\omega_l, \qquad \xi_{jl} \in \mathbb{Q}.$$

Условие $\mathrm{tr}(\omega_i\omega_j^*) = \delta_{ij}$ превращается в систему линейных уравнений для $\xi_{j1}, \ldots, \xi_{jn}$. Ввиду а) она разрешима. Лемма доказана.

28.1.6. Т е о р е м а. *Аддитивная группа кольца k_0 конечно порождена.*

Д о к а з а т е л ь с т в о. Пусть $\omega_1, \ldots, \omega_n$ — база k над $\mathbb{Q}$. Ввиду 28.1.1 можно считать, что все $\omega_i \in k_0$. Пусть $\{\omega_j^*\}$ — двойственная база. Ввиду 28.1.1 существует такое $m \in \mathbb{Z}$, что все $m\omega_j^* \in k_0$. Пусть γ — произвольный элемент из k_0,

$$\gamma = \sum \gamma_i\omega_i, \qquad \gamma_i \in \mathbb{Q}.$$

Умножая это равенство на $m\omega_j^*$ и беря от обеих частей след, получим $m\gamma_j = \mathrm{tr}\,(m\gamma\omega_j^*)$. Так как $m\gamma\omega_j^* \in k_0$, то $m\gamma_j \in \mathbb{Z}$ (лемма 28.1.4). Мы видим, что аддитивная группа кольца k_0 лежит в группе с порождающими $\left\{\frac{1}{m}\omega_i\right\}$, а потому сама конечно порождена (см. 8.1.7). Теорема доказана.

28.1.7. Л е м м а. *Пусть K — подполе в $\mathbb{C}$. Для всякого расширения L/K степени d существует точно d изоморфизмов L в $\mathbb{C}$, тождественных на K. Если $\sigma_1, \ldots, \sigma_d$ — эти изоморфизмы, то*

$$\mathrm{tr}_{L/K}(\alpha) = \alpha^{\sigma_1} + \ldots + \alpha^{\sigma_d} \text{ для каждого } \alpha \in L. \tag{1}$$

Если $\{\omega_i\}$ — база L/K, то

$$\det(\mathrm{tr}_{L/K}(\omega_i\omega_j)) = \det(\omega^{\sigma_j})^2. \tag{2}$$

Д о к а з а т е л ь с т в о. а) Докажем сначала первое утверждение. Пусть $\alpha \in L$, f — минимальный многочлен элемента α над полем K, $\alpha_1, \ldots, \alpha_m$ — корни f в $\mathbb{C}$. Очевидно, существует взаимно однозначное соответствие между изоморфизмами $K(\alpha)/K \to \mathbb{C}$ и отображениями $\alpha \to \alpha_i$. По теореме о примитивном элементе (см. [6], стр. 165) $L = K(\alpha)$ при подходящем α, поэтому всё доказано. Можно обойтись и без теоремы о примитивном элементе — достаточно представить L в виде $K(\gamma_1)\ldots(\gamma_s)$ и заметить, что каждый изоморфизм $K(\gamma_1)\ldots(\gamma_i)/K \to \mathbb{C}$ имеет по предыдущему точно $|K(\gamma_1)\ldots(\gamma_{i+1}) : K(\gamma_1)\ldots(\gamma_i)|$ продолжений на $K(\gamma_1)\ldots(\gamma_{i+1})$.

б) Теперь докажем (1). Если $L = K(\alpha)$, то минимальный многочлен элемента α над K имеет степень $|L : K|$, а потому совпадает с характеристическим многочленом преобразования $x \mapsto x\alpha$ векторного пространства L над полем K.

По предыдущему $\alpha^{\sigma_1}, \ldots, \alpha^{\sigma_d}$ — в точности все его корни, откуда и следует (1). Общий случай сводится к рассмотренному

с помощью формулы

$$\mathrm{tr}_{L/K}(\alpha) = |\, L : K(\alpha)\,| \cdot \mathrm{tr}_{K(\alpha)/K}(\alpha).$$

Докажем ее. Пусть $\{\omega_i\}$ — база $L/K(\alpha)$, $\{\delta_j\}$ — база $K(\alpha)/K$. Тогда $\{\omega_i\delta_j\}$ — база L/K и в ней матрица преобразования $x \mapsto x\alpha$ имеет клеточно-диагональный вид, причем по диагонали повторяется матрица этого преобразования в базе $\{\delta_j\}$.

в) Докажем, наконец, (2). Ввиду (1)

$$\mathrm{tr}_{L/K}(\omega_i\omega_j) = \sum_{\sigma} \omega_i^{\sigma}\omega_j^{\sigma},$$

поэтому матрица, составленная из левых частей этого равенства, есть произведение матрицы (ω_i^{σ}) на ее транспонированную. Отсюда и вытекает (2). Лемма доказана.

Для всякого изоморфизма $\varphi\colon L \mapsto \mathbb{C}$ существует *сопряженный* изоморфизм $\bar{\varphi}\colon x \mapsto \overline{x^{\varphi}}$, $x \in L$, где черта над x^{φ} обозначает взятие комплексно-сопряженного числа. Если $\varphi = \bar{\varphi}$, то изоморфизм φ называется *действительным*, в противном случае — *комплексным*.

Вернемся к полю k. Пусть $n = |\, k : \mathbb{Q}\,|$, s — число действительных, а $2t$ — число комплексных изоморфизмов $k \to \mathbb{C}$, $n = s + 2t$. Пусть $\sigma_1, \ldots, \sigma_s$ — действительные, а $\sigma_{s+1}, \bar{\sigma}_{s+1}, \ldots, \sigma_{s+t}, \bar{\sigma}_{s+t}$ — комплексные изоморфизмы.

Рассмотрим n-мерное евклидово пространство $\mathbb{R}^n$ и отображение $\sigma\colon k \to \mathbb{R}^n$, определенное формулой

$$x^{\sigma} = (x^{\sigma_1}, \ldots, x^{\sigma_s}, \mathrm{Re}\,(x^{\sigma_{s+1}}), \mathrm{Im}\,(x^{\sigma_{s+1}}), \ldots, \mathrm{Re}\,(x^{\sigma_{s+t}}), \mathrm{Im}\,(x^{\sigma_{s+t}})), \quad x \in k,$$

где Re, Im — обозначения действительной и мнимой частей.

28.1.8. Упражнение. Отображение σ есть изоморфное вложение аддитивной группы k в аддитивную группу $\mathbb{R}^n$.

Пусть теперь k^*, k_0^* — мультипликативные группы поля k и кольца k_0. Определим отображение $\tau\colon k^* \to \mathbb{R}^{s+t}$, полагая

$$x^{\tau} = (\ln |\, x^{\sigma_1}|, \ldots, \ln |\, x^{\sigma_{s+t}}|), \quad x \in k^*.$$

28.1.9. Упражнение. Отображение τ — гомоморфизм группы k^* в аддитивную группу $\mathbb{R}^{s+t}$.

28.1.10. Лемма. *Множество k_0^{σ} дискретно в $\mathbb{R}^n$, т. е. имеет лишь конечное пересечение с любым шаром из $\mathbb{R}^n$. Множество $(k_0^*)^{\tau}$ дискретно в $\mathbb{R}^{s+t}$.*

Доказательство. Пусть $\omega_1, \ldots, \omega_n$ — база аддитивной группы кольца k_0. Так как $\det(\mathrm{tr}\,(\omega_i\omega_j)) \neq 0$ (лемма 28.1.5), то строки

$$(\omega_i^{\sigma_1}, \ldots, \omega_i^{\sigma_s}, \omega_i^{\sigma_{s+1}}, \omega_i^{\bar{\sigma}_{s+1}}, \ldots, \omega_i^{\sigma_{s+t}}, \omega_i^{\bar{\sigma}_{s+t}}), \qquad 1 \leqslant i \leqslant n,$$

линейно независимы над $\mathbb{R}$ (лемма 28.1.7), а потому и строки $\omega_1^\sigma, \ldots, \omega_n^\sigma$ линейно независимы над $\mathbb{R}$, т. е. составляют базу евклидова пространства $\mathbb{R}^n$. Возьмем в $\mathbb{R}^n$ биортогональную базу $\{e_j\}$, т. е. базу с условием

$$(\omega_i^\sigma, e_j) = \delta_{ij},$$

где круглые скобки обозначают скалярное произведение в $\mathbb{R}^n$.

Пусть

$$x \in k_0, \quad x = \sum x_i \omega_i, \ x_i \in \mathbb{Z}.$$

Очевидно, $x^\sigma = \sum x_i \omega_i^\sigma$ и ввиду неравенства Коши — Буняковского

$$|x_j| = |(x^\sigma, e_j)| \leqslant \|x^\sigma\| \cdot \|e_j\|.$$

Если x^σ принадлежит некоторому шару в $\mathbb{R}^n$, то для целых чисел x_j имеем лишь конечное число возможностей, откуда следует первое утверждение леммы. Если же $x \in k_0^*$ и x^τ принадлежит шару $\|z\| < r$ в $\mathbb{R}^{s+t}$, то x^σ принадлежит шару радиуса $e^r \sqrt{n}$ в $\mathbb{R}^n$. Лемма доказана.

28.1.11. Упражнение. Ядром сужения τ на k_0^* является совокупность всех корней из единицы, содержащихся в поле k. Это конечная циклическая группа.

Указание: если $x^\tau = 0$, то $\|x^\sigma\| \leqslant \sqrt{n}$.

28.1.12. Теорема. *Мультипликативная группа кольца k_0 конечно порождена.*

Доказательство. Ввиду 28.1.11 достаточно убедиться, что аддитивная группа $A = (k_0^*)^\tau$ конечно порождена, что мы и сделаем. Пусть $a_1, \ldots, a_m$ — максимальная линейно независимая над $\mathbb{R}$ подсистема из A,

$$A' = \left\{\sum \alpha_i a_i \mid \alpha_i \in \mathbb{Z}\right\}, \quad A'' = \left\{\sum \alpha_i a_i \mid 0 \leqslant \alpha_i < 1\right\}.$$

Очевидно, для всякого $x \in A$ существует запись

$$x = x' + x'', \ x' \in A', \ x'' \in A''.$$

Так как $x \in A$, $x' \in A$, то и $x'' \in A$. Но множество A'' ограничено в $\mathbb{R}^{s+t}$, поэтому пересечение $A \cap A''$ конечно (лемма 28.1.10). Следовательно, индекс $q = |A : A'|$ конечен. Так как $qA \subset A'$, то A содержится в аддитивной группе с порождающими $\frac{1}{q} a_1, \ldots, \frac{1}{q} a_m$. Ввиду 8.1.7 группа A конечно порождена. Теорема доказана.

Отметим, что из приведенного доказательства вытекает, что число свободных порождающих группы A не превосходит $s + t$. Более тонкими рассуждениями можно показать, что оно равно $s + t - 1$ и, значит, k_0^* — прямое произведение конечной циклической группы и $s + t - 1$ бесконечных циклических групп (теорема Дирихле).

ЛИТЕРАТУРА

1. Автоморфизмы классических групп: Сб. перев. с англ. и франц.— М.: Мир, 1976.

2. Адян С. И. Проблема Бернсайда и тождества в группах.— М.: Наука, 1975.

3. Белоногов В. А., Фомин А. Н. Матричные представления в теории конечных групп.— М.: Наука, 1976.

4. Биркгоф Г. Теория структур.— М.: ИЛ, 1952.

5. Бусаркин В. М., Горчаков Ю. М. Конечные расщепляемые группы.— М.: Наука, 1968.

6. ван дер Варден Б. Л. Алгебра.— 2-е изд.— М.: Наука, 1979.

7. Виноградов И. М. Основы теории чисел.— 9-е изд.— М.: Наука, 1981.

8. Горчаков Ю. М. Группы с конечными классами сопряженных элементов.— М.: Наука, 1978.

9. Изоморфизмы классических групп над целостными кольцами: Сб. перев. с англ.— М.: Мир, 1980.

10. Кокорин А. И., Копытов В. М. Линейно упорядоченные группы.— М.: Наука, 1972.

11. Коксетер Г. С. М., Мозер У. О. Дж. Порождающие элементы и определяющие соотношения дискретных групп.— М.: Наука, 1980.

12. Кострикин А. И. Введение в алгебру.— М.: Наука, 1977.

13. Коуровская тетрадь: Нерешенные вопросы теории групп.— 7-е изд.— Новосибирск, 1980.

14. Курош А. Г. Теория групп.— 3-е изд.— М.: Наука, 1967.

15. Курош А. Г., Черников С. Н. Разрешимые и нильпотентные группы.— УМН, 1947, 2, № 3, с. 18—59.

16. Линдон Р., Шупп П. Комбинаторная теория групп.— М.: Мир, 1980.

17. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп.— М.: Наука, 1974.

18. Мазуров В. Д. Конечные группы.— В сб.: Итоги науки и техники. Алгебра. Топология. Геометрия. Т. 14.— М., 1976, с. 5—56.

19. Мальцев А. И. Избранные труды, т. I: Классическая алгебра.— М.: Наука, 1976.

20. Мерзляков Ю. И. Рациональные группы.— М.: Наука, 1980.

21. Нейман Х. Многообразия групп.— М.: Мир, 1969.

22. Овсянников Л. В. Аналитические группы.— Новосибирск, 1972.

23. О'Мира О. Т. Лекции о симплектических группах.— М.: Мир, 1979.
24. Понтрягин Л. С. Непрерывные группы.— 3-е изд.— М.: Наука, 1973.
25. Разрешимые и простые бесконечные группы: Сб. перев. с англ. и нем.— М.: Мир, 1981.
26. Судзуки М. Строение группы и строение структуры ее подгрупп.— М.: ИЛ, 1960.
27. Супруненко Д. А. Группы матриц.— М.: Наука, 1972.
28. Фукс Л. Бесконечные абелевы группы.— М.: Мир, 1974, ч. 1, 1977, ч. 2.
29. Холл М. Теория групп.— М.: ИЛ, 1962.
30. Холл Ф. Нильпотентные группы.— Математика (сб.перев.), 1968, 12, № 1, с. 3—36.
31. Черников С. Н. Группы с заданными свойствами системы подгрупп.—М.: Наука, 1980.
32. Чунихин С. А. Подгруппы конечных групп.— Минск, 1964.
33. Шеметков Л. А. Формации конечных групп.— М.: Наука, 1978.
34. Шмидт О. Ю. Абстрактная теория групп.— В кн.: О. Ю. Шмидт. Избранные труды. Математика, М.: Изд-во АН СССР, 1959, с. 17—175.
35. Aschbacher M. The finite simple groups and their classification.— Yale University Press, 1980. [Русский перевод: УМН, 1981, 36, № 2, с. 141—172.]
36. Feit W., Thompson J. G. Solvability of groups of odd order.— Pacif. J. Math., 1963, 13, № 3, p. 775—1029.
37. Gruenberg K. W. Cohomological topics in group theory.— Berlin, 1970.
38. Huppert B. Endliche Gruppen, I.— Berlin, 1967; Huppert B., Blackburn N. Finite groups, II, III.— Berlin, 1981.
39. Kargapolov M. I. Some questions in the theory of soluble groups.— Lecture Notes Math., 1974, 372, p. 389—394.
40. Kegel O. H., Wehrfritz B. A. F. Locally finite groups.—Amsterdam; London, 1973.
41. O'Meara O. T., Lectures on linear groups.— Providence, 1974.
42. Puttaswamaiah B. M., Dixon J. D. Modular representations of finite groups.— N. Y., 1977.
43. Robinson D. J. S. A new treatment of soluble groups with finiteness conditions on their abelian subgroups.— Bull. London Math. Soc., 1976, 8, № 2, p. 113—129. [Русский перевод: УМН, 1979, 34, № 1, 197—215.]
44. Three lectures on polycyclic groups.— London: Queen Mary College Math. Notes, 1973.
45. Wehrfritz B. A. F. Infinite linear groups.—Berlin, 1973.
46. Wielandt H. Finite permutation groups.— N. Y., 1964.
47. Wussing H. Die Genesis der abstrakten Gruppenbegriffes.— Berlin, 1969.

ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ