

# THE THEORY OF GROUPS

---

Marshall Hall, Jr.

PROFESSOR OF MATHEMATICS  
THE OHIO STATE UNIVERSITY

The Macmillan Company  
New York · 1959

М. ХОЛЛ

# ТЕОРИЯ ГРУПП

*Перевод с английского*

Н. В. ДЮМИНА и З. П. ЖИЛИНСКОЙ

*Под редакцией*

Л. А. КАЛУЖНИНА

ИЗДАТЕЛЬСТВО ИНОСТРАННОЙ ЛИТЕРАТУРЫ

Москва · 1962

## **А Н Н О Т А Ц И Я**

По замыслу автора книга должна служить одновременно и учебником по теории групп, предназначенным для студентов и аспирантов, и монографией по некоторым избранным разделам этой дисциплины, находящимся в настоящее время в центре внимания специалистов.

Первые десять глав, снабженные упражнениями, представляют классический курс теории групп и могут быть использованы в качестве учебника. Последние десять глав носят более специальный характер и посвящены избранным вопросам теории групп.

Книга доступна студентам математических факультетов университетов и педагогических институтов; студенты-физики найдут в этой книге необходимые им элементы теории представлений групп; специалист же найдет в ней изложение результатов, опубликованных только в журнальной литературе.

**Редакция литературы по математическим наукам**

## ПРЕДИСЛОВИЕ РЕДАКТОРА ПЕРЕВОДА

Настоящая книга американского математика Маршалла Холла (младшего) является одним из лучших современных трактатов по теории абстрактных групп. По замыслу автора она должна служить одновременно и учебником по теории групп, предназначенным для студентов и аспирантов, и монографией по некоторым избранным разделам этой дисциплины, находящимся в настоящее время в центре внимания специалистов. Поставленная цель, несомненно, достигнута: учащийся сможет по ней быстро ознакомиться с элементарными понятиями и усвоить материал, ставший уже классическим, специалист же здесь найдет связное изложение многочисленных результатов, полученных в самое последнее время и опубликованных пока только в журнальной литературе.

Из сказанного видно, что по своему построению книга М. Холла похожа на известную книгу А. Г. Куроша „Теория групп“ (Гостехиздат, 1 издание, 1944 г.; 2 издание, 1953 г.), ставшую настольной книгой советских алгебраистов, а после ее перевода на немецкий, английский, венгерский и японский языки пользующуюся заслуженной славой среди зарубежных специалистов. Но по своему содержанию книги А. Г. Куроша и М. Холла не совпадают, а во многом дополняют друг друга. Впрочем, это не совсем случайно: М. Холл обошел частичным или полным молчанием ряд важных разделов современной теории групп (как, например, теорию бесконечных абелевых групп, теорию прямых разложений, теорию обобщенных разрешимых и нильпотентных групп) именно потому, что они получили достаточно полное освещение в труде А. Г. Куроша. С другой стороны, для советских алгебраистов предлагаемая книга может быть полезной как раз потому, что в ней он найдет сравнительно полное освещение как раз таких направлений теоретико-групповых исследований, которые отсутствуют в „Теории групп“ А. Г. Куроша и которые до сих пор не излагались в обзорных статьях по теории групп, публикуемых в журнале „Успехи математических наук“.

Начиная с конца прошлого столетия и по сей день, теория абстрактных групп находится в состоянии непрерывного развития. Более того, исследовательская работа по этой дисциплине явно

имеет тенденцию ко все большему расширению. Это видно хотя бы уже из все возрастающего потока оригинальных статей по теории групп, публикуемых во всех крупных математических журналах как в СССР, так и за рубежом. При этом о расцвете теории групп свидетельствует не только число публикуемых работ, но и несомненно более убедительные факты: появление все новых и новых плодотворных постановок проблем и все новые применения именно тонких результатов теории групп в самых различных областях математики. Так, например, можно отметить большое значение теории абелевых групп для дальнейшего развития гомологической алгебры — новой математической дисциплины, приобретающей фундаментальное значение в алгебре, топологии, в анализе и даже, по-видимому, в вычислительной технике и кибернетике. Все новые применения находит теория представлений групп в анализе, в теории чисел, в кристаллографии и в теоретической физике. Теория расширений групп все теснее смыкается с гомологической алгеброй. Теория свободных групп и изучение групп, заданных образующими и определяющими отношениями, дают ценный материал для математической логики, в рамках которой доказывается алгоритмическая неразрешимость ряда вопросов теории групп [например, доказательство алгоритмической неразрешимости проблемы слов в группах, заданных образующими и определяющими отношениями (П. С. Новиков)].

Все это и многое другое, что можно было бы здесь еще привести, подтверждает большое значение теории групп в современной математике и объясняет большой объем и разветвленность теоретико-групповых исследований. Ни один учебник, ни одна монография не способны даже приблизительно осветить все основные направления. Поэтому книги, озаглавленные „Теория групп“, должны быть именно такими, как книга А. Г. Куроша и предлагаемая книга М. Холла. Для ознакомления с другими областями теории групп, не нашедшими места в указанных трудах, следует обращаться к специальным монографиям или обзорным статьям, публикуемым у нас в основном в журнале „Успехи математических наук“ (соответствующие указания, не претендующие на полноту, мы включили в библиографию).

При подборе разделов теории групп, включенных в рассмотрение, автор, естественно, во многом руководствовался личными вкусами. Ценной является подробная трактовка результатов исследований английской школы кембриджского алгебраиста Ф. Холла и его учеников и сотрудников. Сюда относится, в первую очередь, детальное исследование строения конечных  $p$ -групп с применением ряда оригинальных методов, введенных Ф. Холлом (главы 11 и 12): так называемый „собирательный процесс“, исчисление сложных коммутаторов и др. Этими методами были по-

лучены важные тождества и соотношения (формулы Ф. Холла, Э. Витта и др.) и выделен и изучен важный класс  $p$ -групп — регулярные  $p$ -группы. С этим кругом вопросов связаны исследования по ослабленной проблеме Бернсайда (глава 18). Изложение указанных вопросов достаточно подробно, но не претендует на полноту: ряд результатов И. Н. Санова, А. И. Кострикина, М. Лазара, Майер-Вундерли и др. остались вне рассмотрения отчасти из-за их сложности, отчасти потому, что не были известны автору во время написания книги. Таким образом, читателю, желающему ознакомиться с современным состоянием вопросов, нужно будет после прочтения книги проштудировать соответствующую оригинальную литературу. Трактовка же в книге М. Холла является превосходной подготовкой к такому изучению.

Подобные же замечания можно сделать и относительно других разделов: теории мономиальных представлений и понятия перемещения групп (глава 14), дающих мощный метод для доказательства непростоты групп, теории разрешимых и сверхразрешимых конечных групп (главы 9 и 10), теории когомологий и расширений групп (глава 15) и других вопросов.

Большой интерес представляет последняя глава книги, посвященная установлению связи теории групп с теорией проективных плоскостей. Многие из изложенных результатов принадлежат самому автору. Из советских работ, примыкающих к трактуемой тематике, следует указать на работы Л. И. Копейкиной и особенно Л. А. Скорнякова.

Нельзя не отметить несколько странную манеру автора при указании источников, которыми он пользовался, и авторов понятий, методов и результатов, которые он излагает: в некоторых случаях он их указывает, зачастую же обходит молчанием. Это касается как советских, так и зарубежных авторов. Редактор не всегда был в состоянии восстановить источник и не внес поэтому в перевод в этом отношении никаких изменений. Библиография же была дополнена указанием на ряд советских работ, относящихся непосредственно или примыкающих к трактуемой в книге тематике.

Для удобства читателя все работы советских алгебраистов (как указанные автором, так и добавленные редактором перевода) помещены в дополнении к литературе. Более подробное освещение исследований советских авторов по теории групп читатель найдет в сборнике „Математика в СССР за сорок лет“ (Физматгиз, 1959 г.) — в обзорной статье „Общая алгебра“ В. М. Глушкова и А. Г. Куроша.

Л. А. Калужник



## ПРЕДИСЛОВИЕ

Предлагаемая книга должна служить двум целям. Предполагается, что первые десять глав могут лечь в основу курса по теории групп; поэтому в конце каждой главы помещены упражнения. Последние десять глав могут рассматриваться как избранный, факультативный материал для лекций или в качестве справочного материала. Как монография книга предназначена для студентов, прослушавших курс введение в современную алгебру, сравнимый с курсом Биркгофа и Маклейна „Обзор современной алгебры“. Я старался сделать содержание книги по возможности не зависящим от другой литературы, тем не менее там, где мы были вынуждены пользоваться предварительными данными, мы в основном ссылались на монографию Биркгофа и Маклейна.

Современные исследования в области теории групп охватывают очень большую и бурно развивающуюся область. Это видно хотя бы из публикаций, реферируемых в Mathematical Review. Таким образом, нет никакой возможности охватить всю тематику или даже только привести полную библиографию. Поэтому при выборе изложенных тем я в большой мере следовал моим собственным научным интересам, а библиография относится только к той литературе, на которую имеется ссылка в самой книге. Я умышленно постарался сократить некоторые очень интересные разделы, детальное изложение которых имеется в легко доступных недавних публикациях. Для ознакомления с детальными исследованиями по бесконечным абелевым группам мы отсылаем читателя к соответствующим главам второго издания книги А. Г. Курова „Теория групп“ и к монографии Капланского „Бесконечные абелевы группы“. Мы рекомендуем книги М. Судзуки „Строение группы и строение структуры ее подгрупп“<sup>1)</sup> и Коксетера и Мозера „Образующие и отношения для дискретных групп“ тем читателям, которые хотят глубже ознакомиться с этими разделами (обе книги вышли в серии „Ergebnisse“).

---

<sup>1)</sup> Имеется русский перевод (ИЛ, 1960, серия „Библиотека сборника „Математика“).

Книга создана на основании конспектов по курсу „Теория групп“, который я ряд лет читал в Государственном университете штата Огайо. Большая часть предлагаемой книги была написана в Тринити коллеж (Trinity College), Кембридж, в 1956 г., где я проходил стажировку за счет фонда имени Джона Симона Гугенхайма. Я выражаю мою благодарность этому фонду за предоставленную мне возможность создать этот труд, а также членам Тринити коллежа, позволившим мне воспользоваться всеми преимуществами коллежа.

Я должен особенно поблагодарить профессора Филиппа Холла из Кингс коллежа, Кембридж, за многочисленные ценные советы при подготовке рукописи и за предоставление его собственных неопубликованных результатов. В благодарность за его любезность я посвящаю ему эту книгу.

Я хочу также выразить мою признательность за оказанную мне помощь профессорам Герберту Райзеру и Яну Корринге и, наконец, доктору Эрнесту Паркеру за его участие в ходе дел, связанных с подготовкой рукописи.

Колумбус, Огайо.

*Маршалл Холл  
младший*

## Гла́ва 1

### ВВЕДЕНИЕ

#### 1.1. Алгебраические законы

Большая часть алгебры имеет дело с системами элементов, которые, подобно числам, можно складывать или умножать, или подвергать обеим операциям. Пусть дана система, элементы которой обозначены буквами  $a, b, c, \dots$ . Назовем ее  $S = S(a, b, c, \dots)$ . Свойства систем зависят от того, какие из следующих основных законов в них выполняются.

**Законы замкнутости.** А0. *Сложение вполне определено.* М0. *Умножение вполне определено.*

Это значит, что для каждой упорядоченной пары элементов  $a, b \in S$  элементы  $a + b = c$  и  $ab = d$  существуют и однозначно определены в  $S$ .

**Ассоциативные законы.** А1.  $(a + b) + c = a + (b + c).$  М1.  $(ab)c = a(bc).$

**Коммутативные законы.** А2.  $a + b = b + a.$  М2.  $ba = ab.$

**Нуль и единица.** А3. *Существует такой элемент 0, что  $0 + a = a + 0 = a$  для всех  $a \in S.$*  М3. *Существует такой элемент 1, что  $1a = a1 = a$  для всех  $a \in S.$*

**Противоположные и обратные элементы.** А4. Для любого элемента  $a \in S$  существует элемент  $-a \in S$  такой, что  $(-a) + a = a + (-a) = 0.$  М4. <sup>1)</sup> Для любого элемента  $a \neq 0$  существует элемент  $a^{-1} \in S$  такой, что  $(a^{-1})a = a(a^{-1}) = 1.$

**Дистрибутивные законы.** Д1.  $a(b + c) = ab + ac.$  Д2.  $(b + c)a = ba + ca.$

<sup>1)</sup> Закон М4 формулируется здесь для системы с умножением и сложением. Если же сложение не определено и нуля в системе нет, то закон М4 принимает вид: „Для любого элемента  $a$  существует элемент  $a^{-1}$  такой, что  $(a^{-1})a = a(a^{-1}) = 1.“$

Onejejhene. *Tlycmu dahuq qba omogakhenu a u g mohke-  
cmu S e c66a. Muu onpedeareaa mpemebe omogakhenue y mho-  
kecmeba S e c66a mak: ecua y = (x) a u z = (y) g, mo z = (x)*

$\cdot v(x) = \kappa \quad \text{and} \quad \kappa \leftarrow x : v$

Одним из самых очаровательных сюжетов в истории любви является легенда о том, как Ариадна, принцесса Крита, спасла Theseus от Минотавра. Для этого ей пришлось пройти через лабиринт и убить чудовище. Но когда Theseus вернулся домой, Ариадна была забыта. И только через много лет, когда она стала старой, она вспомнила свою любовь и вернулась к нему. Они прожили счастливую жизнь вместе.

## 1.2. Otpakēnā

Boolee  $n$ -Mecthaa ohepanua B mokectre S —  $\exists$ ro fykhuna  
 $f = f(a_1, \dots, a_n)$  or  $n$  aprymehbor  $a_1, \dots, a_n$ . Upnayiajekamix  
 mokectre S, upnayem shahene ee  $f(a_1, \dots, a_n) = q$  ohotosahao  
 ohepanua B mokectre S, ecjin fykhuna f ohepanua B mokectre S,  
 aprymehbor. Ecjin upn moloom brolode jemehbor  $a_1, \dots, a_n$  B moh-  
 jekctre S fykhuna f  $(a_1, \dots, a_n)$  ohepanua B mokectre S amrymo  
 ohepanua f recod ohepanua, nrao to mokectre S amrymo  
 ohepanua f recod ohepanua, nrao to mokectre S amrymo  
 B noje F cokkehne n ymokkehne arjhoreca hoinie ohepanua  
 hrim gnhaphrim ohepanua, a ohepanua ohepanua  $f(a) = a$   
 arjhoreca yhaphon ohepanua, ohepanua aia molooro jremehtra,  
 kosome hyja.

$$\log(x) + \log(y) = \log(xy)$$

Опережение. *Cucumea*, *Yodoaemospaerula* *Beechman* *sauvagei*  
hahm, *hahmiaemerica novae-m. Cucumea*, *Yodoaemospaerula* *sauvagei*  
AO — A4, MO, MI " II1, II2, *hahmiaemerica novae-m.*  
Creyter отмечал, что *sauvagei* AO — A4 соревнуется  
засухоустойчивым *M0 — M4*, кроме *cirysaa a = 0* в *tipedobrann M4*, *Kotia*  
*ogopatria* *zinei* нест *he* *cytotoxicity*. *Ozarko* *B* *introducing* *intrinsic* *3ako-*  
*has* *crookene* *и* *ymokhene* *heparohypophysis*. *Это* *тепаринин*  
*mekky* *crookene* *и* *ymokhene* *nicotriplayterca* *up* *ymokhene* *heparohypophysis*  
*кора* *adrenals* *crookene* *и* *ymokhene* *heparohypophysis*.

*Отображение  $\gamma$  называется произведением отображений  $\alpha$  и  $\beta$  и обозначается  $\gamma = \alpha\beta$ .*

Так как здесь элементы  $y = (x)\alpha$  и  $z = (y)\beta$  однозначно определены в  $S$ , то и элемент  $z = [(x)\alpha]\beta = (x)\gamma$  однозначно определен в  $S$  для любого  $x \in S$ .

**Теорема 1.2.1.** *Отображения некоторого множества  $S$  в себя удовлетворяют законам М0, М1, М3, если под умножением понимать умножение отображений множества  $S$  в себя.*

**Доказательство.** Как уже отмечалось, требование М0 выполняется. Проверим выполнимость закона М1. Пусть  $\alpha, \beta, \gamma$  — три данных отображения. Возьмем произвольный элемент  $x$  из  $S$  и положим  $y = (x)\alpha, z = (y)\beta$  и  $w = (z)\gamma$ . Тогда  $(x)[(\alpha\beta)\gamma] = (z)\gamma = w, (x)[\alpha(\beta\gamma)] = (y)\beta\gamma = w$ . Это значит, что отображения  $(\alpha\beta)\gamma$  и  $\alpha(\beta\gamma)$  дают один и тот же образ произвольного элемента  $x \in S$ , т. е. что  $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ .

Для проверки закона М3 за 1 примем такое отображение, при котором  $(x)1 = x$  для любого элемента  $x \in S$ . Тогда отображение 1 является единицей в том смысле, что  $\alpha 1 = 1\alpha = \alpha$  для любого отображения  $\alpha$ .

В общем случае для отображений ни требование М2, ни М4 не выполняются. Однако закон М4 справедлив для важного класса отображений, а именно для взаимно однозначных отображений множества  $S$  на себя.

**Определение.** *Говорят, что отображение  $\alpha$  множества  $S$  на множество  $T$  взаимно однозначно, если каждый элемент множества  $T$  является образом только одного элемента из  $S$ .*

Такое отображение обозначают  $\alpha : x \rightarrow y$ , где  $x \in S, y \in T$ , и говорят, что множества  $S$  и  $T$  имеют одно и то же кардинальное число<sup>1)</sup> элементов.

**Теорема 1.2.2.** *Взаимно однозначное отображение множества  $S$  на себя удовлетворяет требованиям М0, М1, М3, М4.*

**Доказательство.** Выполнимость условий М0, М1, М3 установлена теоремой 1.2.1. Осталось проверить М4. Если отображение  $\alpha : x \rightarrow y$  множества  $S$  на себя взаимно однозначно, то, по определению, для каждого элемента  $y$  из  $S$  существует точно один  $x$  из  $S$  такой, что  $y = (x)\alpha$ . Сопоставляя этот элемент  $x$  элементу  $y$ , мы определяем взаимно однозначное отображение  $\tau : y \rightarrow x$  множества  $S$  на себя. Из определения отображения  $\tau$  видно, что  $(x)\alpha\tau = x$  для любого элемента  $x \in S$  и  $(y)\tau\alpha = y$  для любого  $y \in S$ . Следовательно,  $\alpha\tau = \tau\alpha = 1$ , и  $\tau$  является ото-

<sup>1)</sup> О кардинальных числах см. Биркгоф и Маклейн [1], стр. 356. (См. также Клини К., Введение в метаматематику, ИЛ, М., 1957.—Прим. перев.)

бражением, удовлетворяющим требованиям закона М4 для обратного элемента  $a^{-1}$ .

Взаимно однозначное отображение некоторого множества на себя называется *подстановкой*. Если данное множество конечно, подстановку можно записать, располагая элементы множества в строчку и подписывая под каждым элементом его образ. Так,  $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$  и  $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$  — две подстановки множества  $S(1, 2, 3)$ . Согласно определению, их произведением является подстановка  $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ . Заметим, что это умножение производится здесь слева направо, однако некоторые авторы определяют произведение подстановок так, что они умножаются справа налево.

### 1.3. Определения группы и некоторых сходных систем

Мы видели, что системы с одной определенной в них операцией (сложением или умножением) подчиняются одним и тем же законам. За исключением коммутативного закона, все они выполняются при умножении взаимно однозначных отображений множества на себя. Законы, которым подчиняются эти взаимно однозначные отображения, мы и используем для определения группы.

**Определение.** (Первое определение группы.) *Группой  $G$  называется некоторое множество элементов  $G(a, b, c, \dots)$  с бинарной операцией, называемой „произведением“, такой, что выполняются:*

G0. *Закон замкнутости. Для каждой упорядоченной пары элементов  $a, b$  из  $G$  произведение  $ab = c$  существует и является однозначно определенным элементом из  $G$ .*

G1. *Ассоциативный закон.  $(ab)c = a(bc)$ .*

G2. *Существование единицы. Существует такой элемент 1, что  $1a = a1 = a$  для любого элемента  $a \in G$ .*

G3. *Существование обратного элемента. Для всякого элемента  $a \in G$  существует такой элемент  $a^{-1} \in G$ , что  $a^{-1}a = aa^{-1} = 1$ . Эта система аксиом избыточна. Можно ослабить требования G2 и G3, заменив их следующими:*

G2\*. *Существует такой элемент 1, что  $1a = a$  для любого  $a \in G$ .*

G3\*. *Для всякого  $a \in G$  существует такой элемент  $x \in G$ , что  $xa = 1$ .*

Можно показать, что из G2\* и G3\* следуют условия G2 и G3. Пусть для некоторого  $a$  имеют место соотношения  $xa = 1$  и  $yx = 1$ , согласно G3\*. Тогда имеем

$$ax = 1 \quad (ax) = (yx)(ax) = y[x(ax)] = y[(xa)x] = y(1x) = yx = 1,$$

т. е. выполняется условие G3. Аналогично

$$a = 1a = (ax)a = a(xa) = a1,$$

так что и G2 удовлетворено.

Единственность единицы 1 и обратного элемента  $a^{-1}$  легко устанавливается (см. упр. 13). Конечно, можно было бы заменить G2 и G3 требованием существования таких элементов 1 и  $x$ , что  $a1 = a$  и  $ax = 1$ . Однако аксиомы  $a1 = a$  и  $xa = 1$  приводят к несколько иной ситуации<sup>1)</sup>.

Существует несколько способов расстановки скобок в упорядоченной последовательности элементов  $a_1a_2 \dots a_n$  для получения их произведения путем последовательного выполнения бинарного умножения. Для  $n = 3$  существует только два таких способа, а именно  $(a_1a_2)a_3$  и  $a_1(a_2a_3)$ . Ассоциативный закон утверждает равенство этих двух произведений. Важным следствием ассоциативного закона является обобщенный ассоциативный закон.

«Все способы расстановки скобок в упорядоченной последовательности элементов  $a_1a_2, \dots, a_n$  при последовательном выполнении бинарных умножений приводят к одному и тому же результату.

Применяя индукцию по  $n$ , легко доказать, что обобщенный ассоциативный закон вытекает из ассоциативного закона (см. упр. 1).

Можно дать другое определение группы, в котором явно не требуется существование единицы.

**ОПРЕДЕЛЕНИЕ.** (ВТОРОЕ ОПРЕДЕЛЕНИЕ ГРУППЫ.) Группа  $G$  — это такое множество элементов  $G(a, b, \dots)$ , что

1) для каждой упорядоченной пары  $a, b$  элементов  $G$  однозначно определено бинарное произведение  $ab = c$ , принадлежащее  $G$ ,

2) для каждого элемента  $a \in G$  однозначно определена унарная операция „обращения”  $a^{-1}$ , где  $a^{-1}$  — опять элемент из  $G$ ,

3) выполняется ассоциативный закон  $(ab)c = a(bc)$ ,

4) имеет место закон обращения  $a^{-1}(ab) = b = (ba)a^{-1}$ .

Легко показать, что любое множество, удовлетворяющее аксиомам первого определения, также удовлетворяет аксиомам второго. Докажем обратное. Предположив выполнимость аксиом второго определения, рассмотрим равенства

$$a^{-1}a = [(a^{-1}a)b]b^{-1} = (a^{-1}a)(bb^{-1}) = a^{-1}[a(bb^{-1})] = bb^{-1}.$$

Для  $a = b$  отсюда следует  $a^{-1}a = aa^{-1}$ , а также то, что элемент  $a^{-1}a = aa^{-1}$  не зависит от  $a$  и представляет один и тот же эле-

<sup>1)</sup> Манн [1].

мент. Назовем его „1“. Тогда аксиома G3 выполняется. Далее,

$$1b = (a^{-1}a)b = a^{-1}(ab) = b$$

и

$$b1 = b(aa^{-1}) = (ba)a^{-1} = b,$$

т. е. имеет место G2. Итак, два определения группы эквивалентны. Имеется третье определение группы.

**ОПРЕДЕЛЕНИЕ.** (ТРЕТЬЕ ОПРЕДЕЛЕНИЕ ГРУППЫ.) *Группа G — это некоторое множество элементов G (a, b, c, ...) с такой бинарной операцией a/b, что:*

L0. Для каждой упорядоченной пары a, b элементов из G однозначно определен элемент a/b = c ∈ G.

$$L1. a/a = b/b.$$

$$L2. a/(b/b) = a.$$

$$L3. (a/a)/(b/c) = c/b.$$

$$L4. (a/c)/(b/c) = a/b.$$

Определим через эту операцию унарную операцию обращения  $b^{-1}$  следующим образом:

$$b^{-1} = (b/b)/b.$$

Пользуясь L3 и L2, получаем

$$(b^{-1})^{-1} = (b^{-1}/b^{-1})/b^{-1} = (b^{-1}/b^{-1})/[(b/b)/b] = b/(b/b) = b.$$

Зададим бинарную операцию умножения, подожив

$$ab = a/b^{-1}.$$

Тогда  $a/b = a/(b^{-1})^{-1} = ab^{-1}$ . Обозначим через 1 общее значение выражений  $a/a = b/b$ . (Это равенство имеет место согласно L1.) Тогда L1 можно записать в виде  $aa^{-1} = 1$ , откуда для любого a имеем  $1 = a^{-1}(a^{-1})^{-1} = a^{-1}a$ . Таким образом, выполняется требование G3 из первого определения группы. В равенстве  $b^{-1} = (b/b)/b$  полагаем  $b = 1$ . Тогда  $1^{-1} = 1 \cdot 1^{-1}$ , и поэтому  $1 = 1/1 = 1 \cdot 1^{-1} = 1^{-1}$ , а L2 принимает форму  $a1^{-1} = a1 = a$ . Так как, по определению,  $b^{-1} = 1/b = 1 \cdot b^{-1}$ , то, положив  $b = a^{-1}$ , получаем  $(a^{-1})^{-1} = 1 \cdot (a^{-1})^{-1}$ , или  $a = 1a$ . Поэтому выполняется аксиома G2 первого определения. L3 превращается в равенство  $1(bc^{-1})^{-1} = cb^{-1}$ , откуда  $(bc^{-1})^{-1} = cb^{-1}$ . В L4 полагаем  $a = x$ ,  $b = 1$ ,  $c = y^{-1}$  и получаем  $(xy)(1y)^{-1} = x1^{-1} = x$ , или  $(xy)y^{-1} = x$ . Теперь для произвольных x, y, z полагаем  $a = xy$ ,  $b = z^{-1}$ ,  $c = y$ . Тогда  $ac^{-1} = (xy)y^{-1} = x$ , и L4 переходит в равенство  $(ac^{-1})(bc^{-1})^{-1} = ab^{-1}$ , откуда  $(ac^{-1})(cb^{-1}) = ab^{-1}$ . Для x, y, z это означает, что  $x(yz) = (xy)z$ , т. е. что выполняется

требование G1. Таким образом, из третьего определения группы следует первое. Если же, наоборот, исходить из первого определения и положить  $ab^{-1} = a/b$ , легко обнаружить, что выполняются законы L0—L4. Таким образом, определения эквивалентны.

Существуют системы, удовлетворяющие только некоторым аксиомам группы. Укажем самые распространенные из них.

**ОПРЕДЕЛЕНИЕ.** Квазигруппой  $Q$  называется система элементов  $Q(a, b, c, \dots)$ , в которой определена такая бинарная операция умножения  $ab$ , что в равенстве  $ab = c$  любые два из элементов  $a, b, c$  системы  $Q$  определяют третий.

**ОПРЕДЕЛЕНИЕ.** Лупой называется квазигруппа, в которой существует элемент 1 такой, что  $1a = a1 = a$  для всякого  $a$ .

**ОПРЕДЕЛЕНИЕ.** Полугруппой называется система  $S(a, b, c, \dots)$  элементов с бинарной операцией умножения  $ab$ , удовлетворяющей требованию  $(ab)c = a(bc)$ .

Ясно, что группа удовлетворяет всем этим определениям. Следуя Курошу, можно еще определить группу как множество, являющееся одновременно и полугруппой, и квазигруппой. Из определения полугруппы следует, что для нее выполняются законы G0 и G1. Пусть  $t$  — единственный элемент, такой, что  $tb = b$  для некоторого элемента  $b$ , и пусть у определяется элементами  $b, a$  и равенством  $by = a$ . Тогда имеем  $(tb)y = by$  и  $t(by) = by$ , или  $ta = a$  для любого  $a$ , так что выполняется G2\*. В квазигруппе G3\* также выполняется. А эти свойства, как мы уже показали, определяют группу.

Назовем систему с бинарным произведением и унарным обращением, удовлетворяющими условию

$$a^{-1}(ab) = b = (ba)a^{-1},$$

квазигруппой со свойством обращения. При этом приведенное тождество будем считать законом обращения. Мы должны показать, что такое произведение определяет квазигруппу. Если  $ab = c$ , то  $b = a^{-1}(ab) = a^{-1}c$  и  $a = (ab)b^{-1} = cb^{-1}$ . Поэтому  $a$  и  $b$  определяют элемент  $c$  однозначно, но также  $c$  и  $a$  определяют не более одного  $b$ , а для данных  $c$  и  $b$  существует не более одного  $a$ . Положим  $a(a^{-1}c) = w$ . Тогда  $a^{-1}[a(a^{-1}c)] = a^{-1}w$ , откуда  $a^{-1}c = a^{-1}w$ . Поэтому  $(a^{-1})^{-1}(a^{-1}c) = (a^{-1})^{-1}(a^{-1}w)$ , откуда  $c = w$ . Значит,  $a(a^{-1}c) = c$  и аналогично  $(cb^{-1})b = c$ . Итак, система является квазигруппой. Заметим, что квазигруппа со свойством обращения не обязательно является лупой. Например, три элемента  $a, b, c$  с отношениями  $a^2 = a$ ,  $ab = ba = c$ ,  $b^2 = b$ ,  $bc = cb = a$ ,  $c^2 = c$ ,  $ca = ac = b$  составляют квазигруппу со свойством обращения (обратным к каждому элементу является он сам), но не имеющую единицы.

### 1.4. Подгруппы, изоморфизмы, гомоморфизмы

Подмножество элементов группы  $G$  может само оказаться группой относительно умножения, определенного в  $G$ . Такое множество  $H$  элементов называется *подгруппой* группы  $G$ .

В любой группе  $G$  единица 1 удовлетворяет условию  $1^2 = 1$ . Наоборот, если элемент  $x \in G$  обладает свойством  $x^2 = x$ , то  $x = x^{-1}(x^2) = x^{-1}x = 1$ . Таким образом, единица подгруппы  $H$ , так как она удовлетворяет уравнению  $x^2 = x$ , должна совпадать с единицей группы  $G$ .

**Теорема 1.4.1.** *Подмножество  $H$  группы  $G$  является подгруппой, если выполняются два условия:*

S1. *Если  $h_1 \in H$ ,  $h_2 \in H$ , то  $h_1h_2 \in H$ .*

S2. *Если  $h_1 \in H$ , то  $h_1^{-1} \in H$ .*

*Доказательство.* Эти два свойства обеспечивают выполнение законов G0, G2, G3 в  $H$ . А так как произведения в  $H$  совпадают с произведениями в группе  $G$ , условие G1 также выполняется в  $H$ .

Между парами групп могут иметь место различные отношения, заслуживающие внимания. Первым таким отношением является *изоморфизм*.

**Определение.** *Взаимно однозначное отображение  $G \rightleftarrows H$  группы  $G$  на группу  $H$  называется изоморфизмом, если из  $g_1 \rightleftarrows h_1$  и  $g_2 \rightleftarrows h_2$  следует, что  $g_1g_2 \rightleftarrows h_1h_2$ .*

**Пример 1.** Так как все подстановки некоторого множества образуют группу (теорема 1.2.2), любое множество подстановок, удовлетворяющее условиям S1 и S2, составляет подгруппу полной группы подстановок. Например, рассмотрим две следующие подгруппы:

$$\begin{array}{ll} G_1 & G_2 \\ x_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, & y_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}, \\ x_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, & y_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 6 & 4 & 5 \end{pmatrix}, \\ x_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, & y_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 5 & 6 & 4 \end{pmatrix}, \\ x_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, & y_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \\ x_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, & y_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 3 & 1 & 2 \end{pmatrix}, \\ x_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, & y_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix}. \end{array}$$

Если отображать  $x_i \in G_1$  на  $y_i \in G_2$ , то во всех случаях произведению будет соответствовать произведение. Значит,  $G_1$  и  $G_2$  изоморфны.

В более общем случае отображение элементов одной группы  $G$  на элементы другой группы  $H$ , при котором, вообще говоря, нескольким элементам соответствует один, называется **гомоморфизмом**, если это отображение сохраняет произведение.

**Определение.** Отображение  $G \rightarrow H$  элементов группы  $G$  на элементы группы  $H$  называется **гомоморфизмом**, если из  $g_1 \rightarrow h_1$  и  $g_2 \rightarrow h_2$  следует, что  $g_1 g_2 \rightarrow h_1 h_2$ .

Пусть  $1$  — единица группы  $G$ , и пусть  $1 \rightarrow e$  ( $e \in H$ ) при гомоморфизме  $G \rightarrow H$ . Тогда  $1^2 \rightarrow e^2$ . Так как  $1^2 = 1$ , то  $e^2 = e$ . Поэтому  $e$  — единица группы  $H$ . Также если  $g \rightarrow h$  и  $g^{-1} \rightarrow k$ , то  $gg^{-1} \rightarrow hk$ , и поэтому  $1 \rightarrow hk = e$ . Значит,  $k = h^{-1}$ , т. е. отображение переводит обратные элементы в обратные. Отметим, что взаимно однозначный гомоморфизм есть изоморфизм.

**Пример 2.** Пусть  $G_1$  — та же группа подстановок, что и в примере 1,  $H$  — мультиликативная группа двух вещественных чисел  $1, -1$ . Тогда гомоморфизмом является отображение

$$\begin{array}{ll} x_1 \rightarrow 1 & x_4 \rightarrow -1 \\ x_2 \rightarrow 1 & x_5 \rightarrow -1 \\ x_3 \rightarrow 1 & x_6 \rightarrow -1. \end{array}$$

Группы подстановок интересны не только сами по себе, но еще и потому, что любая группа изоморфна некоторой группе подстановок.

**Теорема 1.4.2.** (Кэли) Произвольная группа  $G$  изоморфна некоторой группе подстановок своих элементов.

**Доказательство.** Для каждого  $g \in G$  определим отображение  $R(g) : x \rightarrow xg$  для всех  $x \in G$ . При фиксированном  $g$  получаем отображение множества всех элементов группы  $G$  на себя, так как для данного  $g$  отображение  $R(g)$  дает  $yg^{-1} \rightarrow (yg^{-1})g = y$ . Это отображение взаимно однозначно, т. к. из  $x_1g = x_2g$  следует  $x_1 = x_2$ . Итак,  $R(g)$  — подстановка для каждого  $g \in G$ . Отображение  $R(g_1)R(g_2)$  — это соответствие  $x \xrightarrow{R(g_1)} g_1 x \xrightarrow{R(g_2)} g_2 = x(g_1g_2)$ . Поэтому  $R(g_1)R(g_2) = R(g_1g_2)$ . Далее, при  $R(g_1)$  единица отображается в  $g_1$ , а при  $R(g_2)$  — в  $g_2$ . Поэтому если  $g_1 \neq g_2$ , то  $R(g_1) \neq R(g_2)$ . Значит, отображение  $g \xrightarrow{R(g)}$  является изоморфизмом. Отметим, что  $R(1) = I$  — тождественная подстановка и что  $R(g^{-1})R(g) = I$ , так что  $R(g^{-1}) = [R(g)]^{-1}$ .

Группу подстановок  $R(g) : x \xrightarrow{R(g)} xg$  называют **правым регулярным представлением** группы  $G$ . Можно было бы рассматривать подстановки  $L(g) : x \xrightarrow{L(g)} gx$ , т. е. **левое регулярное представление** группы  $G$ . Легко видеть, что группа  $L(g)$  анти-

изоморфна  $G$ . Это означает, что отображение  $g \rightarrow L(g)$  взаимно однозначно и переставляет сомножители, т. е.  $L(g_1g_2) = L(g_2)L(g_1)$ .

Рассмотрим множество подгрупп  $H_j$  группы  $G$ , где  $j$  пробегает некоторое множество индексов  $J$ . Тогда множество элементов группы  $G$ , каждый из которых принадлежит всем подгруппам  $H_j$ , удовлетворяет условиям S1 и S2 и поэтому составляет подгруппу  $H$ , называемую *пересечением* подгрупп  $H_j$ . Пересечение мы будем записывать так:  $H = \bigcap_j H_j$ . Множество всех конечных

произведений вида  $g_1g_2 \dots g_s$ , где каждый элемент  $g_i$  принадлежит некоторой подгруппе  $H_j$ , также удовлетворяет S1 и S2. Это множество составляет подгруппу  $T$ , называемую *объединением* подгрупп  $H_j$  и обозначаемую так:  $T = \bigcup_j H_j$ . Пересечение и объединение двух подгрупп  $H$  и  $K$  соответственно будем записывать так:  $H \cap K$  и  $H \cup K$ . Это обозначение согласуется с обозначением в теории структур и будет рассмотрено более детально в гл. 8.

Произвольное множество элементов группы называется *комплексом*. Если  $A$  и  $B$  — два комплекса в группе  $G$ , то под  $AB$  будем понимать комплекс, состоящий из всех элементов вида  $ab$ , где  $a \in A$ ,  $b \in B$ , и будем называть  $AB$  произведением комплексов  $A$  и  $B$ . Легко проверяется ассоциативный закон  $(AB)C = A(BC)$  для умножения комплексов.

Если  $K$  — некоторый комплекс в группе  $G$ , обозначим через  $\{K\}$  подгруппу, состоящую из всех конечных произведений  $x_1 \dots x_n$ , где  $x_i$  — элемент из  $K$  или обратный к нему. Говорят, что подгруппа  $\{K\}$  порождена множеством  $K$ . Легко видеть, что  $\{K\}$  содержится в любой подгруппе группы  $G$ , содержащей  $K$ .

## 1.5. Смежные классы. Теорема Лагранжа. Циклические группы. Индексы

Пусть даны группа  $G$  и подгруппа  $H$ . Множество элементов вида  $hx$ , где  $h$  — любой элемент из  $H$ , а  $x$  — фиксированный элемент из  $G$ , называется *левым смежным классом* по  $H$  и обозначается  $Hx$ . Аналогично множество элементов вида  $xh$ , где опять  $h$  — любой элемент из  $H$ , называется *правым смежным классом*  $xH$  по подгруппе  $H$ .

**Теорема 1.5.1.** *Два левых (правых) смежных класса группы  $G$  по  $H$  или не пересекаются, или совпадают. Левый (правый) смежный класс по  $H$  и подгруппа  $H$  равномощны.*

*Доказательство.* Если смежные классы  $Hx$  и  $Hy$  не имеют общих элементов, то нечего доказывать. Поэтому предположим, что  $z \in Hx$  и  $z \in Hy$ . Тогда  $z = h_1x = h_2y$ . Отсюда  $x = h_1^{-1}h_2y$  и  $hx = h_1^{-1}h_2y = h'y$ . Поэтому  $Hx \subseteq Hy$ . Аналогично  $hy =$

$= hh_2^{-1}h_1x = h''x$ , откуда  $Hu \subseteq Hx$ . Значит,  $Hx = Hu$ , т. е. классы совпадают. Для правых классов доказательство аналогично. Соответствия  $h \rightarrow hx$ ,  $h \rightarrow xh$ ,  $h \in H$ , показывают, что множества  $H$ ,  $Hx$  и  $xH$  равномощны.

Элемент  $x = x_1 = 1x$ , принадлежащий смежным классам  $xH$  и  $Hx$ , называется *представителем* смежного класса. Согласно теореме 1.5.1, любой элемент  $u \in Hx$  может быть выбран в качестве представителя, т. к.  $Hu = Hx$ . Таким образом, подгруппа  $H = H_1 = 1H$  сама является одним из смежных классов  $G$  по  $H$ . Обычно удобно (а иногда и необходимо) выбрать единицу в качестве представителя подгруппы  $H$ , рассматриваемой как один из смежных классов. Чтобы отметить, что смежные классы  $H$ ,  $Hx_2, \dots, Hx_r$ , не пересекаются и исчерпывают всю группу  $G$ , употребляется запись

$$G = H + Hx_2 + \dots + Hx_r. \quad (1.5.1)$$

Здесь сложение — лишь удобное обозначение; его не следует рассматривать как операцию.

Поскольку  $(Hx)^{-1}$  (множество элементов, обратных к элементам вида  $hx$ ) совпадает с  $x^{-1}H$  и  $(yH)^{-1} = Hy^{-1}$ , имеется взаимно однозначное соответствие между левыми и правыми смежными классами по  $H$ . Поэтому из (1.5.1) получаем

$$G = H + x_2^{-1}H + \dots + x_r^{-1}H. \quad (1.5.2)$$

Кардинальное число  $r$  правых (левых) смежных классов по подгруппе  $H$  группы  $G$  называется *индексом* подгруппы  $H$  в группе  $G$  и обозначается  $[G : H]$ . *Порядком* группы  $G$  называется кардинальное число ее элементов. Единица группы составляет подгруппу, и смежные классы по ней содержат по одному элементу. Поэтому порядок группы равен индексу единичной подгруппы.

**Теорема 1.5.2. (Теорема Лагранжа).** *Порядок группы  $G$  равен произведению порядка подгруппы  $H$  на индекс  $H$  в  $G$ .*

*Доказательство.* Число элементов в каждом из  $r = [G : H]$  смежных классов  $G$  по  $H$  равно числу элементов в подгруппе  $H$ , т. е. ее порядку.

Если  $H$  — подгруппа в  $G$  и  $K$  — подгруппа в  $H$ , то пусть

$$\begin{aligned} G &= H + Hx_2 + \dots + Hx_s, \\ H &= K + Ky_2 + \dots + Ky_r. \end{aligned}$$

Тогда для  $g \in G$  представление  $g = hx_j$ , где  $h \in H$ , однозначно, как и представление  $h = ky_i$ , где  $k \in K$ , для элемента  $h \in H$ . Поэтому  $Ky_i x_j$  ( $i = 1, \dots, r$ ;  $j = 1, \dots, s$ ) — смежные классы группы  $G$  по подгруппе  $K$ . Для того чтобы два таких смежных класса совпадали, они должны принадлежать одному и тому же

смежному классу по  $H$ , и поэтому им должен соответствовать один и тот же представитель  $x_j$ . Умножая  $K_{ij}x_j$  на  $x_j^{-1}$  справа, мы видим, что для них должны также совпадать и представители  $y_i$ . Таким образом, смежные классы  $G$  по  $K$  задаются комплексами  $K_{ij}x_j$ , причем эти выражения представляют различные классы. Итак, мы доказали теорему.

**Теорема 1.5.3.** *Если  $G \supseteq H \supseteq K$ , то  $[G : K] = [G : H] \cdot [H : K]$ .*

Группа  $G$  называется *циклической*, если каждый ее элемент является степенью  $b^t$  некоторого фиксированного элемента  $b$ . Пользуясь равенством  $(b^{-1})^r = b^{-r}$  и ассоциативным законом, можно показать методом полной индукции, что  $b^m b^t = b^{m+t}$  для любых целых показателей  $m$  и  $t$ . Если все степени элемента  $b$  различны, то циклическая группа имеет бесконечный порядок и изоморфна аддитивной группе всех целых чисел; при этом целые числа являются показателями степени образующего элемента  $b$ . Если же не все степени различны и, например,  $b^m = b^t$  при  $m > t$ , то  $b^{m-t} = 1$ , где  $m - t > 0$ . Пусть  $n > 0$  — наименьшее положительное целое число, для которого  $b^n = 1$ . Тогда легко видеть, что элементы  $1, b, \dots, b^{n-1}$  составляют всю группу и что при  $0 \leq r, s < n$  имеем  $b^r b^s = b^{r+s}$ , если  $r+s < n$ , и  $b^r b^s = b^{r+s-n}$ , если  $r+s \geq n$ . Отсюда нетрудно убедиться в том, что для каждого положительного  $n$  существует, с точностью до изоморфизма, одна единственная циклическая группа порядка  $n$ . Она является аддитивной группой классов вычетов целых чисел по модулю  $n$ . Таким образом, циклическая группа, порожденная элементом  $b$ , имеет порядок, равный либо бесконечности, либо  $n$ , причем в последнем случае  $n$  есть наименьшее положительное целое число, для которого  $b^n = 1$ . Назовем *порядком элемента  $b$*  порядок порождаемой им циклической группы  $\{b\}$ .

Строение и число подгрупп группы  $G$ , безусловно, очень важны для описания группы  $G$ . Но если  $G$  не содержит подгрупп, кроме самой себя и единичной, то не существует истинных подгрупп, которые раскрывали бы ее строение. В этом случае имеется очень простое прямое описание группы  $G$ .

**Теорема 1.5.4.** *Группа  $G$ , отличная от единичной, не содержит подгрупп, отличных от единичной и самой себя, тогда и только тогда, когда она является конечной циклической группой простого порядка.*

*Доказательство.* По предположению, если  $b \neq 1$  — элемент из  $G$ , то циклическая группа, порожденная элементом  $b$ , отлична от единичной и должна совпадать с  $G$ . Если  $b$  — элемент бесконечного порядка, то  $b^2$  порождает собственную подгруппу, состоящую из элементов вида  $b^{2j}$ . Поэтому  $b$  — элемент конечного порядка  $n$ , т. е.  $b^n = 1$ . Если  $n$  — непростое число, то  $n = uv$ , где

$u > 1$ ,  $v > 1$ . Тогда степень  $b^u$  порождает собственную подгруппу порядка  $v$ . Поэтому число  $n$  простое, а  $G$  — циклическая группа простого порядка. По теореме Лагранжа группа простого порядка не может содержать подгруппу, отличную от единичной и всей группы. Докажем основное соотношение для индексов подгрупп.

Теорема 1.5.5. (Неравенство для индексов.)  $[A \cup B : B] \geq [A : A \cap B]$ .

*Доказательство.* Обозначим подгруппу  $A \cap B$  через  $D$ . Пусть  $A = D1 + Dx_2 + \dots + Dx_r$ . Утверждается, что все смежные классы  $B1, Bx_2, \dots, Bx_r$  различны в  $A \cup B$ . Действительно, если  $Bx_i = Bx_j$  при  $i \neq j$ , то  $x_j = bx_i$  при  $b \in B$ . Но ведь элементы  $x_i$  и  $x_j$  принадлежат  $A$  и, значит,  $b \in A$ , т. е.  $b \in A \cap B = D$ . Следовательно, смежные классы  $Dx_i$  и  $Dx_j$  имеют общий элемент  $x_j = bx_i$ , что противоречит допущению. Значит, смежных классов в  $A \cup B$  по  $B$  не меньше, чем в  $A$  по  $A \cap B$ . Этим неравенство доказано.

Теорема 1.5.6. (Равенство индексов.) Если числа  $[A \cup B : B]$  и  $[A \cup B : A]$  конечны и взаимно просты, то  $[A \cup B : B] = [A : A \cap B]$  и  $[A \cup B : A] = [B : A \cap B]$ .

*Доказательство.* Согласно теореме 1.5.3,  $[A \cup B : A \cap B] = [A \cup B : B][B : A \cap B] = [A \cup B : A][A : A \cap B]$ . По теореме 1.5.5  $[A \cup B : B] \geq [A : A \cap B]$ . Но из приведенного равенства следует, что  $[A \cup B : B]$  делит  $[A : A \cap B]$ , так как оно взаимно просто с  $[A \cup B : A]$ . Поэтому  $[A \cup B : B] = [A : A \cap B]$  и аналогично  $[A \cup B : A] = [B : A \cap B]$ .

## 1.6. Сопряженные элементы и классы

Пусть  $G$  — группа и  $S$  — некоторое ее подмножество. Тогда множество  $S'$  элементов вида  $x^{-1}sx$ , где  $s \in S$ , а  $x$  — фиксированный элемент группы, называется *трансформацией* множества  $S$  элементом  $x$  и записывается в виде  $S' = x^{-1}Sx$ , или  $S' = S^x$ .

Лемма 1.6.1. Множества  $S$  и  $S^x$  равномощны.

*Доказательство.* Соответствие  $s \xrightarrow{x^{-1}sx}$  является взаимно однозначным, так как если  $s \rightarrow x^{-1}sx = s'$ , то  $s' \rightarrow xs'x^{-1} = x(x^{-1}sx)x^{-1} = s$  — обратное отображение.

Если  $S$  и  $S'$  — два множества в группе  $G$ , содержащей подгруппу  $H$ , и если существует такой элемент  $x \in H$ , что  $S' = S^x$ , то мы говорим, что  $S$  и  $S'$  *сопряжены* по подгруппе  $H$ . Если  $S' = x^{-1}Sx$ , то  $S = (x^{-1})^{-1}S'x^{-1}$ . Кроме того, если  $S'' = y^{-1}S'y$ , то  $S'' = y^{-1}x^{-1}Sxy = (xy)^{-1}S(xy)$ . Так как  $S = 1^{-1}S1$ , мы получаем, что отношение множеств быть сопряженными по  $H$  является отношением эквивалентности, т. к. оно рефлексивно, симмет-

\*) Элемент  $x$  называется *трансформирующим* элементом. — Прим. перев.

рично и транзитивно. Назовем множество всех множеств  $S'$ , сопряженных с данным множеством  $S$ , *классом сопряженных множеств*. Из равенств  $(x^{-1}sx)^{-1} = x^{-1}s^{-1}x$  и  $x^{-1}s_1x \cdot x^{-1}s_2x = x^{-1}(s_1s_2)x$  следует

**Лемма 1.6.2.** *Любое множество, сопряженное с подгруппой, есть также подгруппа.*

Если  $x^{-1}Sx = S$ , то  $S = xSx^{-1}$ . Если также  $y^{-1}Sy = S$ , то  $S = (xy)^{-1}S(xy)$ . Следовательно, множество всех таких  $x \in H$ , что  $S^x = S$ , есть подгруппа в  $H$ , которую мы будем называть *нормализатором* множества  $S$  в  $H$  и обозначать  $N_H(S)$ . Аналогично можно показать, что множество таких элементов  $x \in H$ , что  $x^{-1}sx = s$  для всех  $s \in S$ , является подгруппой в  $H$ ; мы будем называть ее *централизатором* множества  $S$  в  $H$  и обозначать  $C_H(S)$  (или  $Z_H(S)$ , если следовать немецкому правописанию). Отметим, что в случае одноэлементного множества  $S$  понятия нормализатора и централизатора совпадают; кроме того, всегда  $C_H(S) \subseteq N_H(S)$ . Если  $H = G$ , обычно говорят просто о нормализаторе и централизаторе множества  $S$ . Централизатор  $Z$  группы  $G$  в  $G$  называется *центром* группы  $G$ .

**Теорема 1.6.1.** *Число множеств, сопряженных с  $S$  по  $H$ , равно индексу в  $H$  нормализатора множества  $S$  в  $H$ , т. е.  $[H : N_H(S)]$ .*

*Доказательство.* Положим для краткости  $N_H(S) = D$ , и пусть

$$H = D + Dx_2 + \dots + Dx_r, \quad r = [H : N_H(S)].$$

Тогда равенство  $x^{-1}Sx = y^{-1}Sy$ , где  $x, y \in H$ , имеет место в том и только в том случае, когда  $S = (yx^{-1})^{-1}S(yx^{-1})$ , т. е. когда  $yx^{-1} \in D$ , или  $y \in Dx$ . Отсюда два сопряженных с  $S$  по  $H$  множества совпадают тогда и только тогда, когда трансформирующие элементы принадлежат одному левому смежному классу по  $D$ . Поэтому число различных сопряженных с  $S$  множеств равно индексу  $D$  в  $H$ , что и требовалось доказать.

Если  $S$  состоит из одного элемента  $s$ , то элементы, сопряженные с ним в  $G$ , образуют *класс сопряженных элементов*. Множество всех элементов группы  $G$  распадается на непересекающиеся классы сопряженных элементов, что записываем так:

$$G = C_1 + C_2 + \dots + C_s. \quad (1.6.1)$$

Единица 1 всегда образует отдельный класс. Согласно теореме 1.6.1, число элементов в классе  $C_i$  равно индексу некоторой подгруппы  $i$ , следовательно, делит порядок группы  $G$ .

## 1.7. Двойные смежные классы

Пусть  $G$  — группа,  $H$  и  $K$  — две (не обязательно различные) ее подгруппы. Множество элементов вида  $HxK$ , где  $x$  — фикси-

рованный элемент из  $G$ , называется *двойным смежным классом группы  $G$* . Как и для обычных смежных классов, имеет место

**Лемма 1.7.1.** *Два двойных смежных класса  $HxK$  и  $HyK$  либо совпадают, либо не пересекаются.*

**Доказательство.** Если  $z = h_1xk_1 = h_2yk_2$ , то  $h_1xk_1 = h_2^{-1}h_2yk_2k_1^{-1}k$ , откуда  $HxK \subseteq HyK$ ; аналогично  $HyK \subseteq HxK$ . Отсюда  $HxK = HyK$ .

Двойной смежный класс  $HxK'$  содержит все левые смежные классы по  $H$  вида  $Hxk$  и все правые смежные классы по  $K$  вида  $hxK$ . Кроме того, ясно, что  $HxK'$  состоит из полных левых смежных классов по  $H$  и полных правых смежных классов по  $K$ .

**Теорема 1.7.1.** *Число левых смежных классов по  $H$  в  $HxK$  равно  $[K : K \cap x^{-1}Hx]$ , а число правых смежных классов по  $K$  в  $HxK$  равно  $[x^{-1}Hx : K \cap x^{-1}Hx]$ .*

**Доказательство.** Установим следующее взаимно однозначное соответствие между множествами  $HxK$  и  $x^{-1}HxK : hxk \xrightarrow{\sim} x^{-1}hxk$ . Тем самым установлено взаимно однозначное соответствие между левыми смежными классами  $Hxk$  по  $H$  в  $HxK$  и левыми смежными классами  $x^{-1}Hx \cdot k$  по  $x^{-1}Hx$  в  $x^{-1}HxK$ , а также между правыми смежными классами  $hxK$  по  $K$  в  $HxK$  и правыми смежными классами  $x^{-1}hxK$  по  $K$  в  $x^{-1}HxK$ . Условимся, что  $x^{-1}Hx = A$  и  $A \cap K = D$ . Если теперь  $A = 1 \cdot D + u_2D + \dots + u_rD$ ,  $r = [A : D]$ , то  $u_i \in A$ , откуда  $K$ ,  $u_2K, \dots, u_rK$  — правые смежные классы по  $K$  в  $AK$ . Все они различны, так как если бы  $u_iK = u_jK$ , то  $u_i^{-1}u_j \in K$ , но поскольку  $u_i, u_j \in A$ , это означало бы, что  $u_i^{-1}u_j \in D$ , т. е.  $u_iD = u_jD$ , но это противоречит допущению. Каждый правый смежный класс по  $K$  в  $AK$  имеет вид  $aK$ , где  $a \in A$ . Но элемент  $a$  можно представить как  $u_id$ , где  $d \in D$ , отсюда  $u_idK = u_iK$ . Таким образом, число правых смежных классов по  $K$  в  $AK$  равно  $[A : D] = [x^{-1}Hx : x^{-1}Hx \cap K]$ , и в силу взаимной однозначности соответствия это число равно числу правых смежных классов по  $K$  в  $HxK$ . Аналогично можно показать, что число левых смежных классов по  $A$  в  $AK$  равно  $[K : D] = [K : x^{-1}Hx \cap K]$ , т. е. в силу взаимно однозначного соответствия равно числу левых смежных классов по  $H$  в  $HxK$ <sup>1)</sup>.

<sup>1)</sup> Разложение группы  $G$

$$G = Hx_1K + Hx_2K + \dots + Hx_rK$$

В сумму непересекающихся двойных классов будем в дальнейшем называть *разложением группы  $G$  по двойному модулю  $(H, K)$* . Этим разложением автор неоднократно будет пользоваться на протяжении книги. — Прим. ред.

## 1.8. Замечания о бесконечных группах

Многие теоремы о группах не зависят от того, конечен ли их порядок или бесконечен. Но иногда результаты для конечных и бесконечных групп существенно различны, а в случае одинаковых результатов различны методы доказательств.

Бесконечная группа  $G$  может обладать теми или иными свойствами конечности. Важными свойствами такого рода будут, например, следующие:

- 1)  $G$  — группа с конечным числом образующих,
- 2)  $G$  — *периодична*, т. е. все элементы группы  $G$  конечного порядка,

3)  $G$  удовлетворяет условию *максимальности*: каждая возрастающая цепочка  $A_1 \subset A_2 \subset A_3 \subset \dots$  различных подгрупп обрывается,

4)  $G$  удовлетворяет условию *минимальности*: каждая убывающая цепочка  $A_1 \supset A_2 \supset \dots$  различных подгрупп обрывается.

Говорят, что бесконечная группа  $G$  обладает некоторым свойством *локально*, если этим свойством обладает любая ее конечно порожденная подгруппа. Семейство  $H_i$  гомоморфных образов группы  $G$  называется *семейством остатков* для  $G$ , если для любого  $g \neq 1$  из  $G$  существует по крайней мере одна группа  $H_i$ , в которой образ элемента  $g$  не является единицей. Мы будем говорить, что некоторое свойство выполняется в  $G$  *остаточно*, если существует семейство остатков, состоящее из гомоморфных образов группы  $G$ , каждый из которых обладает этим свойством.

**Теорема 1.8.1.** Группа  $G$  удовлетворяет условию максимальности тогда и только тогда, когда  $G$  и все ее подгруппы конечно порождены.

**Доказательство.** Предположим, что некоторая подгруппа  $H$  группы  $G$  не имеет конечной системы образующих. Тогда можно построить бесконечную возрастающую цепочку различных подгрупп в  $H$ :  $\{h_1\} \subset \{h_1, h_2\} \subset \dots \subset \{h_1, \dots, h_i\} \subset \dots$ , выбирая последовательно произвольное  $h_i \in H$ , не принадлежащее  $\{h_1, \dots, h_{i-1}\}$ . Такое  $h_i$  всегда найдется, так как  $H$  не может быть подгруппой, порожденной множеством  $\{h_1, \dots, h_{i-1}\}$ . Обратно, пусть  $G$  и все ее подгруппы конечно порождены. Пусть тогда  $B_1 \subseteq B_2 \subseteq B_3 \subseteq \dots$  — неубывающая цепочка подгрупп группы  $G$ . Покажем, что, начиная с некоторого места, все подгруппы совпадают и, следовательно, не существует бесконечной возрастающей цепочки различных подгрупп. Множество всех таких элементов  $b$  группы  $G$ , что  $b \in B_i$  для некоторого  $B_i$  из цепочки, составляет подгруппу  $B$  группы  $G$ , так как если  $b \in B_i$  и  $b' \in B_j$ , то элементы  $b$  и  $b'$  принадлежат любой подгруппе  $B_k$ , где  $k \geq i, k \geq j$ , а поэтому также их произведения и обратные к ним элементы лежат в  $B_k$ .

По предположению,  $B$  — подгруппа с конечным числом образующих, скажем,  $x_1, \dots, x_n$ . Пусть  $B_{j_1}$  — первая подгруппа среди  $B_i$ , содержащая  $x_1$ , и вообще  $B_{j_k}$  — первая подгруппа среди  $B_i$ , содержащая  $x_k$  ( $k = 1, \dots, n$ ). Пусть  $m$  — наибольшее из чисел  $j_1, \dots, j_n$ . Тогда  $B_m$  содержит все образующие  $x_1, \dots, x_n$ , а потому  $B = B_m = B_{m+1} = \dots$  и все дальнейшие подгруппы в цепочке совпадают с  $B$ . Несколько позже мы увидим, что существуют конечно порожденные группы, которые обладают подгруппами, не имеющими конечной системы образующих.

**Теорема 1.8.2.** *Группа  $G$ , удовлетворяющая условию минимальности, периодична.*

**Доказательство.** Если  $G$  содержит элемент  $b$  бесконечного порядка, то  $\{b\} \subset \{b^2\} \subset \{b^4\} \subset \dots \subset \{b^{2^i}\} \subset \dots$  является бесконечной убывающей цепочкой различных подгрупп.

При исследовании бесконечных групп мы не можем пользоваться методом полной индукции по порядкам групп. Поэтому возникает необходимость чем-то заменить этот метод доказательства, который так эффективен в теории конечных групп. Один из путей состоит в использовании самых общих аксиом теории множеств и упорядочения. Предположим, что в множестве  $S$  элементов  $\{a, b, c, \dots\}$  определено некоторое отношение порядка  $a \leqslant b$ . Это отношение может подчиняться некоторым из следующих аксиом:

O1) если  $a \leqslant b$  и  $b \leqslant a$ , то  $a = b$ ;

O2) если  $a \leqslant b$  и  $b \leqslant c$ , то  $a \leqslant c$ ;

O3) для любой пары  $a, b$  или  $a \leqslant b$ , или  $b \leqslant a$ ;

O4) любое непустое подмножество  $T$  множества  $S$  имеет первый элемент  $x_1$ , т. е. такой элемент  $x_1$ , что  $x_1 \leqslant t$  для любого  $t \in T$ .

Если имеют место первые две аксиомы, то говорят о *частичном упорядочении* множества. Если выполняются первые три аксиомы, то упорядочение называется *простым*. Если, наконец, все четыре аксиомы имеют место, то мы говорим, что множество *вполне упорядочено*. Мы будем пользоваться следующей аксиомой полного упорядочения: *любое множество может быть вполне упорядочено*. Условимся писать  $a < b$ , если  $a \leqslant b$ , но  $a \neq b$ .

Во вполне упорядоченном множестве можно доказывать предложения методом *трансфинитной индукции*. Это делается так. Обозначим через 1 первый элемент множества  $S$ . Пусть  $P(a)$  — некоторое утверждение об элементах множества  $S$ , пусть  $P(1)$  истинно и пусть из того, что  $P(x)$  истинно для всех  $x < a$ , следует истинность  $P(a)$ . Тогда мы заключаем, что  $P(b)$  истинно для всех  $b \in S$ . Действительно, пусть  $T$  есть такое подмножество  $S$ , что  $P(t)$  ложно для  $t \in T$ . Если  $T$  непусто, оно имеет первый

элемент  $c$ . Тогда или  $c = 1$ , или  $P(x)$  истинно для всех  $x < c$ . Но в обоих случаях отсюда следует, что  $P(c)$  истинно, что противоречит выбору  $c$  в множестве  $T$ . Значит,  $T$  пусто, и  $P(b)$  истинно для всех  $b \in S$ . Заметим, между прочим, что во вполне упорядоченном множестве любая убывающая последовательность  $a_1 > a_2 > a_3 > \dots$  обязательно конечна, так как она должна содержать первый элемент.

Другой аксиомой, логически эквивалентной аксиоме полной упорядоченности, является лемма Цорна. В ней опять идет речь об упорядочении множества.

**Лемма 1.8.1. (Лемма Цорна.)** *Если в частично упорядоченном множестве  $S$  любое просто упорядоченное подмножество имеет верхнюю (нижнюю) грань, то  $S$  имеет максимальный (минимальный) элемент.*

Если  $U$  — подмножество в  $S$ , то под *верхней гранью* множества  $U$  здесь понимается такой элемент  $b$ , что  $b \geqslant u$  для всех  $u \in U$ . *Максимальным элементом* при этом называется элемент, не имеющий отличных от себя верхних граней. Перевернув порядок включения, аналогично определяем *нижнюю грань* и *минимальный элемент*.

Рассмотрим множество подгрупп группы  $G$ , частично упорядоченное по включению:  $A \subseteq B$ , если  $A$  — подгруппа в  $B$ . Тогда множество всех элементов, содержащихся в некотором просто упорядоченном подмножестве подгрупп, образует подгруппу. Действительно, если  $g_1$  — элемент одной из подгрупп, а  $g_2$  — некоторой другой, то оба эти элемента содержатся в большей из этих подгрупп вместе со своими произведениями и обратными элементами. По этой причине леммой Цорна удобно пользоваться в теории групп и вообще абстрактных алгебр.

И аксиома полной упорядоченности, и лемма Цорна эквивалентны следующей аксиоме.

**Аксиома выбора.** *Для любого семейства  $F$  непустых подмножеств  $\{S_i\}$  множества  $S$  существует функция выбора  $f(S_i)$ , определенная на  $F$  со значениями в  $S$  такими, что  $f(S_i) = a_i \in S_i$ .*

Оказывается, при определенных заключениях аксиома выбора приводит к парадоксам и поэтому считается подозрительной. Все три принципа безусловно верны для счетного множества  $S$ , т. е. такого множества  $S$ , элементы которого можно поставить во взаимно однозначное соответствие с рядом натуральных чисел 1, 2, 3, .... По-видимому, они верны и для других множеств  $S$  и, возможно, для всех вполне определенных множеств, хотя нужно отметить, что фактически еще никто не построил полного упорядочения в множестве всех действительных чисел. Всякий раз, когда в этой книге мы будем пользоваться одним из этих принципов, выражение „любое множество  $S$ “ следует понимать в смысле

любое множество  $S$ , для которого аксиома выбора выполняется".

Полезным приложением этих методов является следующая

**Теорема 1.8.3.** Пусть  $g$  — элемент группы  $G$ ,  $H$  — ее подгруппа, не содержащая  $g$ . Тогда существует подгруппа  $M$ , содержащая  $H$  и максимальная среди всех подгрупп, не содержащих элемент  $g$ .

**Доказательство.** Воспользуемся леммой Цорна. Подгруппы, содержащие  $H$ , но не содержащие  $g$ , образуют частично упорядоченное множество по включению. Элементы любого просто упорядоченного множества этих подгрупп образуют подгруппу, которая содержит  $H$ , но не содержит  $g$ . Следовательно, существует максимальная подгруппа  $M$ , содержащая  $H$ , но не содержащая  $g$ .

Используя эту теорему, легко получаем следующую теорему.

**Теорема 1.8.4** Пусть  $G$  — конечно порожденная группа и  $H$  — истинная ее подгруппа. Тогда существует максимальная подгруппа  $M$  группы  $G$ , содержащая  $H$ .

**Доказательство.** Пусть  $x_1, \dots, x_m$  — образующие элементы группы  $G$ , и пусть  $y_1$  — первый среди них, не содержащийся в  $H$ . Пусть тогда  $M_1 \supseteq H$ , где  $M_1$  — максимальная подгруппа, не содержащая  $y_1$ . Тогда любая подгруппа, строго содержащая  $M_1$ , содержит  $y_1$ , а значит, и подгруппу  $\{M_1, y_1\} = H_1$ . Если  $H_1 = G$ , то  $M_1$  — искомая максимальная подгруппа. Если же  $H_1 \subset G$ , то выбираем подгруппу  $M_2 \supseteq H_1$ , где  $M_2$  — максимальная подгруппа, не содержащая  $y_2$ , — первый среди  $x_1, \dots, x_m$  элемент, не принадлежащий  $H_1$ . Так как  $G = \{x_1, \dots, x_m\}$ , то, продолжая этот процесс, мы должны достичь такой группы  $M_i$ , что  $M_i \supseteq H_{i-1} \supseteq \dots \supseteq H$ , где  $\{M_i, y_i\} = G$ . Тогда подгруппа  $M_i = M$  и есть искомая максимальная подгруппа.

## 1.9. Примеры групп

Взаимно однозначные отображения множества на себя, сохраняющие некоторое свойство, обычно образуют группу. Многие из наиболее интересных групп получаются именно таким образом. Примерами отображений такого рода являются симметрии геометрической фигуры и конгруэнтные (т. е. сохраняющие расстояния) отображения фигуры на себя. В приведенных ниже примерах групп первые две — группы симметрий.

**Пример 1.** Группы диэдра. Симметрии правильного многоугольника с  $n \geq 3$  сторонами составляют группу порядка  $2n$ . Они определяются полностью, если указать, как отображаются друг на друга вершины. Пронумеруем вершины числами  $1, 2, \dots, n$  по часовой стрелке. Вершина 1 может быть отображена на любую вершину  $1, 2, \dots, n$ , а остальные могут переместиться либо по

часовой стрелке, либо против. Все симметрии порождаются вращением

$$a = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 2 & 3 & 4 & \dots & n & 1 \end{pmatrix}$$

и отражением

$$b = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix}.$$

Здесь  $a^n = 1$ ,  $b^2 = 1$ ,  $ba = a^{-1}b$ . Более того, эти отношения полностью определяют группу, так как любой элемент, порожденный  $a$  и  $b$ , имеет вид  $a^{i_1}b^{j_1} \dots a^{i_r}b^{j_r}$ , и благодаря равенству  $ba^l = a^{-l}b$  (что легко получается из последнего соотношения) каждый элемент может быть приведен к виду  $a^l$  или  $a^l b$  при  $l = 0, 1, \dots, n-1$ . Это все  $2n$  различных элементов группы. Эти отношения также определяют группу для  $n=2$ , порядок которой равен 4. Она называется „четверной“ группой.

ПРИМЕР 2. Симметрии куба. Симметрии куба определяются отображениями восьми вершин куба на себя. Перенумеруем вершины куба так, как показано на рисунке.

Симметриями являются вращения

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 8 & 5 & 2 & 3 & 7 & 6 \end{pmatrix}$$

и отражение

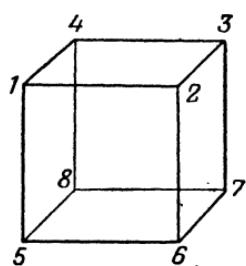


Рис. 1. Симметрии куба.

$$c = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix}.$$

Элементы  $a$  и  $b$  порождают группу  $G_1$ , отображающую каждую вершину в любую другую. Это видно из диаграммы

$$1 \xrightarrow{a} 2 \xrightarrow{a} 3 \xrightarrow{a} 4 \xrightarrow{b} 5 \xrightarrow{a} 6 \xrightarrow{a} 7 \xrightarrow{a} 8 \xrightarrow{a} 5 \xrightarrow{b} 2 \xrightarrow{a^{-1}} 1.$$

На этой диаграмме  $i \xrightarrow{x} j$  означает, что элемент  $x$  переводит  $i$  в  $j$ . Отсюда видно, что  $ba^2$  переводит 4 в 7. Элементы, оставляющие 1 на месте, образуют подгруппу  $H_1$  группы  $G_1$ , и мы можем разложить  $G_1$  по  $H_1$ :

$$G_1 = H_1 + H_1 x_2 + H_1 x_3 + H_1 x_4 + H_1 x_5 + H_1 x_6 + H_1 x_7 + H_1 x_8,$$

где  $x_i$  — элемент, переводящий 1 в  $i$ . В качестве  $x$ -ов мы можем взять  $x_2 = a$ ,  $x_3 = a^2$ ,  $x_4 = a^3$ ,  $x_5 = a^3b$ ,  $x_6 = a^3ba$ ,  $x_7 = a^3ba^2$ ,  $x_8 = a^3ba^3$ . Поскольку есть всего только восемь символов и все

элементы класса  $H_1x_i$  переводят 1 в то же самое  $l$ , здесь выписаны все возможные смежные классы по  $H_1$  и индекс  $H_1$  в  $G_1$  равен 8.

Вращение куба, оставляющее на месте вершину 1, должно циклически переставлять три смежные с 1 вершины. Поэтому  $H_1$  имеет порядок три и состоит из 1,  $b$ ,  $b^2$ , а, следовательно,  $G_1$  имеет порядок 24. Отображение  $c$  не содержится в  $G_1$ , но так как  $c^2 = 1$ ,  $ca = ac$  и  $cb = a^2ba^2c$ , мы видим, что группа  $G$ , порожденная элементами  $a$ ,  $b$  и  $c$ , разлагается в сумму  $G = G_1 + G_1c$  и порядок ее равен 48.  $G$  — полная группа симметрий куба.

**ПРИМЕР 3.** Каков порядок группы  $G$ , порожденной элементами  $a$  и  $b$ , подчиненными следующим отношениям:

$$a^7 = 1, \quad b^3 = 1, \quad ba = a^r b?$$

Каждый элемент  $g \in G$  может быть представлен как конечная последовательность букв  $a$  и  $b$ . Пользуясь соотношением  $ba = a^r b$ , мы можем представить его в виде

$$g = a^i b^j, \quad i = 0, 1, \dots, 6; \quad j = 0, 1, 2.$$

Отсюда видно, что порядок группы  $G$  не больше 21. Он зависит от значения  $r$  в соотношении  $ba = a^r b$ . Так как  $ba^2 = a^r ba = a^r(a^rb) = a^{2r}b$  и, аналогично,  $ba^i = a^{ir}b$ , то  $b^2a = ba^r b = a^rb^2$ , а отсюда  $b^2a^i = a^{ir}b^2$ . Используя это соотношение, получаем  $b^3a = ba^rb^2 = a^rb^3$ . Но ведь  $b^3 = 1$ . Поэтому отсюда получается, что  $a^r = a$ , а также  $a^7 = 1$ . Рассмотрим  $r = 1, 2, 3, 4, 5, 6$ . При  $r = 3, 5, 6$  получаем  $a = 1$ , и  $G$  — циклическая группа порядка 3 с образующим  $b$ . Но при  $r = 1, 2, 4$  ситуация иная. Если  $r = 1$ , то  $ba = ab = c$  — элемент порядка 21. Обратно, в циклической группе порядка 21, где  $c^{21} = 1$ , если положить  $b = c^7$ ,  $a = c^3$ , мы получаем  $a^7 = 1$ ,  $b^3 = 1$ ,  $ba = ab = c$ . При  $r = 2$  роль  $a$  и  $b$  могут выполнять подстановки

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 4 & 5 & 6 & 7 & 1 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 2 & 6 & 3 & 7 & 4 \end{pmatrix}.$$

При  $r = 4$  роль  $a$  и  $b$  могут выполнять соответственно первая из этих двух подстановок и обратная ко второй. Этот пример показывает, что небольшое видоизменение определяющих отношений может очень изменить определяемую ими группу.

**ПРИМЕР 4.** Определим группу подстановок семи букв  $A, B, C, D, E, F, G$ , которые переставляют между собой столбцы

следующей диаграммы, причем порядок букв в столбце несуществен:

$$\begin{aligned} A, & B, C, D, E, F, G; \\ B, & C, D, E, F, G, A; \\ D, & E, F, G, A, B, C. \end{aligned}$$

Сразу видно, что подстановка

$$a = \begin{pmatrix} A & B & C & D & E & F & G \\ B & C & D & E & F & G & A \end{pmatrix}$$

переставляет столбцы циклически. Тогда, если  $G$  — полная искомая группа подстановок и  $H$  — подгруппа, оставляющая первый столбец на месте, то смежный класс  $Ha^i$ ,  $i = 1, \dots, 6$ , состоит из всех элементов, отображающих первый столбец на  $(i+1)$ -ый. Следовательно,

$$G = H + \dots + Ha^6, \quad [G : H] = 7.$$

В подгруппе  $H$  могут быть элементы, переставляющие  $A$ ,  $B$  и  $D$  циклически. Это свойство не определяет отображение остальных букв, но если мы, кроме того, предположим, что  $C$  отображается на себя, то подстановка однозначно определится:

$$b = \begin{pmatrix} A & B & C & D & E & F & G \\ B & D & C & A & F & G & E \end{pmatrix}.$$

Если  $K$  — подгруппа, оставляющая на месте первый столбец и букву  $A$ , то

$$H = K + Kb + Kb^2, \quad b^3 = 1, \quad [H : K] = 3.$$

В подгруппе  $K$  укажем элемент, переставляющий  $B$  и  $D$ . Пусть это элемент

$$c = \begin{pmatrix} A & B & C & D & E & F & G \\ A & D & C & B & F & E & G \end{pmatrix}.$$

Отсюда, если  $T$  — подгруппа, оставляющая на месте буквы  $A$ ,  $B$  и  $D$ , имеем

$$K = T + Tc, \quad c^2 = 1, \quad [K : T] = 2.$$

Внутри подгруппы  $T$  три буквы  $A$ ,  $B$ ,  $D$  фиксированы, а буква  $C$  может отображаться на любую из четырех букв:  $C$ ,  $E$ ,  $F$ ,  $G$ .

Каждая из этих возможностей осуществляется точно одной из подстановок

$$\begin{pmatrix} A & B & C & D & E & F & G \\ A & B & C & D & E & F & G \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F & G \\ A & B & E & D & C & G & F \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F & G \\ A & B & F & D & G & C & E \end{pmatrix},$$

$$\begin{pmatrix} A & B & C & D & E & F & G \\ A & B & G & D & F & E & C \end{pmatrix}.$$

Таким образом,  $T$  имеет порядок 4,  $K$  — порядок 8,  $H$  — порядок 24, вся группа  $G$  — порядок 168. Если семь букв  $A, \dots, G$  рассматривать как точки, а столбцы как прямые, то диаграмма представляет конечную проективную плоскость из 7 точек, а группа  $G$  — группу ее коллинеаций.

**ПРИМЕР 5.** Группа кватернионов. Рассматриваемая группа порядка 8 во многих отношениях исключительна. Ее необычные свойства будут рассмотрены в § 5 гл. 12. Здесь мы хотим представить ее с помощью таблицы умножения, или таблицы Кэли, как ее называли в честь английского математика Кэли. На пересечении строки  $x_i$  и столбца  $x_j$  мы помещаем произведение  $x_k = x_i x_j$ .

$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$

$x_1$	$x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8$
$x_2$	$x_2, x_5, x_4, x_7, x_6, x_1, x_8, x_3$
$x_3$	$x_3, x_8, x_5, x_2, x_7, x_4, x_1, x_6$
$x_4$	$x_4, x_3, x_6, x_5, x_8, x_7, x_2, x_1$
$x_5$	$x_5, x_6, x_7, x_8, x_1, x_2, x_3, x_4$
$x_6$	$x_6, x_1, x_8, x_3, x_2, x_5, x_4, x_7$
$x_7$	$x_7, x_4, x_1, x_6, x_3, x_8, x_5, x_2$
$x_8$	$x_8, x_7, x_2, x_1, x_4, x_3, x_6, x_5$

В этой таблице каждое  $x_i$  встречается точно один раз в каждой строке и каждом столбце. Поэтому в произведении  $ab = c$  любые два элемента однозначно определяют третий. Тем самым рассматриваемая таблица является таблицей умножения квазигруппы. Проверка таблицы показывает также, что  $x_1 x_i = x_i x_1 = x_i$  для любого  $i$ . Таким образом,  $x_1 = 1$  — двусторонняя единица, и

таблица определяет лупу. Оба эти свойства сохраняются, если мы заменим последние две строки такими:

$$\begin{array}{c|ccccccccc} x_7 & x_7, & x_4, & x_2, & x_1, & x_3, & x_8, & x_6, & x_5 \\ x_8 & x_8, & x_7, & x_1, & x_6, & x_4, & x_3, & x_5, & x_2 \end{array}$$

Но, как утверждается, данная таблица — таблица умножения группы. Для доказательства необходимо проверить ассоциативный закон  $(ab)c = a(bc)$  для умножения. Полная проверка ассоциативного закона в этом случае состояла бы из  $8^3 = 512$  частных проверок. Несмотря на то, что проверка для случаев, когда один из элементов  $a, b, c$  равен 1, тривиальна, тем не менее остается еще 343 проверки. Здесь мы воспользуемся обращением теоремы Кэли 1.4.2.

**Теорема 1.9.1.** (Обратная к теореме Кэли.) *Лупа является группой, если ее правые регулярные отображения  $x \rightarrow xg$  составляют группу.*

**Доказательство.** При отображении  $R(g)R(h)$  имеем  $1 \rightarrow g \rightarrow gh$ . Но при отображении  $R(gh)$  также имеем  $1 \rightarrow gh$ , и это единственное отображение, переводящее 1 в  $gh$ . Следовательно,  $R(g)R(h) = R(gh)$ , откуда  $(xg)h = x(gh)$  для любого  $x$ , и ассоциативность установлена.

В нашем случае полагаем  $a = x_2, b = x_3$  и вычисляем

$$A = R(a) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_2 & x_5 & x_8 & x_3 & x_6 & x_1 & x_4 & x_7 \end{pmatrix},$$

$$B = R(b) = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ x_3 & x_4 & x_5 & x_6 & x_7 & x_8 & x_1 & x_2 \end{pmatrix}.$$

Здесь  $A^4 = B^4 = 1, A^2 = B^2, BA = A^3B$ . Легко заметить, что элементы  $A$  и  $B$ , подчиненные этим соотношениям, порождают группу порядка 8, являющуюся именно правым регулярным представлением данной лупы. Следовательно, рассматриваемая лупа есть группа. Вторые строки подстановок — не что иное, как столбцы таблицы умножения. В образующих  $a$  и  $b$  мы имеем  $x_1 = 1, x_2 = a, x_3 = b, x_4 = ab, x_5 = a^2 = b^2, x_6 = a^3, x_7 = b^3 = a^2b, x_8 = a^3b$ , причем  $a^4 = 1, b^4 = 1, b^2 = a^2, ba = a^3b$ .

## Упражнения

1. Показать, что из ассоциативного закона  $(ab)c = a(bc)$  следует независимость произведения  $a_1a_2 \dots a_n$  от расстановки скобок без изменения порядка сомножителей.

2. Показать, что в любой группе  $(ab)^{-1} = b^{-1}a^{-1}$  и вообще

$$(a_1a_2 \dots a_{n-1}a_n)^{-1} = a_n^{-1}a_{n-1}^{-1} \dots a_2^{-1}a_1^{-1}.$$

3. Показать, что  $a$  и  $a^{-1}$  — элементы равных порядков.

4. Показать, что элементы  $ab$  и  $ba$  имеют равные порядки. (Указание: они сопряжены.)

5. Если  $a^m = 1$ ,  $b^n = 1$ , где  $m$  и  $n$  — положительные целые числа, и  $ba = ab$ , показать, что  $(ab)^k = 1$ , где  $k$  — наименьшее общее кратное  $m$  и  $n$ . Найти пример, когда это неверно при  $ba \neq ab$ .

6. Показать, что если группа  $G$  содержит всего один элемент  $a$  порядка 2, то  $xa = ax$  для любого  $x \in G$ .

7. Показать, что единственной конечной группой с двумя классами сопряженных элементов является группа порядка 2.

8. Показать, что если  $p < q$  — простые числа, то группа порядка  $pq$  не может содержать двух различных подгрупп порядка  $q$ .

9. Показать, что если  $H$  — истинная подгруппа конечной группы  $G$ , то сопряженные с  $H$  подгруппы не содержат все элементы группы  $G$ .

10. Показать, что лупы порядков 1, 2, 3, 4 являются группами, и найти лупу порядка 5, которая не является группой.

11. Показать, что двойной класс  $HxK$  содержит точно те правые смежные классы по  $K$ , которые содержат по крайней мере один элемент из  $Hx$ .

12. (Вильям Скотт). Показать, что система с бинарным произведением и такой единицей 1, что  $1a = a1 = a$  для всех  $a$ , будет ассоциативной, если мы допустим равенство двух произведений  $a_1a_2 \dots a_n$ , взятых в одинаковом порядке, но с различной расстановкой скобок.

13. Исходя из аксиом первого определения группы, вывести единственность единицы 1 и обратного элемента  $a^{-1}$ .

14. Показать, что если  $A$  и  $B$  — две конечные подгруппы группы  $G$ , то комплекс  $AB$  содержит точно  $[A : 1][B : 1]/[A \cap B : 1]$  различных элементов.

## Г л а в а 2

### ИНВАРИАНТНЫЕ ПОДГРУППЫ И ГОМОМОРФИЗМЫ

#### 2.1. Инвариантные подгруппы

Подгруппа  $H$  группы  $G$  называется *инвариантной подгруппой*, или *нормальным делителем*, если  $x^{-1}Hx = H$  для всех  $x \in G$ . В терминах § 6 гл. 1 подгруппа  $H$  является инвариантной, если  $N_G(H) = G$ .

Лемма 2.1.1. *Подгруппа  $H$  в  $G$  инвариантна тогда и только тогда, когда каждый левый смежный класс  $Hx$  есть также и правый смежный класс  $xH$ .*

Доказательство. Если  $x^{-1}Hx = H$ , то  $Hx = xH$  и, обратно, если  $Hx = xH$ , то  $x \in yH$ . Отсюда  $yH = xH$ . Значит,  $xH = Hx$  для всех  $x \in G$ , а поэтому  $x^{-1}Hx = H$ .

Следствие 2.1.1. *Подгруппа индекса 2 — инвариантная подгруппа.*

Действительно, если  $G = H + Hx$ , то  $G = H + xH$ .

Для конечных групп из  $x^{-1}Hx \subseteq H$  вытекает  $x^{-1}Hx = H$ , так как подгруппы  $x^{-1}Hx$  и  $H$  имеют равные порядки; для бесконечных же групп из включения не всегда следует равенство. Тем не менее, если  $x^{-1}Hx \subseteq H$  и  $xHx^{-1} \subseteq H$ , то  $H = x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1} \subseteq H$ , откуда  $H = xHx^{-1}$  и, аналогично,  $H = x^{-1}Hx$ . Таким образом, включение  $x^{-1}Hx \subseteq H$  для всех  $x$  достаточно для того, чтобы подгруппа  $H$  была инвариантной.

Группа  $G$ , не содержащая истинных нормальных делителей, называется *простой*. Слово „простая“ следует понимать чисто условно. Группами без собственных подгрупп являются, согласно теореме 1.5.4, конечные циклические группы простых порядков. Эти группы являются простыми и согласно определению и в буквальном смысле (т. е. несложными). Но существует много других простых групп, например группа порядка 168, рассмотренная в примере 4 § 1.9. Все конечные простые группы до сих пор ещё не описаны. Было высказано предположение, что простые конечные группы, за исключением групп простого порядка, имеют четный порядок. Но, кажется, доказательство даже этого утверждения необычайно трудно.

## 2.2. Ядро гомоморфизма

Пусть группа  $H$  — гомоморфный образ группы  $G$ . Рассмотрим множество  $T$  элементов  $t \in G$ , отображаемых на единицу группы  $H$ :

$$G \rightarrow H, \quad T \rightarrow 1. \quad (2.2.1)$$

Как отмечалось в § 1.4,  $1 \rightarrow 1$ , откуда  $1 \in T$ . Если  $t \rightarrow 1$ ,  $t^{-1} \rightarrow u$ , то  $1 = t \cdot t^{-1} \rightarrow u$ , но  $1 \rightarrow 1$ , значит,  $u = 1$ , т. е.  $t^{-1} \rightarrow 1$ , и  $t^{-1} \in T$ . Далее, если  $t_1 \rightarrow 1$  и  $t_2 \rightarrow 1$ , то  $t_1 t_2 \rightarrow 1$ , откуда  $t_1 t_2 \in T$ . Следовательно,  $T$  — подгруппа группы  $G$ . Более того, если  $x \in G$ ,  $t \in T$ , то  $x \rightarrow y$ ,  $t \rightarrow 1$ ,  $x^{-1} \rightarrow y^{-1}$ , откуда  $x^{-1} t x \rightarrow y^{-1} 1 y = 1$ , т. е.  $x^{-1} t x \in T$ . Поэтому  $T$  — нормальный делитель в  $G$ . Множество  $T$  называется **ядром гомоморфизма**  $G \rightarrow H$ .

**Теорема 2.2.1.** (ПЕРВАЯ ТЕОРЕМА О ГОМОМОРФИЗМАХ.) *При гомоморфизме  $G \rightarrow H$  множество  $T$  элементов группы  $G$ , отображаемых на единицу группы  $H$ , является нормальным делителем в  $G$ . Два элемента из  $G$  имеют один и тот же образ в  $H$  тогда и только тогда, когда они лежат в одном смежном классе по  $T$ .*

**Доказательство.** Мы уже показали, что  $T$  — инвариантная подгруппа в  $G$ . Пусть  $x \rightarrow u$ ,  $y \rightarrow u$ ,  $x \in G$ ,  $y \in G$ ,  $u \in H$ . Тогда  $xy^{-1} \rightarrow 1$ , т. е.  $xy^{-1} \in T$ , откуда  $x \in Ty$ , т. е.  $x$  и  $y$  лежат в одном смежном классе по  $T$ . Обратно, если  $x \in Ty$ , т. е.  $x = ty$ , и  $y \rightarrow u$ , то (так как  $t \rightarrow 1$ )  $x \rightarrow u$ , т. е. образы элементов  $x$  и  $y$  совпадают.

## 2.3. Фактор-группы

В предыдущем параграфе было показано, что ядро гомоморфизма группы  $G$  есть нормальный делитель  $T$ . Верно и обратное утверждение: любой нормальный делитель  $T$  есть ядро некоторого гомоморфизма, причем этот гомоморфизм определяется единственным образом. Пусть

$$G = T + Tx_2 + \dots + Tx_r, \quad (2.3.1)$$

где  $T$  — инвариантная подгруппа в  $G$ . В качестве элементов системы  $H$  возьмем смежные классы  $Tx_i$ . Определим произведение в  $H$ -формулой

$$(Tx_i)(Tx_j) = Tx_k, \quad (2.3.2)$$

если  $x_i x_j \in Tx_k$  в  $G$ .

Нужно показать, что произведение определено однозначно. Пусть  $t_1 x_i$  и  $t_2 x_j$  — произвольные элементы соответственно из  $Tx_i$  и  $Tx_j$ . Тогда  $t_1 x_i t_2 x_j = t_1 x_i t_2 x_i^{-1} \cdot x_i x_j = t_3 x_i x_j$ , так как  $T$  — нормальный делитель. Но если  $x_i x_j \notin Tx_k$ , то  $t_3 x_i x_j \notin Tx_k$ . Таким образом, все произведения элементов из  $Tx_i$  на элементы из  $Tx_j$

попадают в один и тот же смежный класс  $Tx_k$ . Значит, произведение (2.3.2) зависит только от смежных классов, а не от выбора в них представителей, следовательно, произведение в  $H$  вполне определено.

Так как  $T$  — нормальный делитель,  $T^2 = T$ ,  $Tx_i = x_i T$ . Следовательно, в  $H$  роль единицы играет  $T$ , так как  $T \cdot Tx_i = Tx_i$ ,  $Tx_i \cdot T = Tx_i T = TTx_i = Tx_i$ . Кроме того, умножение ассоциативно, так как

$$(Tx_i Tx_j) Tx_k = Tx_i x_j x_k = Tx_i (Tx_j Tx_k).$$

Если  $x_i^{-1} \in Tx_j$ , то  $Tx_i Tx_j$  содержит  $x_i x_i^{-1} = 1$ , а поэтому  $Tx_i Tx_j = T$ , откуда в  $H$  обратным к  $Tx_i$  является элемент  $Tx_j$ , так как легко также проверить, что  $Tx_j \cdot Tx_i = T$ . Этим завершается проверка того, что  $H$  есть группа. Эту группу называют **фактор-группой**  $G$  по  $T$  и обозначают  $H = G/T$ .

**Теорема 2.3.1.** (Вторая теорема о гомоморфизмах.) Пусть  $G$  — группа,  $T$  — ее нормальный делитель,  $H = G/T$ . Тогда существует гомоморфизм  $G$  на  $H$  с ядром  $T$ . Этот гомоморфизм задается отображением  $g \rightarrow Tx_i$ , если  $g \in Tx_i$  в группе  $G$ .

**Доказательство.** Рассмотрим отображение  $g \rightarrow Tx_i$  группы  $G$  на группу  $H$  (здесь  $g \in Tx_i$ ). Если  $g_1 \in Tx_i$ ,  $g_2 \in Tx_j$ , то, как было показано,  $g_1 g_2 \in Tx_k$ , где  $x_i x_j \in Tx_k$ . Следовательно,  $g_1 g_2 \rightarrow Tx_k = Tx_i Tx_j$ . Таким образом, отображение  $G$  на  $H$  сохраняет произведение и поэтому является гомоморфизмом. Так как  $T$  — единица группы  $G/T$ , то  $g \rightarrow 1$  ( $= T$  в  $H$ ) тогда и только тогда, когда  $g \in T$  в  $G$ , откуда  $T$  — ядро этого гомоморфизма. Теорема доказана.

**Теорема 2.3.2.** (Третья теорема о гомоморфизмах.) Если  $G \rightarrow K$  — гомоморфизм  $G$  на  $K$  и  $T$  — ядро этого гомоморфизма, то группы  $K$  и  $H = G/T$  изоморфны. Если  $x \rightarrow x^*$  при гомоморфизме  $G \rightarrow K$ , то соответствие  $x^* \rightarrow Tx$  определяет изоморфизм между  $K$  и  $H$ .

**Доказательство.** Так как элементы из  $G$ , лежащие в одном смежном классе по  $T$ , имеют общий образ в  $K$ , соответствие  $x^* \rightarrow Tx$  является взаимно однозначным. Если  $x \rightarrow x^*$ ,  $y \rightarrow y^*$ , то  $xy \rightarrow x^*y^*$ . Но  $xy \in Txy$ , откуда  $x^*y^* \rightarrow Txy = TxTy$ . Таким образом, соответствие  $x^* \rightarrow Tx$  сохраняет произведения и, следовательно, является изоморфизмом групп  $K$  и  $H = G/T$ .

Подытожим результаты этих трех основных теорем о гомоморфизмах. Мы показали, что ядро любого гомоморфизма есть инвариантная подгруппа, что любая инвариантная подгруппа есть ядро некоторого гомоморфизма, образ которого единственен (с точностью до изоморфизма), и что этим образом является фактор-группа данной группы по нормальному делителю.

**Теорема 2.3.3.** Если  $A$  и  $B$  — подгруппы группы  $G$  и хотя бы одна из них инвариантна, то  $A \cup B = AB$ .

**Доказательство.** Мы должны показать, что любое конечное произведение  $x_1x_2 \dots x_s$ , где  $x_i \in A$  или  $B$ , может быть приведено к виду  $ab$ . Если подгруппа  $B$  инвариантна, то  $ba = aa^{-1}ba = ab'$ ; если же инвариантна подгруппа  $A$ , то  $ba = bab^{-1}b = a'b$ . Поэтому произведение  $x_1x_2 \dots x_s$  можно привести к виду, где ни один элемент из  $B$  не предшествует ни одному элементу из  $A$ :  $a_1a_2 \dots a_jb_{j+1} \dots b_s = ab$ , где  $a_i \in A$  и  $b_i \in B$ .

**Теорема 2.3.4.** Пусть  $T$  — инвариантная подгруппа в  $G$ . Тогда существует взаимно однозначное соответствие между подгруппами  $K^*$  группы  $H = G/T$  и подгруппами  $K$  группы  $G$ , содержащими  $T$ , причем  $K$  состоит из всех тех элементов, которые отображаются в  $K^*$ . Если подгруппа  $K^*$  инвариантна в  $H$ , то подгруппа  $K$  инвариантна в  $G$ , и обратно. Кроме того,  $[G : K] = [H : K^*]$ .

**Доказательство.** Очевидно, что образ подгруппы группы  $G$  в  $H$  есть подгруппа. Если теперь  $K^*$  — подгруппа в  $H$ , то полный прообраз  $K$  подгруппы  $K^*$  в  $G$  содержит  $T$  как прообраз единицы. При этом  $K$  является подгруппой.

Итак, полный прообраз подгруппы  $K^*$  группы  $H$  есть вполне определенная подгруппа  $K$  такая, что  $G \supseteq K \supseteq T$ , а  $K^*$  — образ подгруппы  $K$  при гомоморфизме  $G \rightarrow H$ . Значит, соответствие  $K \rightleftarrows K^*$  взаимно однозначно; при этом  $G \supseteq K \supseteq T$  и  $H \supseteq K^* \supseteq 1$ . Если подгруппа  $K^*$  инвариантна в  $H$ , то  $x^{-1}Kx \rightarrow x^{*-1}K^*x^* = K^*$ , откуда  $x^{-1}Kx \subseteq K$  для любого  $x$ , а поэтому  $K$  — нормальный делитель в  $G$ . Обратно, если  $K$  — нормальный делитель, то инвариантность  $K^*$  очевидна. Наконец, нетрудно заметить, что полный прообраз смежного класса  $K^*g^*$  — смежный класс  $Kg$ , откуда  $[G : K] = [H : K^*]$ .

Если произвольная подгруппа  $A$  имеет образ  $A^*$ , то, как легко увидеть, полным прообразом для  $A^*$  служит подгруппа  $A \cup T = AT$ .

## 2.4. Операторы

Отображение  $\alpha : g \rightarrow g^\alpha$  группы  $G$  в себя называется **эндоморфизмом**  $G$ , или **оператором** на  $G$ , если  $(xy)^\alpha = x^\alpha y^\alpha$ . Таким образом, эндоморфизм — это гомоморфизм группы  $G$  в себя. **Автоморфизм** — это взаимно однозначный эндоморфизм группы  $G$  на себя. Если из  $g^\alpha = h^\alpha$  вытекает равенство  $g = h$ , то эндоморфизм  $\alpha$  есть изоморфизм, являющийся в случае конечных групп автоморфизмом. Но бесконечная группа может быть изоморфна собственной подгруппе. Так, соответствие  $x \rightarrow 2x$  — эндоморфизм и даже изоморфизм аддитивной группы целых чисел, но подгруппу четных чисел, но оно не является автоморфизмом этой группы.

Говорят, что подгруппа  $H$  группы  $G$  допустима относительно эндоморфизмов  $\alpha_i$ , если  $H^{\alpha_i} \subseteq H$  для всех  $\alpha_i$ . Из определений немедленно следует, что *объединение и пересечение допустимых подгрупп — снова допустимые подгруппы*. Ясно, что оператор  $\alpha$  можно рассматривать как оператор на допустимой подгруппе. Может случиться, что два оператора, не совпадающие на всей группе, на некоторой допустимой подгруппе действуют одинаково. Кроме того, если соответствие  $G \rightarrow K$  есть гомоморфизм  $G$  на  $K$  с ядром  $T$ , допустимым относительно эндоморфизма  $\alpha$ , мы можем определить соответствующий оператор в  $K$ . Для этого полагаем

$$(Tx)^\alpha = Tx^\alpha. \quad (2.4.1)$$

Это естественное определение, так как действие эндоморфизма на смежном классе  $Tx$  дает только элементы из класса  $Tx^\alpha$ . Легко проверить, что  $\alpha$  — оператор на  $K$  и что если  $x \rightarrow x^*$  при гомоморфизме  $G \rightarrow K$ , то  $x^\alpha \rightarrow x^{*\alpha}$ .

Две группы  $A$  и  $B$  *операторно изоморфны*, если существуют такие взаимно однозначные соответствия  $A \rightleftarrows B$  и  $\alpha_i \rightleftarrows \beta_i$  между двумя группами и их операторами, что из  $a \rightleftarrows b$  следует соответствие  $a^{\alpha_i} \rightleftarrows b^{\beta_i}$ . Таким образом, операторный изоморфизм сильнее, чем изоморфизм.

**Теорема 2.4.1.** Пусть  $G$  — группа,  $\Omega$  — множество операторов на  $G$ ,  $A$  — допустимая подгруппа группы  $G$  и  $T$  — допустимая инвариантная подгруппа. Тогда  $A \cap T$  — допустимая инвариантная подгруппа в  $A$ , причем фактор-группы  $A \cup T/T$  и  $A/A \cap T$  операторно изоморфны.

*Доказательство.*  $A \cap T$  как пересечение  $\Omega$ -подгрупп (т. е. подгрупп, допустимых относительно  $\Omega$ ) есть  $\Omega$ -подгруппа в  $A$ . Если  $u \in A \cap T$ ,  $a \in A$ , то  $a^{-1}ua \in A$ . Но так как  $T$  — инвариантная подгруппа в  $G$  и  $u \in T$ , то  $a^{-1}ua \in T$ . Итак,  $a^{-1}ua \in A \cap T$ , т. е. подгруппа  $A \cap T$  инвариантна в  $A$ .

Обозначим  $A \cap T$  через  $D$ . Пусть

$$A = D + Da_2 + \dots + Da_r. \quad (2.4.2)$$

Утверждаем, что

$$A \cup T = T + Ta_2 + \dots + Ta_r, \quad (2.4.3)$$

где представители  $a_i$  те же, что и в (2.4.2). Действительно, если  $Ta_i = Ta_j$ , то  $a_i a_j^{-1} \in T$ , но ведь  $a_i a_j^{-1} \in A$ , откуда  $a_i a_j^{-1} \in A \cap T = D$ , что противоречит (2.4.2). Следовательно, все смежные классы  $Ta_i$  в (2.4.3) различны. Кроме того, так как  $T$  — нормальный дели-

тель,  $A \cup T = TA$ , а поэтому любой смежный класс по  $T$  в  $A \cup T$  имеет вид  $Ta = Tda_i$ , где  $a = da_i$  из (2.4.2). Но так как  $d \in T$ ,  $Tda_i = Ta_i$ , значит, смежные классы из (2.4.3) исчерпывают  $A \cup T$ . Соответствие

$$Da_i \leftrightarrow Ta_i \quad (2.4.4)$$

дает взаимно однозначное соответствие между смежными классами из (2.4.2) и (2.4.3), т. е. между элементами групп  $A/D$  и  $A \cup T/T$ . Если  $a_i a_j = da_k$ , где  $d \in D$ , то из  $D \subseteq T$  следует, что  $Da_i Da_j = = Da_k$  и  $Ta_i Ta_j = Ta_k$ . Поэтому соответствие (2.4.4) есть изоморфизм между фактор-группами  $A/D$  и в  $A \cup T/T$ . Оператор  $\alpha \in \Omega$  определяет оператор в  $A/D$  и в  $A \cup T/T$  так:  $(Da_i)^\alpha = Da_i^\alpha$  и  $(Ta_i)^\alpha = Ta_i^\alpha$ . Отсюда сразу следует, что соответствие (2.4.4) — операторный изоморфизм. Теорема доказана.

Нетрудно показать, что подгруппа  $K$  группы  $G$  инвариантна тогда и только тогда, когда она допустима относительно всех внутренних автоморфизмов группы  $G$ .

Используя понятие оператора, определим последовательно два понятия, более сильных, чем понятие нормального делителя.

Подгруппа, допустимая относительно всех автоморфизмов группы, называется *характеристической подгруппой*, а подгруппа, допустимая относительно всех эндоморфизмов группы, называется *вполне характеристической подгруппой*. Например, центр  $Z$  группы  $G$  является характеристической подгруппой, так как если  $zg = gz$  для всех  $g \in G$ , то при любом автоморфизме  $\alpha$  имеем  $z^\alpha g^\alpha = g^\alpha z^\alpha$ . Когда  $g$  пробегает группу  $G$ ,  $g^\alpha$  также пробегает всю группу  $G$ , значит,  $z^\alpha \in Z$ . Однако центр не всегда вполне характеристическая подгруппа. Например, рассмотрим группу  $G$  порядка 16, определенную отношениями  $a^4 = 1$ ,  $b^2 = c^2 = 1$ ,  $ba = a^{-1}b$ ,  $ca = ac$ ,  $cb = bc$ . Здесь центр  $Z$  имеет порядок 4 и порождается элементами  $a^2$  и  $c$ . Отображение  $a \rightarrow b$ ,  $b \rightarrow b$ ,  $c \rightarrow b$  определяет эндоморфизм группы  $G$ , отображающий элемент  $c$  центра на элемент  $b$ , не принадлежащий центру. Однако эндоморфизм сохраняет вид любого элемента. Поэтому подгруппы, порожденные всеми элементами вида  $x^3$ , где  $x \in G$ , или всеми элементами вида  $x^{-1}y^{-1}xy$ , где  $x, y \in G$ , являются вполне характеристическими.

Особенно полезное свойство этих двух понятий состоит в том, что в то время, как нормальный делитель  $H$  нормального делителя  $K$  группы  $G$  не является, вообще говоря, нормальным делителем в  $G$ , характеристическая подгруппа характеристической подгруппы характеристична и вполне характеристическая подгруппа вполне характеристической группы вполне характеристична. Кроме того, характеристическая подгруппа нормального делителя является нормальным делителем.

## 2.5. Прямые и декартовы произведения

Пусть  $A$  и  $B$  — две группы. Образуем из элементов этих групп множество упорядоченных пар  $(a, b)$ , где  $a \in A$ ,  $b \in B$ . Эти пары будут элементами новой группы, *прямого произведения*  $A \times B$ , если мы определим умножение равенствами

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2). \quad (2.5.1)$$

Проверка того, что произведение (2.5.1) удовлетворяет групповым аксиомам с элементом  $(1, 1)$  в качестве единицы, проводится исключительно на основании того факта, что групповые аксиомы выполняются для  $A$  и  $B$ . Кроме того, соответствие  $(a, b) \xrightarrow{\cong} (b, a)$  является изоморфизмом групп  $A \times B$  и  $B \times A$ , так что мы можем говорить о прямом произведении  $A$  и  $B$ , не указывая их порядка. Соответствие  $a \xrightarrow{\cong} (a, 1)$  дает изоморфизм между  $A$  и множеством элементов из  $A \times B$ , второй компонентой которых является единица. Аналогично, соответствие  $b \xrightarrow{\cong} (1, b)$  дает изоморфизм между  $B$  и подгруппой элементов вида  $(1, b)$ . Отождествим  $A$  и  $B$  с этими подгруппами. Тогда мы можем говорить, что группа  $G = A \times B$  является прямым произведением своих подгрупп  $A$  и  $B$ . Из равенства  $(a, 1)(1, b) = (a, b) = (1, b)(a, 1)$  следует, что в  $A \times B$  каждый элемент из  $A$  *перестановочен* (или *коммутирует*) с любым элементом из  $B$ , т. е.  $ab = ba$  для  $a \in A$ ,  $b \in B$ .

В прямом произведении  $(a, b)^{-1} = (a^{-1}, b^{-1})$ . Отсюда

$$(a_1, b_1)^{-1}(a_2, 1)(a_1, b_1) = (a_1^{-1}a_2a_1, 1),$$

т. е.  $A$  — нормальный делитель в  $A \times B$ . Аналогично подгруппа  $B$  инвариантна в  $A \times B$ . Единственный элемент  $(1, 1)$  имеет одновременно и вид  $(a, 1)$ , и вид  $(1, b)$ , откуда  $A \cap B = 1$ . Кроме того,  $A \cup B$  содержит все произведения  $(a, 1)(1, b) = (a, b)$ , откуда  $A \cup B = A \times B$ . Эти соотношения между  $A$  и  $B$  полностью характеризуют прямое произведение  $A \times B$ .

**Теорема 2.5.1.** *Группа  $G$  изоморфна прямому произведению двух подгрупп  $A$  и  $B$ , если  $A$  и  $B$  нормальные делители,  $A \cap B = 1$ ,  $A \cup B = G$ .*

**Доказательство.** Мы уже отмечали, что в прямом произведении  $A \times B$  подгруппы  $A$  и  $B$  обладают этими свойствами. Обратно, предположим, что  $A$  и  $B$  — нормальные делители в  $G$ ,  $A \cap B = 1$ ,  $A \cup B = G$ . Рассмотрим элемент  $a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) = = (a^{-1}b^{-1}a)b$ , где  $a \in A$ ,  $b \in B$ . Из инвариантности подгрупп  $A$  и  $B$  в  $G$  следует, что  $a^{-1}b^{-1}ab \in A \cap B$ . Но  $A \cap B = 1$ , откуда  $a^{-1}b^{-1}ab = 1$ , т. е.  $ab = ba$ . По теореме 2.3.3,  $G = A \cup B = AB$ , поэтому любой элемент  $g$  представим в форме  $g = ab$ . Это пред-

ставление единственно, так как из  $a_1 b_1 = a_2 b_2$  следует  $a_2^{-1} a_1 = b_2 b_1^{-1} \in A \cap B = 1$ , откуда  $a_1 = a_2$ ,  $b_1 = b_2$ . Если  $g = ab$ , то между группами  $G$  и  $A \times B$  установим соответствие  $g \leftrightarrow (a, b)$ . Если  $g_1 = a_1 b_1$ ,  $g_2 = a_2 b_2$ , то  $g_1 g_2 = a_1 b_1 a_2 b_2 = (a_1 a_2)(b_1 b_2)$ . Таким образом, это соответствие между  $G$  и  $A \times B$  не только взаимно однозначно, но также сохраняет произведение. Итак, изоморфизм между  $G$  и  $A \times B$  установлен.

Обобщим понятие прямого произведения на случай любого числа групп, конечного или бесконечного. Предположим, что дано семейство групп  $A_i$ , где  $i$  пробегает некоторое множество индексов  $I$  (иногда мы будем считать множество  $I$  вполне упорядоченным). Составим *формальные произведения*  $\prod_{i \in I} a_i$ . Формальные произведения представляют собой системы элементов  $a_i$ , одновременно выбранных по одному из каждой группы  $A_i$ . Все формальные произведения образуют группу, называемую *декартовым произведением* групп  $A_i$ , если определить умножение следующим образом:

$$\prod_{i \in I} a_i \cdot \prod_{i \in I} b_i = \prod_{i \in I} c_i, \quad c_i = a_i b_i \quad (2.5.2)$$

для любого  $i \in I$ .

Подгруппа декартова произведения, в которой  $a_i = 1$  для всех индексов, кроме конечного числа их, называется *прямым произведением* групп  $A_i$ . Ясно, что прямое и декартово произведения совпадают, когда число групп конечно. В обоих случаях элементы  $\prod_i a_i$ , где  $a_i = 1$ , если  $i \neq j$ , образуют нормальный делитель, изоморфный  $A_j$ . Отождествляя  $A_j$  с этой подгруппой для каждого  $j$ , получаем, что  $A_j \prod_{i \neq j} (A_i) = 1$ . Здесь  $\bigcup_{i \in I} A_i$  есть прямое произведение.

**Теорема 2.5.2.** Группа  $G$  изоморфна прямому произведению подгрупп  $A_i$ ,  $i \in I$ , если

- 1) Все  $A_i$  — нормальные делители,
- 2)  $A_j \prod_{i \neq j} (A_i) = 1$  для всех  $j \in I$ ,
- 3)  $G = \bigcup_{i \in I} A_i$ .

*Доказательство* аналогично доказательству теоремы 2.5.1. Из 1) и 2) следует, что любое  $a_j$  перестановочно с любым конечным произведением элементов  $a_i$ ,  $i \neq j$ . Из 1), 2) и 3) также следует, что элемент  $g \in G$  представим в виде конечного произведения элементов из  $A_i$ , причем это представление единственно с точностью до порядка сомножителей, при условии, что все

сомножители взяты из разных  $A_i$ . Этим мы устанавливаем изоморфизм между  $G$  и прямым произведением подгрупп  $A_i$ . Любой элемент из  $G$  может быть представлен в форме  $g = 1$  или  $g = b_1 \dots b_m$ , где  $b_k (k = 1, \dots, m)$  — элементы из различных  $A_i$ ,  $i \in I$ . Тогда  $g$  соответствует элементу  $\prod_{i \in I} a_i$ , где  $a_i = b_k$ , если элемент  $b_k \in A_i$  встречается в произведении для  $g$ , и  $a_i = 1$  в противном случае. Это соответствие и есть изоморфизм между  $G$  и прямым произведением подгрупп  $A_i$ .

### Упражнения

1. Показать, что любая группа диэдра гомоморфна группе порядка 2.
2. Показать, что если  $p$  и  $q$  ( $p < q$ ) — простые числа, то в группе порядка  $pq$  подгруппа порядка  $q$  инвариантна (см. упр. 8 к гл. 1).
3. Показать, что все подгруппы группы кватернионов — нормальные делители.
4. Пусть  $x, y, z$  — три прямые, соединяющие центры противоположных граней куба. Показать, что группа  $G$  симметрий куба индуцирует группу подстановок  $H$  порядка 6 на множестве  $(x, y, z)$ . Показать, что  $H$  — гомоморфный образ группы  $G$ .
5. Пусть  $G$  — совокупность отображений  $x \mapsto ax + b$ , где  $a, b$  — действительные числа и  $a \neq 0$ . множество действительных чисел на себя. Показать, что  $G$  — группа, в которой множество сдвигов  $T: x \mapsto x + t$  составляет нормальный делитель. Указать фактор-группу  $G/T$ .
6. Для каждого элемента  $b$  группы  $G$  определяем оператор сопряжения элементом  $b: g \rightarrow g^b = b^{-1}gb$ . Какие подгруппы допустимы относительно всех таких операторов? Если  $T$  — нормальный делитель в  $G$ , показать, что оператор, индуцируемый в  $H = G/T$ , есть также оператор сопряжения.

## Глава 3

### ЭЛЕМЕНТАРНАЯ ТЕОРИЯ АБЕЛЕВЫХ ГРУПП

#### 3.1. Определение абелевой группы. Циклические группы

Группа  $G$ , удовлетворяющая коммутативному закону

$$G4. \quad ba = ab \text{ для всех } a, b \in G$$

называется *абелевой* в честь математика Абеля.

Мы также говорим, что элементы  $a$  и  $b$  перестановочны, если  $ab = ba$ .

В § 1.5 мы определили циклическую группу как группу, порожденную единственным элементом (скажем,  $b$ ); все ее элементы являются степенями  $b$ .

Так как  $b^i b^j = b^j b^i = b^{i+j}$  для любых целых чисел  $i, j$ , мы видим, что каждая циклическая группа — абелева. Мы также заметили в § 1.5, что с точностью до изоморфизма существует одна-единственная циклическая группа каждого конечного порядка  $n$ . Верно также, что любая подгруппа циклической группы циклична.

**Теорема 3.1.1.** *Всякая подгруппа бесконечной циклической группы, отличная от единичной, является бесконечной циклической группой конечного индекса, и для любого конечного индекса существует одна-единственная подгруппа. Всякая подгруппа конечной циклической группы порядка  $n$  является циклической группой порядка, делящего  $n$ , и для любого порядка, делящего  $n$ , существует точно одна подгруппа.*

**Доказательство.** Пусть  $G$  — циклическая группа, порожденная элементом  $b$ , и  $H$  — подгруппа группы  $G$ . Если  $H$  не совпадает с единичной подгруппой и если  $b^i \in H$ , то  $b^{-i} \in H$  и один из этих показателей положителен. Предположим, что  $m$  — наименьший положительный показатель среди показателей всех элементов подгруппы  $H$ , и пусть  $b^t$  любой элемент из  $H$ . Тогда для подходящего  $r$  имеем  $t = mr + s$ , где  $0 \leq s < m$ . Отсюда  $b^t = (b^m)^r b^s$ . Так как  $b^t$  и  $b^m$  принадлежат  $H$ , то  $b^s$  также принадлежит  $H$ . Но если бы  $s$ , содержащееся в промежутке  $0 \leq s < m$ , было отлично от 0, то это противоречило бы нашему определению числа  $m$  как наименьшего положительного показателя степени элемента  $b$  в подгруппе  $H$ . Итак,  $s = 0$ ,  $b^t = (b^m)^r$ , и все элементы из  $H$  являются степенями элемента  $b^m$ , а это показывает, что  $H$  циклична. Так как для любого целого  $x$  мы имеем

$x = km + i$ , где  $i$  — одно из чисел  $0, 1, \dots, m - 1$ , мы без труда убеждаемся, что

$$G = H + Hb + \dots + Hb^{m-1}. \quad (3.1.1)$$

Равенство (3.1.1) содержит все смежные классы по  $H$ , и все они различны, так как из равенства  $b^i = hb^j$  для  $i \neq j$ ,  $0 \leq i, j < m - 1$ , следовало бы, что или  $b^{i-j} \in H$ , или  $b^{j-i} \in H$ , что противоречит выбору числа  $m$ . Значит,  $[G : H] = m$ . Здесь  $m$  — наименьшая положительная степень элемента  $b$ , содержащаяся в  $H$ , а также индекс  $H$  в  $G$ . Таким образом, если  $G$  бесконечна, то для любого положительного  $m$  элементы  $(b^m)^r$  образуют подгруппу, и, следовательно, существует в точности одна подгруппа индекса  $m$ . Если  $G$  конечна и порядка  $n$ , то  $b^n = 1$  и тем самым  $n = mr$ , т. е.  $m$  делит  $n$ . Для любого  $m$ , делящего  $n$ , элементы  $1, b^m, b^{2m}, \dots, b^{(r-1)m}$ , где  $n = mr$ , образуют подгруппу порядка  $r$  и индекса  $m$ . Поскольку  $n = mr$  может быть любым разложением  $n$  на два сомножителя, очевидно, существует одна и только одна подгруппа любого порядка  $r$ , делящего  $n$ .

### 3.2. Некоторые структурные теоремы для абелевых групп

Бесконечная абелева группа может иметь очень сложную структуру. Так, уже в сравнительно простой мультиликативной группе всех комплексных чисел, кроме нуля, существуют элементы бесконечного и любого конечного порядков.

Если в некоторой абелевой группе  $a^n = 1, b^m = 1$ , то  $(a^{-1})^n = 1$  и  $(ab)^{mn} = 1$ ; следовательно, элементы конечного порядка в любой абелевой группе  $A$  образуют подгруппу  $F$ . Каждый эндоморфизм  $\alpha$  группы  $A$  отображает элемент конечного порядка на элемент конечного порядка. Таким образом,  $F$  является вполне характеристической подгруппой группы  $A$ . В § 1.8 мы ввели термин *периодическая группа* (в некоторых приложениях употребляется термин *группа кручения*) для группы, все элементы которой имеют конечный порядок. Наоборот, группа, в которой все элементы, кроме единицы, имеют бесконечный порядок, называется *апериодической* (или *группой без кручения*).

**Теорема 3.2.1.** Пусть  $A$  — абелева группа и  $F$  — подгруппа всех ее элементов конечного порядка. Тогда  $A/F$  аperiодична.

*Доказательство.* Предположим противное, т. е. что некоторый элемент  $x \neq 1$  в  $A/F$  имеет конечный порядок  $m$ . Пусть при гомоморфизме  $A \rightarrow A/F$  имеет место соответствие  $u \mapsto x$ . Тогда  $u^m \mapsto x^m = 1$ , откуда  $u^m \in F$ , и  $u^m$  имеет конечный порядок, скажем,  $n$ . Тогда  $(u^m)^n = 1$ , и сам элемент  $u$  имеет конечный порядок. Но тогда  $u \in F$  и  $u \mapsto 1$ , хотя мы предположили, что  $x \neq 1$ .

Эта теорема сводит проблему построения всех абелевых групп к трем более конкретным проблемам:

- 1) нахождению всех периодических абелевых групп,
- 2) нахождению всех апериодических абелевых групп,

3) построению абелевой группы  $A$  с заданной периодической группой  $F$  в качестве подгруппы так, чтобы фактор-группа  $A/F$  была изоморфна данной апериодической группе  $H$ .

Ни одна из этих проблем полностью не решена, но мы, по-видимому, знаем больше всего о первой и меньше всего о последней.

Мы будем говорить, что множество элементов  $a_i$  абелевой группы  $A$  *независимо*, если конечное произведение  $\prod_i a_i^{e_i} = 1$  только тогда, когда  $a_i^{e_i} = 1$  для любого  $i$ . Если эти  $a_i$  независимы и, кроме того, порождают  $A$ , мы говорим, что  $a_i$  составляют *базис* группы  $A$ . Таким образом,  $a_i$  составляют базис для  $A$  тогда и только тогда, когда  $A$  является прямым произведением циклических групп, порожденных элементами  $a_i$ .

Предположим, что абелева группа  $A$  порождается элементами  $a_1, \dots, a_r$ . Тогда каждый элемент из  $A$  имеет вид  $a_1^{u_1} \dots a_r^{u_r}$ , где  $u_i$  — целые числа.

Если

$$a_1^{x_1} \dots a_r^{x_r} = 1 \quad (3.2.1)$$

является отношением для этих образующих, то мы говорим, что

$$a_1^{-x_1} \dots a_r^{-x_r} = 1 \quad (3.2.2)$$

есть обратное к нему отношение. Из некоторого множества  $S$  отношений на группе  $A$  мы можем получить другие, перемножая отношения из  $S$  и обратные к ним. Два множества отношений  $S_1$  и  $S_2$  называются *эквивалентными*, если отношения каждого множества могут быть получены таким образом из отношений другого множества. Легко видеть, что это действительно эквивалентность. Мы говорим, что множество  $S$  является множеством *определяющих отношений* для  $A$ , если каждое отношение на  $A$  может быть получено из отношений, принадлежащих  $S$ .

Можно показать, что произвольное множество  $S$  отношений образующих  $a_1, \dots, a_r$  является множеством определяющих отношений для той абелевой группы  $A$ , порожденной элементами  $a_1, \dots, a_r$ , в которой отношения, полученные из отношений  $S$ , имеют место, но никакие другие не выполняются. Может оказаться, конечно, что группа  $A$  сводится к единичному элементу.

**Теорема 3.2.2.** *Абелева группа, порожденная конечным числом  $r$  элементов, имеет базис, состоящий, самое большое, из  $r$  элементов.*

*Доказательство.* Теорема очевидна для  $r = 1$ , так как тогда группа циклическа. Предположим, что  $A$  порождена элементами  $a_1, \dots, a_r$ . Будем вести доказательство индукцией по  $r$ , а для фиксированного  $r$  — по наименьшему возможному положительному числу  $m$ , такому, что  $x_i = m$  в каком-нибудь отношении

$$a_1^{x_1} \dots a_r^{x_r} = 1. \quad (3.2.3)$$

Если имеется единственное отношение, в котором все  $x_i = 0$ , то  $A$  — прямое произведение бесконечных циклических групп  $\{a_i\}$ , и наша теорема верна. В противном случае некоторое отношение или обратное к нему будет содержать несколько положительных показателей. Перенумеруем элементы  $a_i$ , если необходимо, так, чтобы наименьший положительный показатель в некотором отношении был  $x_1 = m$ . Если  $m = 1$ , то мы имеем

$$a_1 = a_2^{-x_2} \dots a_r^{-x_r}, \quad (3.2.4)$$

и  $A$  порождается  $r - 1$  элементами  $a_2, \dots, a_r$ , и, по предположению индукции, теорема верна.

Предположим теперь, что  $x_1 = m > 1$  в отношении

$$a_1^m a_2^{x_2} \dots a_r^{x_r} = 1. \quad (3.2.5)$$

Пусть  $y_1, \dots, y_r$  — показатели степени в некотором другом отношении. Тогда для любого целого числа  $k$  из этого отношения и (3.2.5) мы можем получить отношение с показателями  $y_1 - km, y_2 - kx_2, \dots, y_r - kx_r$ . Мы можем выбрать  $k$  так, чтобы  $0 \leq y_1 - km < m$ . Но так как  $m$  было наименьшим положительным показателем в любом отношении, то должно быть  $y_1 - km = 0$ , и отношение с показателями  $y_1, \dots, y_r$  выводимо из (3.2.5) и отношения с показателями  $0, y_2 - kx_2, \dots, y_r - kx_r$ . Таким образом, множество всех отношений на  $A$  эквивалентно множеству, состоящему из (3.2.5) и отношений для  $a_2, \dots, a_r$ .

Пусть в (3.2.5)  $x_2 = k_2 m + s_2, \dots, x_r = k_r m + s_r$ , где  $k_l$  ( $l = 2, \dots, r$ ) выбраны так, что  $0 \leq s_l < m$ .

Если мы выберем новый элемент

$$a_1^* = a_1 a_2^{k_2} \dots a_r^{k_r}, \quad (3.2.6)$$

то  $a_1^*, a_2, \dots, a_r$  также порождают  $A$ , и в этих образующих (3.2.5) выразится так:

$$a_1^{*m} a_2^{s_2} \dots a_r^{s_r} = 1. \quad (3.2.7)$$

Если здесь какое-нибудь  $s$  отлично от нуля, то оно является положительным числом, меньшим, чем  $m$ , и мы можем применить

нашу индукцию. Если же  $s_2 = \dots = s_r = 0$ , то (3.2.7) превращается в

$$a_1^{*m} = 1, \quad (3.2.8)$$

а так как (3.2.5) и отношения между  $a_2, \dots, a_r$  были множеством определяющих отношений для  $A$  между образующими  $a_1, a_2, \dots, a_r$ , отсюда следует, что (3.2.8) и отношения между  $a_2, \dots, a_r$  являются множеством определяющих отношений между образующими  $a_1^*, a_2, \dots, a_r$ . Следовательно,  $A$  является прямым произведением циклической группы порядка  $m$ , порожденной элементом  $a_1^*$ , и группы, порожденной  $r - 1$  элементами  $a_2, \dots, a_r$ , которая (по индукции) является прямым произведением, самое большое,  $r - 1$  циклических подгрупп. Таким образом, теорема доказана во всех случаях.

Чтобы изучить периодические абелевые группы, нам понадобится лемма, которая выполняется в любой группе.

**Лемма 3.2.1.** *Пусть  $x$  — элемент порядка  $tp$  в некоторой группе, причем  $t$  и  $p$  — взаимно простые числа. Тогда  $x$  имеет единственное представление вида  $x = uy = zu$ , где  $u$  — элемент порядка  $t$  и  $z$  — порядка  $p$ ,  $u$  и  $z$  — степени элемента  $x$ .*

**Доказательство.** Обозначим через  $(a, b)$  наибольший общий делитель двух целых чисел  $a$  и  $b$ . Так как  $t$  и  $p$  взаимно просты,  $(t, p) = 1$ . С помощью алгоритма Евклида найдем такие целые числа  $u$  и  $v$ , что  $ut + vp = 1$ , и, значит,  $x = x^{vn}x^{ut} = x^{ut}x^{vn}$ . Положим  $y = x^{vn}$ ,  $z = x^{ut}$ . Тогда  $x = uy = zu$ , причем  $y^p = x^{vnp} = 1$ ,  $z^n = x^{utn} = 1$ . Таким образом, порядок  $y$  — некоторый делитель  $t_1$  числа  $t$ , а порядок  $z$  — некоторый делитель  $n_1$  числа  $n$ . Но из  $x = uy = zu$  следует, что порядок  $x$  — делитель числа  $t_1n_1$ . Так как этот порядок равен  $tp$ , то отсюда следует, что  $t_1 = t$  является порядком  $u$  и  $n_1 = n$  — порядком  $z$ . Предположим, что  $x$  допускает другое представление  $x = u_1z_1 = z_1y_1$ , где  $u_1$  порядка  $t$  и  $z_1$  — порядка  $n$ . Прежде всего,  $y_1$  и  $z_1$  перестановочны с  $x$ , так как  $xy_1 = u_1z_1y_1 = u_1x$  и  $xz_1 = z_1y_1z_1 = z_1x$ . Но тогда  $u_1$  и  $z_1$  перестановочны с  $u$  и  $z$  — элементами, являющимися степенями  $x$ .  $yz = x = u_1z_1$  приводит к  $w = u_1^{-1}y = z_1z^{-1}$ . Но  $u$  и  $u_1$  — перестановочные элементы порядка  $t$ , а  $z$  и  $z_1$  — перестановочные элементы порядка  $n$ . Следовательно, элемент  $w$  удовлетворяет равенствам  $w^p = 1$ ,  $w^n = 1$ , а так как  $(t, n) = 1$ , это дает  $w = 1$ . Поэтому  $u_1 = u$ ,  $z_1 = z$ , что и доказывает единственность представления. Повторным применением этой леммы получаем следующий результат.

**Лемма 3.2.2.** *Пусть  $x$  — элемент порядка  $n = n_1n_2 \dots n_r$ , где  $(n_i, n_j) = 1$  для  $i \neq j$ . Тогда  $x$  допускает одно-единственное*

*представление  $x = x_1 x_2 \dots x_r$ , где  $x_j x_i = x_i x_j$ , и  $x_i$  имеет порядок  $n_i$ . Каждое  $x_i$  является степенью  $x$ .*

В частности, если  $n = p_1^{e_1} \dots p_r^{e_r}$ , где  $p_1, \dots, p_r$  — различные простые числа, мы можем применить эту лемму, считая  $n_i = p_i^{e_i}$ .

В периодической абелевой группе  $A$  рассмотрим множество  $P$  элементов, порядки которых являются степенями фиксированного простого числа  $p$ ; сюда мы относим также единицу, так как она имеет порядок  $p^0 = 1$ . Если  $x^{p^a} = 1$ ,  $y^{p^b} = 1$ , то  $(xy)^{p^c} = 1$ , где  $c = \max(a, b)$  и  $(x^{-1})^{p^a} = 1$ . Следовательно,  $P$  является подгруппой, которую мы назовем *силовской  $p$ -подгруппой*  $S(p)$ .

Мы будем называть  $P$  также абелевой  $p$ -группой.

**Теорема 3.2.3.** *Периодическая абелева группа  $A$  является прямым произведением своих силовых подгрупп  $S(p)$ .*

**Доказательство.** Ясно, что  $\prod_p S(p)$ , прямое произведение силовых подгрупп группы  $A$ , является подгруппой группы  $A$ . Но, согласно лемме 3.2.2, если  $x \in A$  имеет порядок  $n = p_1^{e_1} \dots p_r^{e_r}$ , то  $x = x_1 x_2 \dots x_r$ , где  $x_i \in S(p_i)$ ; поэтому любой элемент  $x$  из  $A$  принадлежит прямому произведению силовых подгрупп. Следовательно, рассматриваемое прямое произведение должно совпадать с  $A$ .

### 3.3. Конечные абелевы группы. Инварианты

Конечная абелева группа является, очевидно, периодической и конечно порожденной. Применяя результаты предыдущего параграфа, мы можем сформулировать следующее утверждение.

**Теорема 3.3.1.** *Конечная абелева группа порядка  $n = p_1^{e_1} \dots p_r^{e_r}$  разложима в прямое произведение силовых подгрупп  $S(p_1), \dots, S(p_r)$ . Здесь  $S(p_i)$  — группа порядка  $p_i^{e_i}$ , являющаяся прямым произведением циклических групп порядков  $p_i^{e_{i_1}}, \dots, p_i^{e_{i_s}}$ , где  $e_{i_1} + \dots + e_{i_s} = e_i$ .*

**Доказательство.** В абелевой группе порядка  $n$ , как мы знаем, порядки элементов делят  $n$ . Следовательно, силовская подгруппа, принадлежащая простому числу, не делящему  $n$ , может состоять только из единицы. Таким образом, если  $p_1, \dots, p_r$  являются различными простыми делителями  $n$ , группа является прямым произведением  $S(p_1) \times \dots \times S(p_r)$ . Но это еще не очень много говорит нам о порядках групп  $S(p_i)$ , некоторые из них могли бы быть просто единичными группами. Так как группа  $S(p_i)$  или совпадает с единичной, или разлагается в прямое произведение циклических групп порядков  $p_i^{e_{i_1}}, \dots, p_i^{e_{i_s}}$ , то порядок  $S(p_i)$  равен

произведению этих порядков (скажем,  $p_i^{t_i}$ , где  $t_i = e_{i_1} + \dots + e_{i_s}$ ), а порядок всей группы равен произведению порядков групп  $S(p_i)$ . Но в силу единственности разложения целого числа  $n$  в произведение простых множителей отсюда вытекает, что  $p_i^{t_i} = p_i^{e_i}$  во всех случаях. Как вывод из этой теоремы и теоремы 3.1.1, мы получаем

**Следствие 3.3.1.** *Абелева группа порядка  $n$  содержит элемент порядка  $p$ , если  $p$  — простое число, делящее  $n$ .*

Конечная абелева  $p$ -группа  $A(p)$  обычно может быть записана в виде прямого произведения циклических групп различными способами. Например, если  $a^8 = 1, b^4 = 1$ , группа  $A(2) = \{a\} \times \{b\}$  имеет порядок 32. Если мы положим  $c = ab, d = a^4b$ , то  $c^8 = 1, d^4 = 1, a = c^5d^{-1}, b = c^4d$ . Мы легко проверяем, что  $A(2) = \{c\} \times \{d\}$ . В этом случае  $A(2)$  допускает разложение в прямое произведение циклических групп двумя различными способами, но число сомножителей и их порядки те же самые. Такое утверждение вообще верно для конечных абелевых  $p$ -групп, но так как циклическая группа порядка 6 представима в виде прямого произведения циклических групп порядков 2 и 3, то оно неверно для конечных абелевых групп, не являющихся  $p$ -группами. Если  $A$  — абелева  $p$ -группа, представленная в виде прямого произведения циклических групп порядков  $p^{e_1}, \dots, p^{e_r}$ , то эти числа называются *инвариантами* группы. В частном, но важном случае, когда все инварианты —  $p, \dots, p$ , мы говорим, что группа  $A$  — *элементарная абелева группа*. Ясно, что инварианты абелевой группы  $A$  определяют ее с точностью до изоморфизма. Но они являются инвариантами в более сильном смысле, выраженном более точно в следующей теореме.

**Теорема 3.3.2.** *Если конечная абелева  $p$ -группа  $A$  разлагается в прямое произведение циклических групп двумя способами  $A = A_1 \times \dots \times A_r = B_1 \times \dots \times B_s$ , то число сомножителей в обоих случаях то же самое,  $r = s$ , и порядки подгрупп  $A_1, \dots, A_r$  совпадают с порядками  $B_1, \dots, B_s$  при некоторой подходящей нумерации.*

*Доказательство.* Применим индукцию по порядку группы  $A$ . Теорема очевидна, когда  $A$  имеет порядок  $p$ .

Если  $A$  — любая абелева  $p$ -группа, обозначим через  $A_p$  подгруппу элементов  $x$  из  $A$ , для которых  $x^p = 1$ , и через  $A^p$  — подгруппу элементов вида  $y^p, y \in A$ . Пусть  $a_1, \dots, a_r$  — базис  $A$ , где  $a_i$  — элемент порядка  $p^{e_i}$  ( $i = 1, \dots, r$ ). Перенумеруем элементы  $a_i$  так, чтобы  $e_1 \geq e_2 \geq \dots \geq e_r$ . Тогда можно легко проверить, что  $a_1^{p^{e_1-1}}, \dots, a_r^{p^{e_r-1}}$  — базис  $A_p$  и что порядок  $A_p$  равен  $p^r$ . Если  $A$  — элементарная абелева, то  $A^p = 1$ . В противном

случае, пусть  $e_m$  — последний показатель, превосходящий 1, т. е.  $e_1 \geq e_2 \geq \dots \geq e_m > e_{m+1} = \dots = e_r = 1$ . Тогда, как легко можно показать,  $a_1^p, \dots, a_m^p$  — базис  $A^p$ .

Пусть  $b_1, \dots, b_s$  — другой базис  $A$ , где  $b_i$  порядка  $p^{f_i}$  ( $i = 1, \dots, s$ ) и  $f_1 \geq f_2 \geq \dots \geq f_s$ . Тогда, если в качестве базиса выбраны  $a_1, \dots, a_r$ , порядок  $A_p$  равен  $p^r$ , а если  $b_1, \dots, b_s$ , он равен  $p^s$ ; отсюда следует, что  $r = s$ . Если группа  $A$  — элементарная абелева группа, то на этом доказательство заканчивается. Если нет, то пусть

$$f_1 \geq f_2 \geq \dots \geq f_n > f_{n+1} = \dots = f_s = 1.$$

Тогда  $A^p$  имеет инварианты  $p^{e_1-1}, \dots, p^{e_m-1}$  и инварианты  $p^{f_1-1}, \dots, p^{f_n-1}$ . По предположению индукции,  $m = n$  и  $e_1 - 1 = f_1 - 1, \dots, e_m - 1 = f_m - 1$ . Отсюда и из факта, что  $r = s$ , получается, что  $e_1 = f_1, \dots, e_r = f_r$ , что и требовалось доказать.

**Следствие 3.3.2.** *Две конечные абелевые  $p$ -группы, имеющие разные инварианты, неизоморфны.*

**Теорема 3.3.3.** *Абелева группа  $A$  с инвариантами  $p^{e_1}, \dots, p^{e_r}$  ( $e_1 \geq \dots \geq e_r$ ) обладает подгруппой  $K$  с инвариантами  $p^{k_1}, \dots, p^{k_t}$ , ( $k_1 \geq \dots \geq k_t$ ) тогда и только тогда, когда  $t \leq r$  и  $k_1 \leq e_1, \dots, k_t \leq e_t$ .*

**Доказательство.** Докажем сначала, что показатели инвариантов подгруппы  $K$  группы  $A$  удовлетворяют неравенствам теоремы, применяя индукцию по порядку группы  $A$ . Если порядок  $A$  равен  $p$ , теорема очевидна.

Так как  $K_p$  — подгруппа в  $A_p$ , то  $t \leq r$ ; это доказывает теорему в случае, когда  $A$  — элементарная абелева группа. В противном случае полагаем  $e_1 \geq \dots \geq e_m > e_{m+1} = \dots = e_r = 1$  и  $k_1 \geq \dots \geq k_u > k_{u+1} = \dots = k_t = 1$ . Тогда  $K^p$  — подгруппа в  $A^p$  и инварианты  $K^p$  суть  $p^{k_1-1}, \dots, p^{k_u-1}$ , а инварианты  $A^p$  —  $p^{e_1-1}, \dots, p^{e_m-1}$ . Согласно предположению индукции,  $u \leq m$  и  $k_i - 1 \leq e_i - 1$ ,  $i = 1, \dots, u$ . Отсюда  $k_i \leq e_i$  ( $i = 1, \dots, u$ ), а так как  $k_{u+1} = \dots = k_t = 1$ , то также  $k_i \leq e_i$  ( $i = u + 1, \dots, t$ ), откуда  $k_i \leq e_i$  ( $i = 1, \dots, t$ ).

Если неравенства теоремы выполняются, то существует подгруппа группы  $A$  с заданными инвариантами, в качестве базиса которой мы можем выбрать подходящие степени первых  $t$  базисных элементов группы  $A$ . Но, вообще говоря, неверно, что при заданной группе  $A$  и ее подгруппе  $K$  можно всегда выбрать базис для  $A$  и базис для  $K$  так, чтобы базис  $K$  состоял из степеней элементов базиса  $A$  (см. упр. 5).

**Упражнения**

1. Абелева группа  $A$  порождается элементами  $a, b, c$  с определяющими отношениями  $a^3b^9c^9 = 1, a^9b^{-3}c^9 = 1$ . Найти базис для  $A$  и порядки базисных элементов.
2. Показать, что конечная абелева  $p$ -группа порождается своими элементами высшего порядка.
3. Абелева группа имеет инварианты  $p^3, p^2$ . Сколько подгрупп порядка  $p^2$  она содержит?
4. Приведите два примера абелевых  $p$ -групп, которые содержат точно  $p^2 + p + 1$  подгрупп порядка  $p$ .
5. Пусть  $A$  — абелева группа, порожденная  $a$  и  $b$  с определяющими отношениями  $a^{p^3} = 1, b^p = 1$ . Пусть  $K$  — подгруппа, порожденная элементом  $x = a^pb$ . Показать, что невозможно выбрать базис для  $A$  и базис для  $K$  так, чтобы базисный элемент для  $K$  был степенью базисного элемента для  $A$ .

## Г л а в а 4

### ТЕОРЕМЫ СИЛОВА

#### 4.1. Ложность обращения теоремы Лагранжа

Согласно теореме Лагранжа, порядок подгруппы конечной группы является делителем порядка группы. Но, обратно, если мы имеем группу  $G$  порядка  $n$  и если  $n$  делится на  $m$ , то  $G$  может не иметь подгруппу порядка  $m$ . Например, можно проверить, что следующая группа подстановок порядка 12 не содержит подгрупп порядка 6:

$$\begin{array}{cc} \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{array} \right) \\ \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{array} \right) & \left( \begin{array}{cccc} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{array} \right) \end{array}$$

Однако эта группа имеет подгруппы порядков 2, 3 и 4.

Таким образом, если  $m$  делит  $n$ , мы, вообще говоря, не можем быть уверенными, что группа порядка  $n$  содержит подгруппу порядка  $m$ . Но если  $m$  — простое число или его степень, то всегда такая подгруппа существует. Вопрос о существовании и числе таких подгрупп выясняется в *теоремах Силова*, которым посвящена настоящая глава. Мы начнем с теоремы, которая послужит отправной точкой для *теорем Силова*.

**Теорема 4.1.1.** *Если порядок группы  $G$  делится на простое число  $p$ , то  $G$  содержит элемент порядка  $p$ .*

*Доказательство.* Пусть  $n = mp$  — порядок группы  $G$ . Если  $m = 1$ , то  $G$  — циклическая группа порядка  $p$ , и теорема дока-

зана. Будем проводить доказательство индукцией по  $m$ . Если  $G$  содержит истинную подгруппу  $H$ , индекс которой  $[G : H]$  не делится на  $p$ , то порядок  $H$  делится на  $p$  и, согласно предположению индукции,  $H$  содержит элемент порядка  $p$ . Предположим теперь, что индекс любой истинной подгруппы группы  $G$  делится на  $p$ . Тогда, согласно § 1.6,  $n = n_1 + n_2 + \dots + n_s$ , где каждое  $n_i$  обозначает число элементов в некотором классе сопряженных элементов группы  $G$ . При этом  $n_i \neq 1$  есть индекс истинной подгруппы группы  $G$ , который, по предположению, делится на  $p$ . Можно считать, что  $n_1 = 1$ , так как единица составляет класс. Поэтому количество  $n_i$ , равных единице, кратно  $p$ . Элемент  $a_i$  составляет класс сопряженных элементов группы  $G$  тогда и только тогда, когда он принадлежит центру  $Z$  группы  $G$ . Таким образом, центр  $Z$  имеет порядок, кратный  $p$ . Но для любого  $z \in Z$  и любого  $g \in G$  имеем  $zg = gz$ . Следовательно, элементы центра  $Z$  перестановочны друг с другом, т. е.  $Z$  — абелева группа. Но теперь, согласно следствию из теоремы 3.3.1,  $Z$  содержит элемент порядка  $p$ .

## 4.2. Три теоремы Силова

Если простое число  $p$  делит порядок группы  $G$ , то теорема 4.1.1 гарантирует существование по крайней мере одной подгруппы порядка  $p$ . Мы покажем теперь, что если  $G$  имеет порядок  $n = p^m s$ , то она содержит также подгруппы порядков  $p^2, p^3, \dots, p^m$ .

**Теорема 4.2.1.** (Первая теорема Силова.) *Если  $G$  имеет порядок  $n = p^m s$ , где  $p$  — простое число, которое не делит  $s$ , то  $G$  содержит подгруппы порядков  $p^i$  ( $i = 1, \dots, m$ ), причем каждая подгруппа порядка  $p^i$  ( $i = 1, \dots, m - 1$ ) инвариантна, по крайней мере, в одной подгруппе порядка  $p^{i+1}$ .*

*Доказательство* проведем индукцией по  $i$ . Как доказано выше,  $G$  содержит подгруппу порядка  $p$ . Пусть  $P$  — подгруппа порядка  $p^i$ , где  $i \geq 1$ . Запишем  $G$  как сумму двойных смежных классов по  $P$ :  $P : G = P + Px_2P + \dots + Px_rP$ . Пусть  $Px_jP$  состоит из  $a_j$  правых смежных классов по  $P$ . Тогда  $[G : P] = a_1 + a_2 + \dots + a_r$ , где  $a_j = [x_j^{-1}Px_j : x_j^{-1}Px_j \cap P]$ , и  $a_1 = 1$  для двойного класса  $P \cdot 1 \cdot P = P$ . Поэтому или  $a_j = 1$ , или есть степень числа  $p$ . Так как  $p$  делит  $[G : P]$ , число слагаемых  $a_j$ , равных единице, должно быть кратным  $p$ . Если  $a_j = 1$ , то  $x_j^{-1}Px_j = P$ , а потому и  $x_j$  и смежный класс  $Px_j = x_jP$  принадлежит нормализатору  $K$  подгруппы  $P$ . Обратно, если  $x_j \in K$ , то  $x_j^{-1}Px_j = P$  и  $a_j = 1$ . Таким образом,  $[K : P]$  равно числу слагаемых  $a_j$ , равных единице, а поэтому  $p$  делит  $[K : P]$ . Следовательно, фактор-группа  $K/P$  имеет порядок  $[K : P]$ , кратный  $p$ . Поэтому  $K/P$  содержит подгруппу  $J^*$

порядка  $p$ . По теореме 2.3.4,  $J^* = J/P$ , где  $J \subseteq K$  и  $[J : P] = [J^* : 1] = p$ , а поэтому  $J$  — подгруппа порядка  $p^{i+1}$ , содержащая  $P$  в качестве нормального делителя.

**Определение.** Группа  $P$  называется  $p$ -группой, если все ее элементы, отличные от единицы, имеют порядки, равные степеням простого числа  $p$ .

**Определение.** Подгруппа  $S$  группы  $G$  называется силовской  $p$ -подгруппой группы  $G$ , если  $S$  —  $p$ -подгруппа, не содержащая ни в какой другой  $p$ -подгруппе группы  $G$ .

Используя эти определения, мы можем сформулировать несколько следствий из первой теоремы Силова.

**Следствие 4.2.1.** Любая конечная группа  $G$  порядка  $n = p^m s$ ,  $(p, s) = 1$ ,  $p$  — простое, содержит силовскую  $p$ -подгруппу порядка  $p^m$ , причем любая  $p$ -подгруппа содержится в некоторой силовской  $p$ -подгруппе группы  $G$ .

Любая группа порядка  $p^m$  является  $p$ -группой. Согласно теореме 4.1.1, если порядок группы делится на два разных простых числа, то она не может быть  $p$ -группой. Следовательно, любая конечная  $p$ -группа имеет порядок, равный степени простого числа  $p$ , скажем,  $p^m$ .

**Следствие 4.2.2.** Любая подгруппа  $p$ -группы  $P$  порядка  $p^m$  содержится в некоторой максимальной подгруппе порядка  $p^{m-1}$ , причем все максимальные подгруппы группы  $P$  инвариантны в  $P$ .

**Теорема 4.2.2.** (Вторая теорема Силова). В конечной группе  $G$  все силовские  $p$ -подгруппы сопряжены.

**Доказательство.** Пусть  $P_1$  и  $P_2$  — две силовские  $p$ -подгруппы. Тогда имеем разложение по двойному модулю:  $G = P_1 P_2 + P_1 x_2 P_2 + \dots + P_1 x_s P_2$ . Пусть  $b_i$  — число правых смежных классов по  $P_2$  в  $P_1 x_i P_2$ . Иначе,  $b_i = [x_i^{-1} P_1 x_i : x_i^{-1} P_1 x_i \cap P_2]$ , а поэтому либо равно единице, либо степени простого числа  $p$ . Но число  $b_1 + \dots + b_s = [G : P_2]$  не делится на  $p$ . Следовательно,  $b_i = 1$  для некоторого  $i$  и  $x_i^{-1} P_1 x_i = P_2$ .

**Теорема 4.2.3.** (Третья теорема Силова.) Число силовских  $p$ -подгрупп конечной группы  $G$  равно  $1 + kp$  и делит порядок группы  $G$ .

**Доказательство.** Это утверждение очевидно, если имеется только одна силовская  $p$ -подгруппа. В противном случае пусть  $S_0$  — одна из силовских  $p$ -подгрупп, а  $S_1, \dots, S_r$  — все остальные. Если эти последние трансформировать элементами из  $S_0$ , то они распадаются на некоторое число непересекающихся классов сопряженных (относительно  $S_0$ ) между собой подгрупп. Согласно второй теореме Силова,  $S_i$  — единственная силовская  $p$ -подгруппа в своем нормализаторе  $K_i$ . Следовательно, нормализатор подгруппы  $S_i$  в  $S_0$  ( $i \neq 0$ ) является собственной подгруппой группы  $S_0$ .

и тем самым число сопряженных с  $S_i$  относительно  $S_0$  подгрупп степени числа  $p$ , равно  $p^{e_i}$ , где  $e_i \geq 1$ . Следовательно,  $r = p^{e_1} + \dots + p^{e_s} = kp$ , и число всех силовских  $p$ -подгрупп равно  $1 + r = 1 + kp$ . Число силовских  $p$ -подгрупп равно, согласно второй теореме Силова, индексу нормализатора группы  $S_0$ , а потому делит порядок группы  $G$ .

**Теорема 4.2.4.** Пусть  $K$  — нормализатор силовской  $p$ -подгруппы  $P$  конечной группы  $G$ . Если  $H$  — такая подгруппа, что  $G \supseteq H \supseteq K \supseteq P$ , то  $H$  совпадает со своим нормализатором в  $G$ .

**Доказательство.** Пусть  $x^{-1}Hx = H$ . Тогда  $H \supseteq x^{-1}Px = P'$ , где  $P'$  — силовская  $p$ -подгруппа в  $H$ . Следовательно, существует такой элемент  $u \in H$ , что  $u^{-1}P'u = P$ , откуда  $u^{-1}x^{-1}Pxu = P$ , и тем самым  $xu \in K$ , а отсюда  $x \in H$ , т. е. группа  $H$  совпадает со своим нормализатором.

Следующая теорема, представляя самостоятельный интерес, допускает ряд важных применений, как это будет показано в последующих главах.

**Теорема 4.2.5 (Бернсайда).** Пусть  $G$  — конечная группа,  $h$  — ее  $p$ -подгруппа, и пусть  $h$  содержится в двух различных силовских  $p$ -подгруппах, причем в одной из них является нормальным делителем, а в другой не является. Тогда  $h$  имеет  $r > 1$ ,  $r \not\equiv 0 \pmod{p}$ , сопряженных подгрупп  $h = h_1, h_2, \dots, h_r$ , таких, что

а) все  $h_i$  инвариантны в группе  $H = h_1 \cup h_2 \cup \dots \cup h_r$ ,  
 б) не существует такой силовской  $p$ -подгруппы, чтобы все группы  $h_1, h_2, \dots, h_r$  были бы в ней нормальными делителями.

в) подгруппы  $h_1, h_2, \dots, h_r$  составляют полный класс сопряженных подгрупп в группе  $N_H$  — нормализаторе группы  $H$ .

**Доказательство.** Пусть  $N_h$  — нормализатор подгруппы  $h$ . Пусть  $Q$  — силовская  $p$ -подгруппа группы  $G$ , в которой  $h$  неинвариантна, и такая, что группа  $D = N_h \cap Q$  максимальна. Пусть  $q$  — нормализатор  $D$  в  $Q$ , а  $N_D$  — нормализатор  $D$  в  $G$ . Мы утверждаем, что  $Q \supseteq q \supset D \supset h$ . Действительно,  $h$  — инвариантная подгруппа индекса  $p$  в некоторой подгруппе группы  $Q$ , но  $h$  не является нормальным делителем в  $Q$ . Отсюда  $Q \supset D \supset h$ .

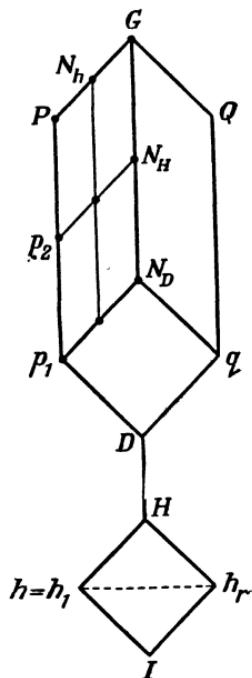


Рис. 2. Теорема Бернсайда.

Кроме того,  $D$  как истинная подгруппа в  $Q$  строго содержится в своем нормализаторе  $q$  в  $Q$ . Итак,  $Q \supseteq q \supset D \supset h$ . Далее, так как  $D = N_h \cap Q$ , подгруппа  $h$  неинвариантна в  $q$  и тем более неинвариантна в  $N_D$ . Пусть  $h = h_1, \dots, h_s (s > 1)$  — подгруппы, сопряженные с  $h$  в  $N_D$ . Так как  $h$  — нормальный делитель в  $D$  и  $N_D$  индуцирует автоморфизмы в  $D$ , каждая подгруппа  $h_i$  также инвариантна в  $D$  и тем более в  $H = h_1 \cup h_2 \cup \dots \cup h_s \subseteq D$ . Нормализатор  $N_H$  подгруппы  $H$  содержит  $N_D$ , так как элементы из  $N_D$  трансформируют  $H$  в себя.

Пусть  $p_1$  — силовская подгруппа группы  $N_h \cap N_D$  и  $P_1 \supseteq p_1$  — силовская подгруппа группы  $N_h$ . По условию  $P_1$  — силовская подгруппа в  $G$ . Тогда  $D \subset P_1$ , так как  $D$  не совпадает со своим нормализатором в  $P_1$ . Теперь  $N_h \cap N_D \subseteq N_D \subseteq N_H$ . Пусть  $p_2 \supseteq p_1$  — силовская подгруппа в  $N_H$  и  $P \supseteq p_2$  — силовская подгруппа в  $G$ . Если  $P \not\subseteq N_h$ , то  $P \cap N_h \supseteq p_1 \supset D$ , что противоречит свойству максимальности группы  $D$ . Следовательно,  $P \subseteq N_h$ , а поэтому  $N_h \cap N_H \supseteq P \cap N_H = p_2$ , так как  $p_2$  — силовская подгруппа в  $N_H$ .

Пусть  $h = h_1, \dots, h_s, \dots, h_r$  — сопряженные с  $h$  относительно  $N_H$  подгруппы (и, следовательно, все нормальные делители в  $H$ ). Нормализатором подгруппы  $h$  в  $N_H$  является  $N_H \cap N_h$ , и поэтому число сопряженных с  $h$  в  $N_H$  подгрупп равно  $r = [N_H : N_H \cap N_h]$ . Но  $N_H \cap N_h \supseteq p_2$ , где  $p_2$  — силовская подгруппа группы  $N_H$ . Следовательно,  $r \not\equiv 0 \pmod{p}$ .

Если бы все  $h_1, \dots, h_r$  были инвариантными подгруппами некоторой силовской подгруппы  $S_p$ , то  $S_p \subseteq N_H$  и каждая силовская  $p$ -подгруппа группы  $N_H$  содержала бы подгруппы  $h_i$  в качестве нормальных делителей. Но  $q \subseteq N_D \subseteq N_H$  —  $p$ -подгруппа в  $N_H$ , содержащая  $h = h_1$ , но не в качестве нормального делителя.

### 4.3. Конечные $p$ -группы

Из силовских теорем следует, что группа  $G$  порядка  $n = p_1^{e_1} \dots p_r^{e_r}$  содержит подгруппу порядка  $p_i^{e_i}$  для любого  $i = 1, \dots, r$ , и все подгруппы этого порядка изоморфны, так как они даже сопряжены в  $G$ . Поэтому задачу построения конечных групп можно рассматривать как состоящую из двух частей:

1) построение групп, порядки которых равны степеням простого числа,

2) построение групп порядка  $n$  из групп, порядки которых являются степенями простых чисел, делящих  $n$ .

Если все силовские подгруппы циклически (это, конечно, имеет место, когда все  $e_i = 1$ ), мы умеем решать вторую задачу; решение ее будет изложено в главе 9 (теорема 9.4.3). Таким образом, хотя ни одна из этих проблем ни в каком смысле в общем случае не решена, следует решить первую, чтобы иметь материал для

решения второй. Как нам кажется, трудности построения группы, исходя из силовских подгрупп, очень сильно зависят от сложности строения групп порядка, равного степени простого числа, т. е.  $p$ -групп, как мы их будем в дальнейшем называть.

Первый очень важный результат о  $p$ -группах состоит в следующем.

**Теорема 4.3.1.** Центр конечной  $p$ -группы отличен от единичной подгруппы.

**Доказательство.** Пусть  $P$  — конечная  $p$ -группа. Представим  $P$  как сумму классов сопряженных элементов:

$$P = C_1 + C_2 + \dots + C_r. \quad (4.3.1)$$

Здесь  $C_1$  состоит только из единицы. Пусть  $h_i$  — число элементов в классе  $C_i$ , равное по теореме 1.6.1 индексу некоторой подгруппы  $P$ , т. е. оно или равно 1 (для элемента из центра), или — степени числа  $p$ . Но  $P$  имеет порядок  $p^m$ , значит, имеет место равенство

$$p^m = h_1 + h_2 + \dots + h_r. \quad (4.3.2)$$

Так как  $h_1 = 1$ , в правой части равенства (4.3.2) некоторые  $h_i$  также должны быть равными единице, следовательно, центр  $P$  строго больше единичной подгруппы.

Сформулируем следствие 4.2.2 в виде теоремы.

**Теорема 4.3.2.** Всякая истинная подгруппа  $p$ -группы  $P$  порядка  $p^m$  содержится в максимальной подгруппе порядка  $p^{m-1}$ , и все максимальные подгруппы группы  $P$  — нормальные делители в  $P$ .

Еще одним следствием из первой теоремы Силова 4.2.1 является тот факт, что никакая истинная подгруппа  $p$ -группы не совпадает со своим нормализатором. Оказывается, что имеет место даже в некотором смысле обратное утверждение, которое мы сейчас и докажем.

**Теорема 4.3.3.** В конечной группе  $G$  ни одна собственная подгруппа не совпадает со своим нормализатором тогда и только тогда, когда  $G$  — прямое произведение своих силовских подгрупп.

**Доказательство.** Пусть любая собственная подгруппа группы  $G$  не совпадает со своим нормализатором. По теореме 4.2.4 нормализатор  $K$  силовской подгруппы  $P$  совпадает со своим нормализатором, откуда, по условию,  $K$  должно быть равно  $G$ . Таким образом,  $P$  — нормальный делитель группы  $G$ . Отсюда и из теоремы 2.5.2 следует, что объединение силовских подгрупп является их прямым произведением, следовательно,  $G$  — прямое произведение своих силовских подгрупп.

Предположим теперь, что  $G = P_1 \times \dots \times P_r$ , где  $P_i$  — группа порядка  $p_i^{e_i}$  и  $p_i \neq p_j$ , если  $i \neq j$ . Если теперь  $g = g_1 g_2 \dots g_r$ , где  $g_i \in P_i$ , то условия леммы 3.2.2. выполнены и, значит,  $g_i$  есть степень элемента  $g$ . Таким образом, если элемент  $g \in G$  лежит в подгруппе  $H$  группы  $G$ , все его компоненты также находятся в  $H$ . Поэтому  $H$  — прямое произведение  $H = H_1 \times \dots \times H_r$  групп  $H_i$ , где  $H_i = H \cap P_i$  — подгруппа в  $P_i$ . Если  $H$  — собственная подгруппа в  $G$ , то некоторые  $H_j$  являются собственными подгруппами  $P_j$ . Заменяя эти  $H_i$  большими подгруппами из  $P_j$ , в которых они инвариантны, мы получим подгруппу, строго содержащую  $H$  в качестве нормального делителя.

**Теорема 4.3.4.** *Если  $A$  — нормальный делитель порядка  $p$  в  $p$ -группе  $P$ , то  $A$  лежит в центре  $P$ .*

*Доказательство.* Так как  $A$  имеет порядок  $p$ , она циклична и порождается элементом  $a$ , причем  $1, a, \dots, a^{p-1}$  — все элементы  $A$ . Поскольку  $A$  — инвариантная подгруппа, сопряженные с  $a$  элементы находятся в множестве  $a, a^2, \dots, a^{p-1}$ . Но число этих элементов равно индексу централизатора элемента  $a$  и поэтому равно либо 1, либо степени числа  $p$ . Но число сопряженных с  $a$  элементов не превосходит  $p - 1$  и поэтому равно 1. Тем самым элемент  $a$  и подгруппа  $A$  лежат в центре группы  $P$ .

#### 4.4. Группы порядков $p, p^2, pq, p^3$

Группа простого порядка  $p$  не может иметь собственных подгрупп и поэтому является циклической группой, порожденной любым своим элементом, отличным от единицы. В теореме 1.5.4 мы уже показали, что группа  $G$ , не имеющая собственных подгрупп, — циклическая группа простого порядка.

Нециклическая группа  $G$  порядка  $p^2$  содержит две различные подгруппы порядка  $p$ , например  $\{a\}$  и  $\{b\}$ , где  $a^p = 1, b^p = 1$  и  $\{a\} \cap \{b\} = 1$ . Так как они являются максимальными собственными подгруппами группы  $G$ , то, согласно следствию 4.2.2, они инвариантны, поэтому из теоремы 2.5.1 следует, что  $G = \{a\} \times \{b\}$ , и, следовательно,  $G$  — абелева группа с базисом  $a, b$ .

Предположим, что порядок группы  $G$  равен  $pq$ , где  $p < q$  и  $(p, q) = 1$ . Согласно третьей теореме Силова, число подгрупп порядка  $q$  равно такому числу  $1 + kq$ , что оно делит  $p$ ; поэтому оно равно 1. Эта единственная подгруппа  $\{b\}$  инвариантна и  $b^q = 1$ . Число подгрупп порядка  $p$  равно такому числу  $1 + kp$ , которое делит  $q$ , и, следовательно, оно равно или 1, или  $q$ . Если оно равно 1, тогда при некотором  $a$ , таком, что  $a^p = 1$ , мы получаем инвариантную подгруппу  $\{a\}$ , а  $G$  является прямым произведением  $G = \{a\} \times \{b\}$ . Очевидно, что тогда группа  $G$  — циклическая с образующим элементом  $c = ab$  порядка  $pq$ . Теперь рассмотрим

случай, когда группа  $G$  обладает  $1 + kp = q$  подгруппами порядка  $p$  и подгруппа  $\{a\}$  порядка  $p$  неинвариантна. Тогда  $a^p = 1$ ,  $b^q = 1$ , а так как подгруппа  $\{b\}$  инвариантна,  $a^{-1}ba = b^r$  при некотором  $r$ . Если  $r = 1$ ,  $G$  является абелевой и, более того, циклической группой, рассмотренной выше. Пусть  $r \neq 1$ . Тогда  $a^{-1}b^i a = b^{ir}$  для произвольного  $i$  и, в частности,  $a^{-1}b^r a = b^{r^2}$ , откуда следует, что  $a^{-2}ba^2 = a^{-1}b^r a = b^{r^3}$ . И вообще  $a^{-j}ba^j = b^{r^j}$ . Следовательно, при  $j = p$  мы имеем  $b = a^{-p}ba^p = b^{rp}$ , откуда  $r^p \equiv 1 \pmod{q}$ . То, что это необходимое условие для  $r$ , является также и достаточным для того, чтобы мы имели группу  $G$  порядка  $pq$ , вытекает из следующего правила умножения двух элементов некоторого множества:

$$(a^u b^v)(a^x b^y) = a^{u+x} b^{vr^x+y},$$

и из доказательства того, что относительно этого правила умножения рассматриваемое множество является группой порядка  $pq$ . Последнее правило умножения является частным случаем более общего правила, которое будет рассмотрено в теореме 6.5.1.

Существует три типа абелевых групп порядка  $p^3$ ; они характеризуются инвариантами  $(p^3)$ ,  $(p^2, p)$  и  $(p, p, p)$  соответственно. Для описания неабелевых групп порядка  $p^3$  мы рассмотрим отдельно два случая: 1)  $p = 2$  и 2)  $p$  — нечетное число. Пусть  $p = 2$ , т. е.  $G$  неабелева группа порядка 8. Группа  $G$  не содержит элемент порядка 8, так как, в противном случае, она была бы циклической. Если все ее элементы порядка 2, то  $(ab)^2 = 1$ , или  $abab = 1$ ,  $ba = a^2bab^2 = ab$ , и группа  $G$  абелева. Поэтому группа  $G$  обладает элементом порядка 4, пусть, например,  $a^4 = 1$ . Если  $b \notin \{a\} = A$ , тогда  $G = A + Ab$  и  $b^2 \in A$ . Если  $b^2 = a$  или  $b^2 = a^3$ , то  $b$  — элемент порядка 8 и  $G$  — циклическая группа. Следовательно,  $b^2 = 1$ , или  $b^2 = a^2$ . Так как  $A$  — инвариантная подгруппа, то  $b^{-1}ab \in A$ , а так как  $b^{-1}ab$  — элемент порядка 4, то  $b^{-1}ab = a$ , или  $b^{-1}ab = a^3$ . Но при  $b^{-1}ab = a$ ,  $G$  — абелева группа. Поэтому  $b^{-1}ab = a^3$ . Итак, мы нашли две неабелевые группы: группу диэдра с определяющими отношениями

$$a^4 = 1, \quad b^2 = 1, \quad b^{-1}ab = a^3$$

и группу кватернионов с определяющими отношениями

$$a^4 = 1, \quad b^2 = a^2, \quad b^{-1}ab = a^3. \quad \text{Доказательство}$$

Легко проверить, что обе системы определяющих отношений действительно определяют две группы порядка 8, неизоморфные друг другу.

Теперь рассмотрим неабелевы группы порядка  $p^3$  при нечетном простом  $p$ . Так как  $G$  — нециклическая группа, она не содержит элемента порядка  $p^3$ . Предположим сначала, что  $G$  содержит элемент  $a$  порядка  $p^2$ ,  $a^{p^2} = 1$ . Тогда подгруппа  $\{a\} = A$ , являясь максимальной, инвариантна в группе  $G$ . Если  $b \notin A$ , тогда  $G = A + Ab + \dots + Ab^{p-1}$ ,  $b^p \in A$  и  $b^{-1}ab = a^r$ , причем  $r \neq 1$ , так как  $G$  — неабелева группа. Так как для произвольного  $j$  справедливо равенство  $b^{-j}ab^j = a^{r^j}$  и так как  $b^p$ , являясь элементом подгруппы  $A$ , перестановочен с  $a$ , имеем  $a = b^{-p}ab^p = a^{rp}$ , откуда  $r^p \equiv 1 \pmod{p^2}$ . Согласно теореме Ферма,  $r^p \equiv r \pmod{p}$ , следовательно,  $r \equiv 1 \pmod{p}$ . Пусть  $r = 1 + sp$ . Тогда при таком  $j$ , что  $js \equiv 1 \pmod{p}$ , мы имеем

$$b^{-j}ab^j = a^{(1+sp)^j} = a^{1+sjp} = a^{1+p}.$$

Так как  $(j, p) = 1$  и  $b^j \notin A$ , то в равенстве

$$G = A + Ab + \dots + Ab^{p-1}$$

под  $b$  можно понимать  $b^j$ , тогда  $b^{-1}ab = a^{1+p}$ .

Пусть  $b^p \in A$ , тогда  $b^p = a^t$ . Здесь  $t$  должно быть кратно  $p$ , так как порядок элемента  $b$  отличен от  $p^3$ . Пусть  $b^p = a^{up}$ . Тогда, учитывая, что  $a^i b = b a^{i(1+p)}$ , получаем

$$(ba^{-u})^p = b^p a^{-u [1+(1+p)+(1+p)^2+\dots+(1+p)^{p-1}]} = \\ = b^p a^{-up-up(1+2+\dots+p-1)} = b^p a^{-up} = 1.$$

Здесь учитываем, что  $1+2+\dots+p-1 = p(p-1)/2$  кратно  $p$ , так как  $p$  нечетно. Теперь при  $b_1 = ba^{-u}$  имеем  $a^{p^2} = 1$ ,  $b_1^p = 1$ ,  $b_1^{-1}ab_1 = a^{1+p}$ . Последнее соотношение имеет место, так как  $b_1^{-1}ab_1 = a^u(b^{-1}ab)a^{-u}$ .

Наконец, пусть  $G$  не содержит элементов порядка  $p^2$ . Порядок центра  $Z$  группы  $G$  равен  $p$ , так как если бы он был равен  $p^2$ , то группа была бы абелевой. Фактор-группа  $G/Z$  задается отношениями  $x^p = 1$ ,  $y^p = 1$ ,  $yx = xy$ . Если при гомоморфизме  $G \rightarrow G/Z$   $a \rightarrow x$ ,  $b \rightarrow y$ , то  $a^p = 1$ ,  $b^p = 1$ ,  $a^{-1}b^{-1}ab = c \in Z$ . Если бы  $a^{-1}b^{-1}ab = 1$ , то так как элементы  $a$  и  $b$  в совокупности с  $Z$  порождают всю группу  $G$ ,  $G$  была бы абелевой. Отсюда  $c \neq 1$  и  $c$  порождает центр  $Z$ , а группа  $G$  задается следующими определяющими отношениями:

$$a^p = 1, b^p = 1, c^p = 1, ab = bac, ac = ca, bc = cb.$$

## ТАБЛИЦА ОПРЕДЕЛЯЮЩИХ ОТНОШЕНИЙ

I. Группа  $G$  порядка  $p$ .1) Циклическая,  $a^p = 1$ .II. Группа  $G$  порядка  $p^2$ .1) Циклическая,  $a^{p^2} = 1$ .2) Элементарная абелева,  $a^p = 1$ ,  $b^p = 1$ ,  $ba = ab$ .III. Группа  $G$  порядка  $pq$ ,  $p < q$ .1) Циклическая,  $a^{pq} = 1$ .

2) Неабелева,  $a^p = 1$ ,  $b^q = 1$ ,  $a^{-1}ba = b^r$ ,  $r^p \equiv 1 \pmod{q}$ ,  
 $r \not\equiv 1 \pmod{q}$ ,  $p$  делит  $q - 1$ . Решения сравнения  $r^p \equiv 1 \pmod{q}$ ,  
 $r \not\equiv 1 \pmod{q}$ , следующие:  $r, r^2, \dots, r^{p-1}$ , причем все эти реше-  
ния дают одну и ту же группу, так как замена образующего  
элемента  $a$  циклической группы  $\{a\}$ ,  $a^p = 1$ , на  $a^j$  приводит  
к замене  $r$  на  $r^j$ .

IV. Группа  $G$  порядка  $p^3$ .

Абелевы группы:

1)  $a^{p^3} = 1$ .2)  $a^{p^2} = 1$ ,  $b^p = 1$ ,  $ba = ab$ .3)  $a^p = b^p = c^p = 1$ ,  $ba = ab$ ,  $ca = ac$ ,  $cb = bc$ .Неабелевы группы порядка  $2^3 = 8$ :4) группа диэдра,  $a^4 = 1$ ,  $b^2 = 1$ ,  $ba = a^{-1}b$ .5) группа кватернионов,  $a^4 = 1$ ,  $b^2 = a^2$ ,  $ba = a^{-1}b$ .Неабелевы группы порядка  $p^3$ ,  $p$  — нечетное:4)  $a^{p^2} = 1$ ,  $b^p = 1$ ,  $b^{-1}ab = a^{1+p}$ .5)  $a^p = 1$ ,  $b^p = 1$ ,  $c^p = 1$ ,  $ab = bac$ ,  $ca = ac$ ,  $cb = bc$ .

## Упражнения

1. Показать, что если  $H$  — инвариантная подгруппа конечной группы  $G$  и индекс  $[G:H]$  взаимно прост с  $p$ , то любая силовская  $p$ -подгруппа группы  $G$  содержится в  $H$ .

2. Показать, что в любой группе  $G$  инвариантная подгруппа  $K$  порядка  $p^a$  содержитя в каждой силовской  $p$ -подгруппе группы  $G$ .

3. Показать, что любая группа порядка  $p^2q$ , где  $p$  и  $q$  — различные простые числа, содержит инвариантную силовскую подгруппу.

4. Показать, что группа порядка 200 содержит инвариантную силовскую подгруппу.

5. Сколько элементов порядка 7 содержит группа порядка 168, не имеющая инвариантной подгруппы?

6. В следующей таблице указано число групп каждого из порядков от 1 до 20. Проверить ее, за исключением групп шестнадцатого порядка.

Порядок	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
число групп	1	1	1	2	1	2	1	5	2	2	1	5	1	2	1	14	1	5	1	5

# Гла́ва 5

## ГРУППЫ ПОДСТАНОВОК

### 5.1. Циклы

Согласно теореме Кэли (см. гл. 1), любая группа может быть представлена как группа подстановок. Как отмечалось там же, для одной и той же группы существует несколько таких представлений. То, что подстановка  $\pi$  переводит элемент  $x_i$  в  $x_j$ , будем обозначать так:  $(x_i)\pi = x_j$ .

*Конечным циклом* называется подстановка  $\pi$  конечного множества элементов  $x_1, x_2, \dots, x_n$ , такая, что  $(x_1)\pi = x_2, \dots, (x_{n-1})\pi = x_n, (x_n)\pi = x_1$ .

*Бесконечным циклом* называется подстановка  $\pi$  бесконечного множества элементов  $x_i (i = -\infty, \dots, +\infty)$ , такая, что  $(x_i)\pi = x_{i+1}$ .

Конечный цикл будем обозначать  $(x_1, x_2, \dots, x_n)$ , а бесконечный  $(\dots, x_{-1}, x_0, x_1, \dots)$ . Ясно, что циклы  $(x_2, x_3, \dots, x_n, x_1)$  и  $(x_1, x_2, \dots, x_n)$  представляют одну и ту же подстановку.

**Теорема 5.1.1.** *Пусть  $\pi$  — произвольная подстановка элементов некоторого множества  $S$ . Множество  $S$  можно разбить на такие непересекающиеся подмножества, что  $\pi$  индуцирует цикл на каждом из них.*

*Доказательство.* Пусть  $x_1$  — элемент множества  $S$ . Если  $(x_1)\pi = x_1$ , то  $(x_1)$  — уже цикл. Если  $(x_1)\pi \neq x_1$ , то обозначим элемент  $(x_1)\pi$  через  $x_2$ . Затем выписываем элементы множества  $S$   $(x_2)\pi = x_3, \dots, (x_i)\pi = x_{i+1}$  до тех пор, пока они не начнут повторяться. Если элементы  $(x_1)\pi = x_2, \dots, (x_{n-1})\pi = x_n$  все различны, а элемент  $(x_n)\pi$  уже встречался, то  $(x_n)\pi = x_i$  для некоторого  $i = 1, \dots, n$ . Если  $i = 2, \dots, n$ , то  $(x_{i-1})\pi = x_i$ , что противоречит условию  $x_n \neq x_{i-1}$ . Следовательно,  $(x_n)\pi = x_1$  и подстановка  $\pi$  индуцирует конечный цикл  $(x_1, \dots, x_n)$  из элементов  $x_1, \dots, x_n$ . Пусть элементы  $(x_1)\pi^i = x_{i+1} (i = 1, \dots)$  все различны, и пусть  $x_0$  — такой элемент, что  $(x_0)\pi = x_1$ . Затем последовательно из условий  $(x_{i-1})\pi = x_i (i = 0, -1, -2, \dots)$  определяем элементы  $x_{-1}, x_{-2}, \dots$ . Все элементы этой последовательности различны, так как подстановка  $\pi$  не может переводить два элемента в один и тот же элемент. Таким образом, любой элемент  $x$  множества  $S$  принадлежит некоторому подмножеству, которое подстановка  $\pi$  переставляет циклически. Но ведь любой элемент такого

подмножества определяет его однозначно, так как равенством  $(x)\pi = y$  каждый из элементов  $x$  и  $y$  однозначно определяется другим. Следовательно, различные подмножества не пересекаются.

Мы можем, таким образом, представить любую подстановку  $\pi$  в виде произведения циклов, и так как циклы действуют на непересекающихся множествах элементов, то порядок их записи не имеет значения.

При записи подстановки  $\pi$  в виде произведения циклов циклы длины 1 обычно опускаются; при этом подразумевается, что подстановка  $\pi$  оставляет на месте отсутствующие элементы. Так, например,  $\pi = (1)(2)(3, 4, 5) = (3, 4, 5)$ . При таком соглашении подстановку можно рассматривать как групповое произведение ее циклов, если только количество этих циклов конечно.

**Теорема 5.1.2.** *Порядок подстановки  $\pi$  равен наименьшему общему кратному длин ее циклов.*

**Доказательство.** Для цикла  $(x_1, \dots, x_n)$  имеем  $(x_i)\pi^j = x_{i+j}$ , где  $i+j$  берется по модулю  $n$ . Следовательно,  $(x_i)\pi^t = x_i$  тогда и только тогда, когда  $t$  кратно числу  $n$ . Тогда  $(x_i)\pi^m = x_i$  для всех  $x_i \in S$  в том и только в том случае, когда  $m$  кратно длинам всех циклов подстановки  $\pi$ . Следовательно, при таком  $m$   $\pi^m = 1$ . Если  $\pi$  содержит цикл бесконечной длины или как угодно длинные циклы, то подстановка  $\pi$  имеет бесконечный порядок.

Полезна следующая выкладка.

**Лемма 5.1.1.** *Если*

$$T = (a_{11} \dots a_{1r})(a_{21} \dots a_{2s}) \dots (a_{m1} \dots a_{mt})$$

и

$$S = \begin{pmatrix} a_{11} \dots a_{1r} & a_{21} \dots a_{2s} \dots a_{m1} \dots a_{mt} \\ b_{11} \dots b_{1r} & b_{21} \dots b_{2s} \dots b_{m1} \dots b_{mt} \end{pmatrix}.$$

то

$$S^{-1}TS = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt}).$$

**Доказательство.** Для произвольного элемента  $b_{jk}$  имеем

$$b_{j, k} \xrightarrow{S^{-1}} a_{j, k} \xrightarrow{T} a_{j, k+1} \xrightarrow{S} b_{j, k+1},$$

т. е. подстановка  $S^{-1}TS$  переводит элемент  $b_{jk}$  в элемент  $b_{j, k+1}$ .

Группа всех подстановок некоторого множества элементов называется *симметрической группой*. Симметрическую группу множества из  $n$  символов обозначают через  $S_n$ .

**Теорема 5.1.3.** *Две подстановки сопряжены в симметрической группе тогда и только тогда, когда они имеют одинаковое число циклов каждой длины.*

*Доказательство.* Необходимость этого условия следует из леммы 5.1.1. Для доказательства достаточности предположим, что

$$T = (a_{11} \dots a_{1r})(a_{21} \dots a_{2s}) \dots (a_{m1} \dots a_{mt})$$

и

$$R = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt})$$

имеют одинаковое число циклов каждой длины, включая и циклы длины 1. Так как по условию  $T$  и  $R$  имеют одинаковое число циклов каждой длины, то эти подстановки можно записать в указанном виде. Тогда

$$Q = \begin{pmatrix} a_{11} \dots a_{1r} \dots a_{m1} \dots a_{mt} \\ b_{11} \dots b_{1r} \dots b_{m1} \dots b_{mt} \end{pmatrix}$$

— такая подстановка, что  $Q^{-1}TQ = R$ .

Отметим, что эта теорема не накладывает никаких условий конечности, и «одинаковые числа» можно понимать как равные кардинальные числа. При доказательстве мы должны включить в рассмотрение циклы длины 1, так как в случае бесконечного исходного множества подстановки  $T$  и  $R$  могли бы иметь одинаковое число циклов длины, большей 1, но оставлять на месте разное число элементов. Так, подстановки  $T = (0, 1)(2, 3)(4, 5) \dots$  и  $R = (0)(1, 2)(3, 4)(5, 6) \dots$  не сопряжены в симметричной группе множества чисел  $0, 1, 2, 3, \dots$

## 5.2. Транзитивность

**Теорема 5.2.1.** Пусть  $G$  — группа подстановок множества символов  $X = \{x_1, \dots, x_n\}$ ,  $S$  — некоторое подмножество множества  $X$ . Тогда подстановки из группы  $G$ , оставляющие на месте символы из  $S$ , образуют подгруппу  $K$ . Подстановки, переставляющие между собой символы из  $S$ , образуют подгруппу  $H$ , которая содержит  $K$  в качестве нормального делителя.

*Доказательство.* Если две подстановки  $a$  и  $b$  из группы  $G$  переставляют символы из множества  $S$  или оставляют их на месте, то этими же свойствами обладают подстановки  $ab$  и  $a^{-1}$ . Значит, существует подгруппа  $H$ , переставляющая элементы подмножества  $S$ , и ее подгруппа  $K$ , оставляющая каждый элемент из  $S$  на месте. Если  $h \in H$ ,  $k \in K$ , то  $h^{-1}kh$  — подстановка, оставляющая элементы из  $S$  на месте. Поэтому  $K$  — нормальный делитель группы  $H$ .

**Определение.** Группа подстановок  $G$  элементов  $x_1, \dots, x_n$  называется *транзитивной* на подмножестве  $S$  множества  $x_1, \dots, x_n$ , если для любой подстановки  $\sigma \in G$  и любого элемента  $x_i \in S$  ( $x_i \sigma \in S$ ) и если для  $x_i, x_j \in S$  существует такая подстановка

$\sigma \in G$ , что  $(x_i)\sigma = x_j$ .<sup>1</sup> Подмножество  $S$  называется *областью транзитивности* группы  $G$ .

Теорема 5.2.2. *Если для фиксированного элемента  $x_1$  множество  $S$  состоит из всех таких  $x_i$ , что  $x_i = (x_1)\sigma$ , где  $\sigma \in G$ , то  $S$  является областью транзитивности.*

Доказательство. Если  $(x_1)\sigma = x_i$ ,  $(x_1)\tau = x_j$ , то  $(x_i)\sigma^{-1}\tau = x_j$ . Кроме того, если  $(x_1)\sigma = x_i$ ,  $(x_i)\rho = x_k$ , то  $(x_1)\sigma\rho = x_k$ .

Теорема 5.2.3. *Пусть  $S$  — область транзитивности группы подстановок  $G$ , и  $x_1 \in S$ . Для каждого  $x_i \in S$  выберем такую  $\sigma_i \in G$ ; что  $(x_1)\sigma_i = x_i$ . Пусть  $H$  — подгруппа группы  $G$ , оставляющая на месте  $x_1$ . Тогда  $G = H\sigma_1 + H\sigma_2 + \dots + H\sigma_i + \dots$*

Доказательство. Если  $g = h\sigma_i$ , где  $h \in H$ , то  $(x_1)g = x_i$ , значит, смежные классы  $H\sigma_i$  различны. Далее, пусть  $g$  — некоторый элемент из группы  $G$ . Тогда  $(x_1)g = x_i$  для некоторого  $x_i \in S$ . Тогда  $(x_1)g\sigma_i^{-1} = x_1$ , откуда  $g\sigma_i^{-1} \in H$ ,  $g = h\sigma_i \in H\sigma_i$  и, следовательно, смежные классы  $H\sigma_i$  исчерпывают группу  $G$ .

Следствие 5.2.1. *Если область транзитивности  $S$  группы  $G$  содержит точно  $r$  элементов, то подгруппа  $H$ , оставляющая на месте один элемент из  $S$ , имеет индекс  $r$  в  $G$ .*

Определение. Группа  $G$  называется *k-кратно транзитивной на множестве  $S$* , если она транзитивна на  $S$  и если любое упорядоченное множество, состоящее из  $k$  различных элементов множества  $S$ , может быть переведено в любое другое упорядоченное множество из  $k$  различных элементов множества  $S$  некоторой подстановкой из группы  $G$ .

Теорема, аналогичная теореме 5.2.2, имеет место для  $k$ -кратно транзитивных групп. Если группа  $G$  переводит фиксированное множество  $x_1, \dots, x_k$  из  $k$  элементов в любое другое упорядоченное множество элементов  $y_1, \dots, y_k$  из  $S$ , то  $G$  есть  $k$ -кратно транзитивная группа на множестве  $S$ . Подгруппа группы  $G$ , оставляющая на месте  $r < k$  элементов из множества  $S$ , является  $(k - r)$ -кратно транзитивной группой на множестве остальных элементов множества  $S$ . Если  $G$  —  $r$ -кратно транзитивная группа и если подгруппа  $H$ , оставляющая на месте  $r$  элементов, сама  $s$ -кратно транзитивна, то группа  $G$  —  $(r + s)$ -кратно транзитивна.

### 5.3. Представления группы подстановками

Как уже отмечалось, любая абстрактная группа может быть представлена, вообще говоря, более чем одним способом как группа подстановок. Будем называть группу  $P$  подстановок представлением группы  $G$ , если существует отображение группы  $G$  на  $P$ :  $g \rightarrow \pi(g)$ ,  $g \in G$ ,  $\pi(g) \in P$ , такое, что  $\pi(g_1)\pi(g_2) = \pi(g_1g_2)$ .

1) В противном случае группа подстановок  $G$  называется *интранзитивной* на подмножестве  $S$ . — Прим. перев.

Заметим, что  $P$  является гомоморфным образом группы  $G$ . Если же группа  $P$  даже изоморфна  $G$ , мы будем говорить, что  $P$  есть *точное* представление группы  $G$ . Подобно тому как все гомоморфные образы группы  $G$  описываются при помощи факторгрупп по нормальным делителям, все представления группы  $G$  транзитивными группами подстановок могут быть описаны в терминах левых смежных классов по подгруппам группы  $G$ .

Так как уже для неабелевой группы порядка 6 существует точное представление транзитивной группой подстановок трех, а также шести элементов, то мы должны различать некоторые группы подстановок, изоморфные как абстрактные группы.

**Определение.** Группа  $P_1$  подстановок множества  $S_1$  изоморфна, как группа подстановок, группе  $P_2$  подстановок множества  $S_2$ , если существует изоморфизм  $\pi_{P_1} \leftrightarrow \pi_{P_2}$  между  $P_1$  и  $P_2$  и взаимно однозначное соответствие  $x_i \leftrightarrow y_i$  между множествами  $S_1$  и  $S_2$  такое, что  $(x_i)\pi_{P_1} = x_j$  тогда и только тогда, когда  $(y_i)\pi_{P_2} = y_j$ <sup>1)</sup>.

**Теорема 5.3.1.** Пусть  $G$  — группа и  $H$  — ее подгруппа. Тогда имеют место следующие утверждения:

а) каждому элементу  $g \in G$  соответствует следующая подстановка левых смежных классов по  $H$ :

$$\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}, \quad x \in G;$$

в) отображение  $g \rightarrow \pi(g)$  есть представление группы  $G$  транзитивной группой подстановок левых смежных классов по подгруппе  $H$ , причем  $\pi(g)$  оставляет  $H$  на месте в том и только в том случае, когда  $g \in H$ .

Обратно, пусть  $g \rightarrow \pi(g)$  есть представление группы  $G$  транзитивной группой подстановок  $P$  множества элементов  $S$ . Тогда справедливы следующие утверждения:

с) если  $s_1$  — некоторый элемент из  $S$ , множество элементов  $g \in G$ , таких, что подстановки  $\pi(g)$  оставляют элемент  $s_1$  на месте, образуют подгруппу  $H$  группы  $G$ ;

д) между элементами множества  $S$  и левыми смежными классами по  $H$  можно установить взаимно однозначное соответствие так, чтобы группа подстановок  $P$  была изоморфна группе подстановок, описанной в первой части теоремы.

**Доказательство.** а) Отображение  $Hx \rightarrow (Hx)g = Hxg$  взаимно однозначно, причем любой левый смежный класс является

<sup>1)</sup> Изоморфизм групп подстановок называется иногда подобием, а изоморфные группы подстановок — подобными. В дальнейшем мы иногда будем пользоваться этими терминами. — Прим. перев.

образом, так как  $(Hxg^{-1})g = Hx$ . Поэтому  $\pi(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$  есть подстановка множества левых смежных классов по  $H$ .

в) Из равенства  $(Hxg_1)g_2 = Hx(g_1g_2)$  следует, что  $\pi(g_1)\pi(g_2) = \pi(g_1g_2)$ . Поэтому  $g \rightarrow \pi(g)$  — представление группы  $G$ . Отображение  $H \rightarrow Hg = H$  имеет место тогда и только тогда, когда  $g \in H$ . Иначе говоря,  $\pi(g)$  оставляет  $H$  на месте в том и только том случае, когда  $g \in H$ . Так как подстановка  $\pi(x)$  отображает  $H$  на  $Hx$ , это представление транзитивно.

с) Легко проверяется, что указанные элементы группы образуют подгруппу  $H$ , так как если  $g_1$  и  $g_2$  обладают этим свойством, то элементы  $g_1g_2$  и  $g_1^{-1}$  обладают им также.

д) Множество тех элементов  $g \in G$ , для которых имеет место равенство  $(s_i)\pi(g) = s_i$ , не пусто в силу транзитивности группы подстановок  $P$ . Если  $x_i$  — один из таких элементов, то сразу видно, что все они составляют весь левый смежный класс  $Hx_i$ , где  $H$  — подгруппа, рассмотренная в пункте с). Обратно, все элементы из левого смежного класса  $Hx$  обладают тем свойством, что под действием соответствующих им подстановок элемент  $s_i$  переходит в один и тот же элемент. Этим установлено взаимно однозначное соответствие  $s_i \leftrightarrow Hx_i$  между элементами множества  $S$  и левыми смежными классами по  $H$ . Пусть  $P_1$  — группа подстановок множества левых смежных классов по  $H$ , определенная

в пунктах а) и в), причем подстановка  $\pi_1(g) = \begin{pmatrix} Hx \\ Hxg \end{pmatrix}$ ,  $g \in G$ , принадлежит группе  $P_1$ . Если в группе  $P$  имеет место равенство  $(s_i)\pi(g) = s_j$ , то  $(s_i)[\pi(x_i)\pi(g)] = s_j$ , откуда  $x_i g \in Hx_j$ , значит,  $(Hx_i)g = Hx_j$ . Наоборот, из последнего соотношения следует, что  $(s_i)\pi(g) = s_j$ . Таким образом, соотношение  $(s_i)\pi(g) = s_j$  выполняется тогда и только тогда, когда  $Hx_i \pi_1(g) = Hx_j$ . В частности,  $\pi(g)$  — тождественная подстановка тогда и только тогда, когда  $\pi_1(g)$  тождественна. Итак,  $P$  и  $P_1$  являются гомоморфными образами группы  $G$  с одним и тем же ядром, причем соответствие  $\pi(g) \leftrightarrow \pi_1(g)$  является изоморфиzmом между ними. Вследствие взаимной однозначности соответствия  $s_i \leftrightarrow Hx_i$  между  $S$  и множеством левых смежных классов по  $H$  получаем, что группа подстановок  $P$  изоморфна группе  $P_1$ , так как равенство  $(s_i)\pi(g) = s_j$  выполняется тогда и только тогда, когда  $Hx_i \pi_1(g) = Hx_j$ .

Этой теоремой все представления группы  $G$  транзитивными группами подстановок сводятся к представлениям множества смежных классов группы  $G$  по подгруппе  $H$ . Если  $H$  — единичная подгруппа, мы приходим к правому регулярному представлению, рассмотренному в § 1.4.

**Теорема 5.3.2.** Элементы, переходящие при представлении  $g \rightarrow \pi(g)$  (теорема 5.3.1) в единицу, образуют наибольшую инвариантную подгруппу группы  $G$ , содержащуюся в  $H$ , а поэтому представление точно тогда и только тогда, когда  $H$  не содержит собственных инвариантных подгрупп группы  $G$ .

**Доказательство.** Для каких  $g \in G$  подстановка  $\pi(g)$  — тождественная подстановка? Пусть  $Hxg = Hx$  для всех  $x \in G$ . Тогда  $x^{-1}Hxg = x^{-1}Hx$ , т. е.  $g \in x^{-1}Hx$ . Следовательно,

$$g \in \bigcap_x x^{-1}Hx = N,$$

причем ясно, что  $N$  — нормальный делитель группы  $G$  и  $N \subset H$ . Кроме того, любой нормальный делитель группы  $G$ , содержащийся в  $H$ , содержится и во всех  $x^{-1}Hx$ , а поэтому и в  $N$ . Таким образом,  $N$  есть наибольший нормальный делитель группы  $G$ , содержащийся в  $H$ . Обратно, если  $g \in N$ , то  $Hxg = Hx$  при любом  $x$ , а значит,  $\pi(g) = 1$ . Следовательно, равенство  $N = 1$  является необходимым и достаточным условием точности представления  $g \rightarrow \pi(g)$  группы  $G$ .

**Следствие 5.3.1.** Единственным точным транзитивным представлением абелевой группы служит регулярное представление.

**Теорема 5.3.3.** Два точных представления группы  $G$  подстановками множеств смежных классов группы  $G$  по подгруппам  $H_1$  и  $H_2$  изоморфны как группы подстановок в том и только в том случае, когда существует такой автоморфизм  $\alpha$  группы  $G$ , что  $H_1^\alpha = H_2$ .

**Доказательство.** Если  $\alpha$  — автоморфизм группы  $G$ , для которого  $H_1^\alpha = H_2$ , то соответствие

$$H_1 x \rightleftharpoons H_1^\alpha x^\alpha = H_2 x^\alpha$$

— взаимно однозначное соответствие между смежными классами по  $H_1$  и  $H_2$ ; если  $g \rightarrow \pi_1(g)$  — представление группы  $G$  подстановками множеств смежных классов по  $H_1$ , а  $g \rightarrow \pi_2(g)$  — по подгруппе  $H_2$ , то

$$\pi_1(g) \rightleftharpoons \pi_2(g^\alpha).$$

Обратно, предположим, что имеет место изоморфизм представлений

$$\pi_1(g) \rightleftharpoons \pi_2(g^*)$$

Так как оба представления точные, то этим определяется взаимно однозначное соответствие  $g \rightleftharpoons g^*$ , которое является автоморфизмом  $\beta$  группы  $G$ . При рассматриваемом изоморфизме представлений

$\pi_1(g) \leq \pi_2(g^*)$  имеем  $H_1 \not\supseteq H_2 u$ . Таким образом, если  $H_1 g = H_1$ , то  $H_2 ug^\beta = H_2 u$ , или  $u^{-1}H_2 u g^\beta = u^{-1}H_2 u$ , и обратно. Следовательно, если  $g \in H_1$ , то  $g^\beta \in u^{-1}H_2 u$ , и наоборот. Но  $H_1^\beta = u^{-1}H_2 u$ , или  $H_2 = uH_1^\beta u^{-1} = H_1^\alpha$ , где  $\alpha$  — автоморфизм группы  $G$ .

#### 5.4. Знакопеременная группа $A_n$

Рассмотрим полином от  $n$  переменных:  $\Delta = \prod_{i < j} (x_i - x_j)$ ;  $i, j \leq n$ ,  $n \geq 2$ . Если в нем произвести перестановку переменных  $x_1, x_2, \dots, x_n$ , то он перейдет в  $\Delta$  или в  $-\Delta$ . Записывая полином  $\Delta$  в виде

$$\begin{aligned}\Delta = & (x_1 - x_2)(x_1 - x_3) \dots (x_1 - x_n) \times \\ & \times (x_2 - x_3) \dots (x_2 - x_n) \times \\ & \dots \dots \dots \dots \times (x_{n-1} - x_n),\end{aligned}$$

видим, что перестановка  $(x_1, x_2)$  переводит  $x_1 - x_2$  в  $x_2 - x_1 = -(x_1 - x_2)$  и переставляет между собой остальные сомножители первой строки и соответствующие сомножители второй строки, а остальные скобки оставляет без изменения. В результате перестановка  $(x_1, x_2)$  переводит  $\Delta$  в  $-\Delta$ . Будем называть подстановку *четной*, если она не изменяет полином  $\Delta$ , и *нечетной*, если она переводит его в  $-\Delta$ .

**Теорема 5.4.1.** Четные подстановки множества  $x_1, x_2, \dots, x_n$  образуют инвариантную подгруппу индекса 2 в симметрической группе  $S_n$ . Она называется знакопеременной группой  $A_n$ .

**Доказательство.** Непосредственно проверяется, что произведение двух четных подстановок четно, произведение двух нечетных подстановок — четно, а произведение четной и нечетной подстановок и нечетной подстановки на четную — нечетно. Отметим также, что тождественная подстановка четна.

Мы видим, что четные подстановки группы  $S_n$  образуют подгруппу  $A_n$ . Так как  $(x_1, x_2)$  — нечетная подстановка, смежный класс  $A_n(x_1, x_2)$  состоит только из нечетных подстановок. Если  $\pi$  — любая подстановка, то одна из подстановок  $\pi, \pi \cdot (x_1, x_2)$  четная, а другая — нечетная. Так как  $\pi = [\pi \cdot (x_1, x_2)] \cdot (x_1, x_2)$ , смежные классы  $A_n$  и  $A_n \cdot (x_1, x_2)$  исчерпывают всю группу  $S_n$ , т. е.  $S_n = A_n + A_n \cdot (x_1, x_2) = A_n + (x_1, x_2) \cdot A_n$ . Следовательно,  $A_n$  — подгруппа индекса 2 в  $S_n$ , и поэтому она инвариантна.

Цикл  $(x_i, x_j)$  длины 2 называется *транспозицией*. По теореме 5.1.3 все транспозиции группы  $S_n$  сопряжены с циклом  $(x_1, x_2)$ . Произвольная подстановка  $\pi$  и обратная к ней подстановка  $\pi^{-1}$  имеют одинаковую четность. Следовательно

$\pi^{-1}(x_1, x_2)\pi = (x_i, x_j)$  — нечетная подстановка. Нечетность транспозиции  $(x_i, x_j)$  можно проверить и непосредственно.

Любой цикл длины  $n$  записывается как произведение  $n - 1$  транспозиций:  $(x_1, x_2, \dots, x_n) = (x_1, x_2)(x_1, x_3) \dots (x_1, x_n)$ . Отсюда, согласно теореме 5.1.1, любая конечная подстановка представима в виде произведения транспозиций. Произведение четного числа транспозиций — четная подстановка, нечетного числа — нечетная. Итак, хотя представление подстановки в виде произведения транспозиций и неоднозначно, число транспозиций, участвующих в произведении, всегда имеет одну и ту же четность.

**Теорема 5.4.2.** Группа  $A_n$ ,  $n \geq 3$ ,  $(n - 2)$ -кратно транзитивна.

**Доказательство.** Пусть  $y_1, \dots, y_{n-2}, y_{n-1}, y_n$  — некоторая перестановка элементов  $x_1, \dots, x_{n-2}, x_{n-1}, x_n$ . Пусть

$$u = \begin{pmatrix} x_1, & \dots, & x_{n-2}, & x_{n-1}, & x_n \\ y_1, & \dots, & y_{n-2}, & y_{n-1}, & y_n \end{pmatrix}$$

и

$$v = \begin{pmatrix} x_1, & \dots, & x_{n-2}, & x_{n-1}, & x_n \\ y_1, & \dots, & y_{n-2}, & y_n, & y_{n-1} \end{pmatrix}.$$

Тогда  $v = u(y_{n-1}, y_n)$ , и одна из подстановок  $u$  и  $v$  четная, другая — нечетная. Поэтому группа  $A_n$   $(n - 2)$ -кратно транзитивна, но не  $n$ -кратно транзитивна. Ясно, что она не может также быть и  $(n - 1)$ -кратно транзитивной, так как в этом случае она была бы и  $n$ -кратно транзитивной.

В группе подстановок бесконечного множества  $\omega$  элементов знакопеременная группа  $A_\omega$  определяется как группа, состоящая из подстановок, разлагающихся в произведение четного числа транспозиций. Являясь нормальным делителем,  $A_\omega$  — подгруппа индекса 2 в группе  $H_\omega$  тех подстановок, каждая из которых перемещает только конечное число элементов. Согласно теореме 5.1.3, подгруппа  $H_\omega$  инвариантна в группе  $S_\omega$  и  $A_\omega$  будет нормальным делителем в  $S_\omega$  индекса 2 в  $H_\omega$ .

**Теорема 5.4.3.** Знакопеременная группа  $A_n$  является простой для всех  $n$ , конечных или бесконечных, кроме случая  $n = 4$ .

**Доказательство.** Группа  $A_2$  состоит только из тождественной подстановки.  $A_3$  — циклическая группа порядка 3 и, следовательно, простая. Группу  $A_4$  нужно рассмотреть особо. Итак, мы можем предположить, что число символов  $n \geq 5$ .

**Лемма 5.4.1.** Знакопеременная группа  $A_n$ ,  $n \geq 3$ , порождается всеми циклами  $(a, b, c)$  длины три.

**Доказательство.** Ясно, что группа  $A_n$  порождается произведениями пар транспозиций. Если две транспозиции одинаковы, их

произведение равно тождественной подстановке. Если они имеют одну общую букву, как, например,  $(a, b)$  и  $(a, c)$ , то  $(a, b)(a, c) = (a, b, c)$ . Если они не имеют общих букв, то  $(a, b)(c, d) = (a, b)(a, c)(c, a)(c, d) = (a, b, c)(c, a, d)$ , и лемма доказана.

Мы докажем, что любая инвариантная подгруппа  $G$  группы  $A_n$ ,  $n \geq 5$ , отличная от единичной, содержит все циклы длины три и, следовательно, совпадает с  $A_n$ . Для этого рассмотрим ряд случаев. Заметим, что так как  $G \subseteq A_n$ , то любой элемент из подгруппы  $G$  может быть представлен как произведение конечного числа конечных циклов.

**Случай 1.** *Подгруппа  $G$  содержит цикл  $(a, b, c)$  длины три.*

Тогда любой другой цикл  $(x, y, z)$  длины три лежит вместе с циклом  $(a, b, c)$  в знакопеременной группе  $A_r$ , конечного множества, состоящим из  $r$  букв, где можно считать, что  $r \geq 5$ . Так как  $A_r$  — группа  $(r - 2)$ -кратно транзитивная и  $r - 2 \geq 3$ , циклы  $(a, b, c)$  и  $(x, y, z)$  сопряжены в группе  $A_r$  и *тем более* в группе  $A_n$ . Но инвариантная подгруппа  $G$  должна содержать все элементы, сопряженные с  $(a, b, c)$  в группе  $A_n$ , а значит, и все циклы длины 3. Следовательно, по лемме 5.4.1  $G = A_n$ .

**Случай 2.** *Подгруппа  $G$  содержит элемент  $g$  с циклом длины  $s \geq 4$ .*

Пусть

$$g = (a_1, a_2, \dots, a_r) \dots (c_1, c_2, \dots, c_{s-3}, c_{s-2}, c_{s-1}, c_s),$$

тогда  $t = (c_{s-2}, c_{s-1}, c_s) \in A_n$  и

$$t^{-1}gt = (a_1, a_2, \dots, a_r) \dots (c_1, c_2, \dots, c_{s-3}, c_{s-1}, c_s, c_{s-2}).$$

Но элемент  $gt^{-1}g^{-1}t = (c_{s-3}, c_s, c_{s-2})$  принадлежит  $G$ , так как  $G$  — инвариантная подгруппа.

Этим мы свели случай 2 к случаю 1. Сейчас рассмотрим случаи, когда длины циклов не превышают 3.

**Случай 3.** *Некоторый элемент  $g \in G$  имеет, по меньшей мере, два цикла длины 3.*

Пусть

$$g = (a_1, a_2, a_3)(b_1, b_2, b_3) \dots (c_1, \dots, c_r).$$

Для элемента  $t = (a_3, b_1, b_2) \in A_n$

$$h = t^{-1}gt = (a_1, a_2, b_1)(b_2, a_3, b_3) \dots (c_1, \dots, c_r) \in G$$

и

$$gh^{-1} = (a_2, b_2, a_3, b_1, b_3) \in G.$$

Этим случай 3 сведен к случаю 2.

**Случай 4.** *Некоторый элемент  $g \in G$  имеет по меньшей мере один цикл длины 3, а остальные его циклы — длины 2.*

Пусть

$$g = (x_1, x_2)(y_1, y_2) \dots (z_1, z_2)(a, b, c) \dots (d, e, f).$$

Тогда  $g^2 = (a, c, b) \dots (d, f, e) \in G$ , и мы свели этот случай или к случаю 1, или к случаю 3.

**Случай 5.** Некоторый элемент  $g \in G$  состоит только из циклов длины 2, причем количество их не меньше четырех. Если  $g = (x, y)(z, u) \dots (a, b)(c, d) \in G$ , для элемента  $t = (y, a)(b, c) \in A_n$  имеем

$$\begin{aligned} h &= t^{-1}gt = (x, a)(z, u) \dots (y, c)(b, d) \in G, \\ gh &= (x, c, b)(y, a, d) \in G. \end{aligned}$$

Случай 5 свелся к случаю 3.

**Случай 6.** Элемент  $g \in G$  имеет только два цикла длины два.

Пусть

$$g = (a, b)(c, d) \in G.$$

Поскольку, по предположению,  $n \geq 5$ , кроме букв  $a, b, c, d$ , множество содержит еще хоть одну букву  $e$ . Возьмём элемент  $t = (a, b, e) \in A_n$ , тогда

$$\begin{aligned} h &= t^{-1}gt = (b, e)(c, d) \in G, \\ gh &= (a, e, b) \in G, \end{aligned}$$

и мы пришли к случаю 1.

Знакопеременная группа  $A_4$  из элементов 1, 2, 3, 4 не является простой, так как она содержит нормальный делитель, состоящий из четырех элементов  $(1), (12)(34), (13)(24), (14)(23)$ .

## 5.5. Интранзитивные группы. Подпрямые произведения

Пусть группа  $G$  подстановок интранзитивна, и пусть  $S_i(x_{i_1}, \dots)$ ,  $i \in I$  ( $I$  — множество индексов) — различные множества символов, на которых группа  $G$  транзитивна. Если вместо подстановок группы  $G$  рассматривать только подстановки множества  $S_i$ , то последние образуют группу  $G_i$ . Для любого  $i \in I$  элемент  $g$  из  $G$  определяет элемент  $g_i$  из  $G_i$ , а именно, подстановку букв из  $S_i$ , индуцируемую элементом  $g$ .

Кроме того, мы можем положить

$$g = \prod_i g_i, \tag{5.5.1}$$

рассматривая  $g$  как элемент декартова произведения групп  $G_i$ , так как групповая операция в группе  $G$  согласуется с этой же

операцией в декартовом произведении  $\prod_i G_i$ . Таким образом, интранзитивную группу можно рассматривать как подгруппу декартова произведения транзитивных групп. Мы будем говорить, что  $G$  есть *подпрямое произведение групп*  $G_i$ . Более точно, некоторая группа называется подпрямым произведением групп  $G_i$ , если

- 1)  $G$  — подгруппа декартова произведения групп  $G_i$ ;
- 2) для любого элемента  $g_j \in G_j$  существует по меньшей мере один элемент  $g \in G$ ,  $j$ -й компонентой которого является  $g_j$ .

Это второе условие требует, чтобы все элементы групп  $G_i$  участвовали в образовании элементов группы  $G$ .

Если все компоненты  $g_i$  участвуют в образовании подпрямого произведения  $G \subseteq \prod_i G_i$  независимо друг от друга, то  $G$  совпадает со всем декартовым произведением. Но в общем случае это не так. Следующая теорема выясняет характер возможной зависимости между компонентами подпрямого произведения. Пусть  $G_i$  и  $G_j$  — две компоненты или же, возможно, две группы, заданные двумя непересекающимися множествами компонент  $G_i$ ,  $i \in I_1$ , и  $G_j$ ,  $j \in I_2$ ,  $I_1 \cap I_2 = \emptyset$ . Если рассматривать только компоненты  $G_i$  и  $G_j$ , то элементы группы  $G$  индуцируют группу  $G^*$ , которая является подпрямым произведением групп  $G_i$  и  $G_j$ . Можно описать связь между компонентами  $G_i$  и  $G_j$  в группе  $G$ , выявляя строение индуцированного подпрямого произведения  $G^*$  групп  $G_i$  и  $G_j$ .

**Теорема 5.5.1.** *Пусть  $G^*$  — подпрямое произведение групп  $G_i$  и  $G_j$ ,  $H_{ij}$  и  $H_{ji}$  — подгруппы групп  $G_i$  и  $G_j$  соответственно, состоящие из элементов, которые участвуют в образовании тех элементов из  $G^*$ , одна компонента которых равна единице. Тогда подгруппа  $H_{ij}$  инвариантна в  $G_i$ ,  $H_{ji}$  — в  $G_j$ , причем существует изоморфизм между фактор-группами  $G_i/H_{ij} \cong K \cong G_j/H_{ji}$ , такой, что элемент  $(g_1, g_2)$ ,  $g_1 \in G_i$ ,  $g_2 \in G_j$  принадлежит подгруппе  $G^*$  тогда и только тогда, когда  $g_1$  и  $g_2$  имеют общий образ  $k$  при гомоморфизмах  $G_i \rightarrow K$ ,  $G_j \rightarrow K$ .*

*Доказательство.* Пусть  $(h, 1)$  — элементы подгруппы  $H_{ij}$  группы  $G_i$ , второй компонентой которых служит единица подгруппы  $G_j$  группы  $G^*$ . Тогда легко проверить, что подгруппа  $H_{ij}$  инвариантна в  $G_i$ , аналогично проверяется, что подгруппа  $H_{ji}$  инвариантна в  $G_j$ . Далее, для некоторого элемента  $g_1 \in G_i$  множество элементов  $g_2 \in G_j$ , таких, что  $(g_1, g_2) \in G^*$ , как легко видеть, составляет смежный класс по  $H_{ji}$ . Аналогично множество элементов  $g_1 \in G_i$ , таких, что  $(g_1, g_2) \in G^*$ , где  $g_2 \in G_j$ , как легко видеть, составляет смежный класс по  $H_{ij}$ . Далее, если  $(g_1, g_2) \in G^*$ , то все элементы из множества  $(H_{ij}g_1, H_{ji}g_2)$  принадлежат  $G^*$ , и никакой другой элемент  $(g'_1, g'_2)$  из  $G^*$  не содержит в качестве

компонент элементы смежных классов  $H_{ij}g_1$  и  $H_{ji}g_2$ . Следовательно, для любого элемента  $(g_1, g_2)$  из  $G^*$  устанавливается взаимно однозначное соответствие  $H_{ij}g_1 \leftrightarrow H_{ji}g_2$  между смежными классами по  $H_{ij}$  в  $G_i$  и смежными классами по  $H_{ji}$  в  $G_j$ .

Если элементы  $(g_1, g_2)$  и  $(g_3, g_4)$  принадлежат группе  $G^*$ , то элемент  $(g_1g_3, g_2g_4)$  также принадлежит  $G^*$ , значит, установленное соответствие сохраняет операцию умножения, т. е. является изоморфизмом между фактор-группами  $G_i/H_{ij}$  и  $G_j/H_{ji}$ . Если положить  $G_i/H_{ij} \cong K \cong G_j/H_{ji}$ , то при условии, что  $(g_1, g_2) \in G^*$ , элементы  $g_1$  и  $g_2$  принадлежат соответствующим смежным классам и поэтому имеют один и тот же образ  $k$  при гомоморфизмах  $G_i \rightarrow K$ ,  $G_j \rightarrow K$ .

Обратно, если две группы  $G_i$  и  $G_j$  обладают инвариантными подгруппами  $H_{ij}$  и  $H_{ji}$ , соответственно со свойством  $G_i/H_{ij} \cong K \cong G_j/H_{ji}$ , то все пары  $(g_1, g_2)$ , где  $g_1 \in G_i$ ,  $g_2 \in G_j$ , обладающие тем свойством, что  $g_1$  и  $g_2$  имеют один и тот же образ  $k$  при гомоморфизмах  $G_i \rightarrow K$ ,  $G_j \rightarrow K$ , образуют подпрямое произведение  $G^*$  в описанном выше смысле.

## 5.6. Примитивные группы

Предположим,  $G \neq 1$  — группа подстановок некоторого множества, которое может быть разбито на непересекающиеся подмножества  $S_1, \dots, S_m$  так, что любая подстановка из группы  $G$  либо отображает все множество  $S_i$  на себя, либо на другое множество  $S_j$ . Если такое разбиение можно провести нетривиальным образом, т. е. так, чтобы подмножеств было больше одного и чтобы не все они имели по одному элементу, то группа  $G$  называется *импримитивной*, а множества  $S_1, \dots, S_m$  — областями импримитивности. Из определения ясно, что интранзитивная группа *тем более* импримитивна. Если группа  $G$  не импримитивна, то она называется *примитивной*. Таким образом, примитивная группа есть транзитивная группа, основное множество которой нельзя разбить на собственные подмножества, переводимые одно в другое этой группой подстановок.

**Теорема 5.6.1.** Пусть  $G$  — транзитивная, но импримитивная группа. Пусть  $S_1$  — одна из областей импримитивности,  $y_1$  — один из элементов множества  $S_1$  и  $H$  — подгруппа подстановок, оставляющих элемент  $y_1$  на месте. Тогда элементы группы  $G$ , отображающие  $S_1$  на себя, образуют подгруппу  $K$ , причём  $H \subset K \subset G$ . Число областей импримитивности равно индексу  $[G:K]$ , и каждая область импримитивности состоит из  $[K:H]$  элементов. Обратно, если  $G$  — транзитивная группа и  $H$  — подгруппа подстановок, оставляющих на месте элемент  $y_1$ , и если существует подгруппа  $K$ , такая,

что  $G \supset K \supset H$ , то группа  $G$  импримитивна и одна из ее областей импримитивности состоит из  $[K : H]$  элементов, в которые подстановки из подгруппы  $K$  переводят элемент  $y_1$ . Существует  $[G : K]$  областей импримитивности, соответствующих левым смежным классам по  $K$ . Таким образом, группа  $G$  подстановок примитивна тогда и только тогда, когда подгруппа  $H$ , оставляющая на месте некоторый элемент, максимальна.

**Доказательство.** Пусть  $G$  — транзитивная и импримитивная группа подстановок. Пусть  $S_1, \dots, S_m$  — области импримитивности для группы  $G$ , и пусть  $H$  — подгруппа, оставляющая на месте элемент  $y_1$  из  $S_1$ . Если

$$G = H + Hx_2 + \dots + Hx_n, \quad (5.6.1.)$$

то, согласно теореме 5.3.1, мы можем отождествить элементы  $y_1, \dots, y_n$  основного множества группы подстановок  $G$  с левыми смежными классами  $Hx_i$  из разложения (5.6.1), на которых действуют подстановки  $\pi(g) : Hx_i \rightarrow Hx_i g$ , где  $g$  — любой элемент из  $G$ . Если  $y_1, y_2, \dots, y_t$  образуют множество  $S_1$ , то элементы группы  $G$ , отображающие это множество на себя, образуют подгруппу  $K$ . Подстановка, оставляющая на месте  $y_1$ , должна отображать множество  $S_1$  на себя, откуда  $H \subset K$ , причем включение строгое, так как подстановка, переводящая  $y_1$  в  $y_2$ , принадлежит подгруппе  $K$ , но не принадлежит  $H$ . Так как подгруппа  $K$  транзитивна на множестве  $S_1$ , из разложения

$$K = H + Hx_2 + \dots + Hx_t \quad (5.6.2)$$

следует, что число элементов  $t$  в множестве  $S_1$  равно  $[K : H]$ . Так как множество  $S_1$  строго содержится в основном множестве, подгруппа  $K$  строго содержится в группе  $G$ . Далее, если  $S_i$  — любая область импримитивности, то существует подстановка из группы  $G$ , которая переводит элемент  $y_1$  в некоторый элемент из  $S_i$ , а значит отображает все множество  $S_1$  на все множество  $S_i$ . Поэтому  $S_1$  и  $S_i$  имеют равное число элементов. Более того, при подстановке  $Hx_i \rightarrow Hx_i g$  имеет место отображение  $Kx_i \rightarrow Kx_i g$ , откуда видно, что области импримитивности — это левые смежные классы по  $K$  в разложении (5.6.1), а потому их число равно  $[G : K]$ .

Обратно, пусть транзитивная группа  $G$  подстановок задана как группа подстановок  $Hx_i \rightarrow Hx_i g$  смежных классов по подгруппе  $H$ , фиксирующей элемент  $y_1$ , и пусть существует такая подгруппа  $K$ , что  $G \supset K \supset H$ . Тогда смежные классы по  $K$  состоят из смежных классов по  $H$  и являются областями импримитивности для группы  $G$ . Следовательно, группа  $G$  примитивна тогда и только тогда, когда подгруппа  $H$  максимальна.

Отметим некоторые элементарные факты, которые вытекают из определения примитивности и из доказанной теоремы.

Любая дважды транзитивная группа примитивна. Действительно, если  $S_1$  — некоторая собственная часть основного множества символов, на котором действует дважды транзитивная группа  $G$ , то существует подстановка, которая один из элементов  $S_1$  оставляет на месте, а другой элемент из  $S_1$  отображает в произвольный элемент, не принадлежащий  $S_1$ . Поэтому  $S_1$  не может быть областью импримитивности.

Другой факт заключается в том, что группа подстановок степени  $n$  (т. е. группа подстановок  $n$  символов) может иметь область импримитивности из  $t$  элементов только тогда, когда  $t$  делит  $n$ , так как по теореме 5.6.1  $n = [G : H]$  и  $t = [K : H]$ . Поэтому группа простого порядка, безусловно, примитивна. Далее, в  $p$ -группе любая подгруппа содержится в максимальной подгруппе индекса  $p$ , которая инвариантна (следствие 4.2.2). Поэтому группа подстановок, являющаяся  $p$ -группой, импримитивна, если только ее степень не равна  $p$ , причем в последнем случае она циклична порядка  $p$ .

**Теорема 5.6.2.** Пусть  $G$  — примитивная группа подстановок  $n$  символов,  $H$  — ее транзитивная подгруппа подстановок  $m$  символов, оставляющая остальные  $n - m$  символов на месте. Тогда

1) если  $H$  примитивна, то  $G(n - m + 1)$ -кратно транзитивна;

2) в любом случае группа  $G$  дважды транзитивна.

**Доказательство.** Группа  $H$  транзитивна на подмножестве из  $m$  символов. Любая подгруппа, сопряженная с  $H$ , транзитивна на некотором множестве из  $m$  символов, а так как группа  $G$  транзитивна, любой символ попадает по меньшей мере в одно из этих множеств. Если бы эти множества либо не пересекались, либо совпадали, то они были бы областями импримитивности для группы  $G$ . Следовательно, для подгруппы  $H$  существуют сопряженные с ней подгруппы, которые переставляют некоторые, но не все, из тех символов, которые переставляет подгруппа  $H$ . Пусть  $H'$  — одна из подгрупп, сопряженных с  $H$  и такая, что группы  $H$  и  $H'$  переставляют наибольшее возможное количество общих символов. Положим

$$\begin{aligned} H &: (a_1, \dots, a_r, c_1, \dots, c_s), \\ H' &: (b_1, \dots, b_r, c_1, \dots, c_s), \quad r + s = m. \end{aligned} \tag{5.6.3}$$

Эту запись мы понимаем так, что  $c_1, \dots, c_r$  — это символы, переставляемые как группой  $H$ , так и группой  $H'$ ,  $a_1, \dots, a_r$  — это остальные символы, переставляемые группой  $H$ ,  $b_1, \dots, b_r$  — это

остальные символы, переставляемые группой  $H'$ . Утверждается, что если группа  $H$  примитивна, то  $r = 1$ , а если  $H$  импримитивна и  $r > 1$ , то  $a_1, \dots, a_r$  составляют область импримитивности для  $H$ . Возьмем элемент  $h'$  из  $H'$ :

$$h' = \begin{pmatrix} b_1, \dots, b_u, b_{u+1}, \dots, b_r, c_1, \dots, c_{r-u}, c_{r-u+1}, \dots, c_s \\ b, \dots, b, c, \dots, c, b, \dots, b, c, \dots, c \end{pmatrix} \quad (5.6.4)$$

Здесь элементы нижней строки не уточняются, а просто указано, что  $u$  элементов вида  $b_i$  отображается в элементы  $b$ , некоторое число элементов  $b$  отображается в элементы  $c$ , некоторое число  $c$  — в  $b$  и  $c$  — в  $c$ . При этом следует отметить, что число  $r - u$  элементов вида  $b_i$ , отображаемых в элементы вида  $c_j$ , должно быть равно числу элементов вида  $c_j$ , отображаемых в элементы вида  $b_i$ , так как в нижней строчке подстановки  $h'$  должно быть ровно  $r$  элементов вида  $b_i$ .

Отсюда следует, что подгруппа  $h'^{-1}Hh'$  переставляет  $r$  элементов вида  $a_k$ ,  $r - u$  элементов вида  $b_i$  и  $(s - r + u)$  элементов вида  $c_j$ , а поэтому эта подгруппа переставляет всего  $s + u$  элементов таких, которые переставляются также подгруппой  $H$ . Таким образом, если  $r > 1$  и подгруппа  $H'$  примитивна, мы можем найти элемент  $h'$ , переводящий некоторые, но не все, элементы вида  $b_i$  в элементы того же вида, откуда  $1 \leq u < r$ ; поэтому число  $s + u$  указанных выше элементов больше, чем  $s$ , но меньше, чем  $r + s = m$ . Во всяком случае мы получаем, что  $r = 1$ , если подгруппа  $H$  примитивна, а если  $r = 1$ , то, независимо от того, примитивна подгруппа  $H$  или нет, подгруппа  $H \cup H'$  дважды транзитивна на  $m + 1$  символах, а потому примитивна. Теперь мы можем повторить проделанный цикл рассуждений, но так, чтобы роль подгруппы  $H$  играла подгруппа  $H \cup H'$ . Тогда у нас получится еще большая подгруппа, уже трижды транзитивная на  $m + 2$  символах и т. д. В конце концов мы получим всю группу  $G$ , которая окажется  $(n - m + 1)$ -кратно транзитивной.

В случае, когда группа  $H$  импримитивна, проведенное рассуждение неприменимо. Но мы можем увеличивать число  $s$  символов, сдвигаемых одновременно подгруппами  $H$  и  $H'$ , до тех пор, пока символы  $b_1, \dots, b_r$  не составят область импримитивности для  $H'$ , а  $a_1, a_2, \dots, a_r$  — область импримитивности для  $H$ . Кроме того,  $H \cup H'$  — транзитивная группа на  $s + 2r = m + r$  символах. Таким образом, если  $m$  меньше, чем  $n/2$ , то  $m + r$  будет меньше, чем  $n$ . Мы можем продолжить построение транзитивных подгрупп над все возрастающим числом символов, пока не получится транзитивная подгруппа  $H$  над  $m$  символами, причем  $m$  больше  $n/2$ , но меньше  $n$ . Тогда любая подгруппа  $H'$ , сопряженная с  $H$ , переставляет несколько тех же символов, что и подгруппа  $H$ . Предположим, что подгруппа  $H$

транзитивна на наибольшем возможном числе символов, не превосходящем  $n$ . Если  $s + 2r = n$  и  $r = 1$ , то подгруппа  $H$  транзитивна на  $n - 1$  символах, а потому группа  $G$  дважды транзитивна. Если это не имеет места, мы построим группу  $H$ , для которой  $s + 2r = n$  и  $r \neq 1$ . В этом случае символы вида  $a_k, b_i$  и  $c_j$  составляют все множество, на котором действует группа  $G$ . Но так как группа  $G$  примитивна, то существует такой элемент  $g$  группы  $G$ , который отображает символ  $b_1$  в некоторый определенный символ  $b_i$ , но не все символы такого вида — в символы того же вида, а поэтому он отображает по меньшей мере один элемент вида  $a_k$  или  $c_j$  в элемент вида  $b_i$ . Тогда обе подгруппы  $H$  и  $g^{-1}Hg$  оставляют на месте указанный элемент  $b_i$ , и их объединение есть транзитивная группа над большим числом символов, чем подгруппа  $H$ .

Итак, мы в конце концов получим транзитивную подгруппу на  $n - 1$  символах, и поэтому группа  $G$  дважды транзитивна.

Второй из двух рассмотренных в доказательстве случаев действительно встречается. Это показывает пример 4 в главе 1, где рассматривается транзитивная группа на семи буквах, которая, следовательно, примитивна. Она обладает транзитивной подгруппой на четырех буквах  $C, E, F, G$  и дважды, но не трижды, транзитивна.

## 5.7. Кратно-транзитивные группы

Симметрическая группа степени  $n$ , очевидно,  $n$ -кратно транзитивна, а знакопеременная группа  $A_n$  (как мы уже заметили в § 5.4)  $(n - 2)$ -кратно транзитивна. Мы исключим эти группы из дальнейших рассуждений о кратной транзитивности групп. Существует бесконечно много трижды транзитивных групп. Но, кроме знакопеременной и симметрической групп, известны только четыре группы, которые четырежды транзитивны. Это группы Матье (Mathieu) степеней 11, 12, 23 и 24, причем группы степеней 12 и 24 пятикратно транзитивны и содержат в качестве подгрупп, оставляющих на месте одну букву, группы степеней 11 и 23 соответственно. Эти несколько таинственные группы были предметом серьезных исследований, но осталось неизвестным, являются ли эти группы в самом деле исключением или же они принадлежат некоторому бесконечному семейству четырежды транзитивных групп.

Теорема 5.7.1, доказанная Миллером [1], дает оценку кратности транзитивности для групп подстановок степени  $n$ . Эта теорема вместе с „постулатом Бертрана“ (Bertrand) устанавливает, что для  $n > 12$  группа подстановок степени  $n$  не может быть  $t$ -кратно транзитивной, если  $t \geq 3\sqrt{n} - 2$ . Постулат Бертрана (правильно доказанный Чебышевым в 1850 году) утверждает, что

для любого действительного числа  $x \geq 7$  существует простое число  $p$  в интервале  $x/2 < p \leq x - 2$ . Теорема Миллера дает значительно лучшую оценку для многих частных значений  $n$ . Известны еще лучшие оценки, но из-за сложности доказательств мы их опускаем<sup>1)</sup>.

**Теорема 5.7.1.** *Пусть  $G$  —  $t$ -кратно транзитивная группа степени  $n$ . Пусть  $H$  — подгруппа, оставляющая на месте  $t$  букв, и  $P$  — силовская  $p$ -подгруппа группы  $H$ , которая оставляет на месте  $w \geq t$  букв. Тогда нормализатор подгруппы  $P$  в группе  $G$  является  $t$ -кратно транзитивной группой на множестве из  $w$  букв, инвариантных при  $P$ <sup>2)</sup>.*

**Доказательство.** Пусть  $a_1, \dots, a_t$  и  $b_1, \dots, b_t$  — два упорядоченных множества, в каждом из которых по  $t$  букв, причем оба являются подмножествами множества из  $w$  букв, инвариантных при  $P$ . Тогда, так как группа  $G$   $t$ -кратно транзитивна, существует элемент  $x$  из  $G$ , переводящий  $a_i$  в  $b_i$  при  $i = 1, \dots, t$ . Тогда  $x^{-1}Px$  оставляет на месте  $b_1, \dots, b_t$ , а, значит, подгруппы  $P$  и  $x^{-1}Px$  являются силовскими подгруппами группы  $G$ , оставляющими на месте  $b_1, \dots, b_t$ . Согласно второй теореме Сильсона, эти подгруппы сопряжены в группе, для которой буквы  $b_1, \dots, b_t$  инвариантны. Поэтому для некоторой подстановки  $y$ , оставляющей на месте  $b_1, \dots, b_t$ , имеет место равенство  $y^{-1}(x^{-1}Px)y = P$ . Если  $z = xy$ , то  $z^{-1}Pz = P$ , причем подстановка  $z$  переводит элементы  $a_1, \dots, a_t$  в элементы  $b_1, \dots, b_t$ . Значит, в нормализаторе подгруппы  $P$  существует элемент, отображающий любое упорядоченное подмножество, состоящее из  $t$  букв множества из  $w$  букв, оставляемых на месте подгруппой  $P$ , на любое другое упорядоченное подмножество того же самого множества из  $w$  букв. Таким образом, нормализатор подгруппы  $P$  в группе  $G$   $t$ -кратно транзитивен на множестве из  $w$  букв, инвариантных при  $P$ ; теорема доказана.

**Теорема 5.7.2.** *Для целого числа  $n$  вида  $n = kp + r$ , где  $p$  — простое число,  $p > k$ ,  $r > k$ , группа подстановок степени  $n$ , за исключением случая  $k = 1$  и  $r = 2$ , не может быть  $(r+1)$ -кратно транзитивной, если только она не совпадает с группами  $S_n$  или  $A_n$ .*

**Доказательство.** Предположим, что группа  $G$  степени  $n$   $(r+1)$ -кратно транзитивна. Подгруппа  $H$ , оставляющая на месте первые  $r$  букв  $1, 2, \dots, r$ , транзитивна тогда на остальных  $kp$  буквах. Поэтому порядок группы  $H$  делится на  $p$ , а сама она

<sup>1)</sup> Паркер получил оценку для  $t$  порядка величины  $\sqrt[3]{n}$  для подходящих значений  $n$ . Наилучшую оценку  $t < 3 \log n$  получил Виландт [1].

<sup>2)</sup> В дальнейшем мы будем употреблять выражение „символ  $a$  инвариантен относительно  $H$ “ (где  $H$  — множество подстановок) вместо „символ  $a$  остается на месте при всех подстановках из  $H$ “. — Прим. перев.

содержит силовскую  $p$ -подгруппу  $P$ . Подгруппа группы  $H$ , оставляющая одну из рассматриваемых  $k p$  букв на месте, имеет индекс  $k p$  в группе  $H$ , а поэтому ее порядок не делится на высшую степень числа  $p$ , которая делит порядок группы  $H$ . Следовательно, подгруппа  $P$  должна переставлять каждый из  $k p$  символов, на которых подгруппа  $H$  транзитивна. Далее, так как  $k p < p^2$ , подгруппа  $P$  не содержит транзитивной подгруппы степени  $p^2$ . Так как число символов в каждой области транзитивности группы  $P$  должно делить порядок  $P$ , то группа  $P$ , рассматриваемая как группа подстановок  $k p$  символов, обладает в точности  $k$  областями транзитивности, по  $p$  символов в каждой. (Мы уже исключили случай, когда какая-либо область транзитивности состоит из одного единственного элемента.) В каждой из этих областей транзитивности группа  $P$  действует как циклическая группа порядка  $p$ . Поэтому  $P$  есть подпрямое произведение  $k$  циклических групп порядка и степени  $p$  каждая. Значит, любой элемент из  $P$  имеет порядок  $p$ ; кроме того,  $P$  — абелева группа. В остальном же для нас несущественно, как именно образовано подпрямое произведение  $P$ .

Пусть  $N$  — нормализатор подгруппы  $P$  в  $G$ . По теореме 5.7.1 нормализатор  $N$  действует как симметрическая группа  $S_r$  на первых  $r$  буквах из основного множества букв  $G$ . Рассмотрим сперва случай, когда  $r \geqslant 5$ . Пусть  $N_1$  — подгруппа группы  $N$ , являющаяся знакопеременной группой  $A_r$  тех же  $r$  букв. По теореме 5.4.3 группа  $A_r$  простая, составного порядка  $r!/2$  и, так как  $r \geqslant 4$ , неабелева. Пусть  $T_1, \dots, T_k$  — области транзитивности (в каждой из которых по  $p$  элементов) для группы  $P$ . Мы получим гомоморфный образ группы  $N_1$ , если будем комбинировать подстановки первых  $r$  букв с подстановками на областях транзитивности  $T_i$ , переставляемыми между собой элементами из  $N_1$ . Этот образ является подпрямым произведением группы  $A_r$ , действующей на первых  $r$  буквах, и группы  $B$ , некоторым образом переставляющей  $k$  областей транзитивности  $T_i$  между собой. Но группа подстановок  $k$  символов не может иметь порядок, превосходящий  $k!$ , и поэтому вследствие неравенства  $k! < r!/2$  она не может иметь фактор-группу, изоморфную простой группе  $A_r$ ; таким образом, единственной фактор-группой этой группы, изоморфной некоторой фактор-группе группы  $A_r$ , является единичная группа. Следовательно, это подпрямое произведение, в силу результата § 5.5, оказывается прямым произведением групп  $A_r$  и  $B$ . Полным прообразом в группе  $N_1$  подгруппы этого прямого произведения, порожденной подгруппой  $A_r$ , с одной стороны, и единицей группы  $B$  — с другой, является подгруппа  $N_2$ , которая на первых  $r$  буквах действует как  $A_r$ , а каждую область транзитивности  $T_i$  отображает на себя. Мы должны прервать

исследование группы  $N_2$ , чтобы рассмотреть в группе подстановок  $p$  букв  $x_1, \dots, x_p$  нормализатор циклической группы, порожденной подстановкой  $a = (x_1, \dots, x_p)$  этих букв. Учитывая, что  $a^p = 1$ ,  $b^{-1}ab = a^l$  и  $c^{-1}ac = a^j$ , мы видим, что и  $bc$ , и  $cb$  трансформируют подстановку  $a$  в подстановку  $a^{ij}$ . Таким образом, автоморфизмы циклической группы, индуцированные преобразованиями из нормализатора этой группы, сами образуют абелеву группу. (Мы увидим в следующей главе, что автоморфизмы циклической группы порядка  $p$  образуют циклическую группу порядка  $p - 1$ .)

Пусть теперь  $u$  — некоторая подстановка букв  $x_1, \dots, x_p$ , перестановочная с  $a$ . Умножив  $u$  на подходящую степень  $a^i$ , получим подстановку  $v = ua^i$ , перестановочную с  $a$  и оставляющую на месте букву  $x_1$ . Но из этих двух свойств подстановки  $v$  легко вывести, что  $v$  оставляет на месте  $x_2, \dots, x_p$  и, значит,  $v = 1$ , откуда  $u = a^{-i}$ . Отсюда вытекает, что группа  $N_2$  на каждой из  $k$  областей транзитивности  $T_i$  (состоящей из  $p$  букв) группы  $P$  обладает инвариантной подгруппой порядка  $p$ , состоящей из степеней некоторой подстановки  $p$  букв, и фактор-группой по этой группе, состоящей из элементов, индуцирующих различные автоморфизмы на группе порядка  $p$ . Эта фактор-группа абелева. Таким образом, любая фактор-группа или абелева, или имеет абелеву фактор-группу. Поэтому единственной фактор-группой, изоморфной фактор-группе группы  $A_r$ , является единичная группа. Таким образом, оставив временно действия над  $T_2, T_3, \dots, T_k$  вне рассмотрения и применяя результат из § 5.5 к первым  $r$  буквам и области  $T_1$ , мы получаем, что группа  $N_2$  содержит подгруппу, которая на первых  $r$  буквах действует, как  $A_r$ , а на области  $T_1$  — тождественно. Эта подгруппа  $N_3$  в свою очередь обладает подгруппой  $N_4$ , которая на первых  $r$  буквах действует как  $A_r$ , а на областях  $T_1$  и  $T_2$  — тождественно.

Повторяя это рассуждение несколько раз, мы получим подгруппу, которая на первых  $r$  буквах действует, как группа  $A_r$ , а на всех других — тождественно. Но группа  $A_r$  содержит цикл  $(a, b, c)$  длины 3, и поскольку группа  $G$ , по предположению, самое меньшее пятикратно транзитивна на всех  $n$  буквах ( $r \geq 5$ ), этот цикл может быть трансформирован в любой другой цикл длины 3 группы  $G$ . Согласно лемме 5.4.1, все циклы длины 3 порождают группу  $A_n$ . Итак, группа  $G$  содержит  $A_n$ . Следовательно,  $G = A_n$  или  $G = S_n$ .

Приведенные рассуждения существенно используют предположение  $r \geq 5$ . Остается рассмотреть случаи  $r = 3$ ,  $k = 1$  или 2;  $r = 4$ ,  $k = 1, 2$  или 3. Рассмотрим сначала случай, когда группа  $P$  циклическая и порождается некоторым элементом  $a$ , причем  $k = 1$ .

или 2. Как мы отмечали выше, если  $u = (12)(3)\dots$  и  $v = (1)(23)\dots$  — элементы нормализатора  $N$  группы  $P$  (который оказывается симметрической группой первых трех или четырех букв, оставляемых на месте группой  $P$ ), то, так как группа  $P$  циклична, элементы  $uv$  и  $vu$  трансформируют подстановку  $a$  в одну и ту же ее степень. Поэтому подстановка  $u^{-1}v^{-1}uv = (1, 2, 3)\dots$  перестановочна с  $a$ . Этот элемент  $w = u^{-1}v^{-1}uv$  либо отображает области транзитивности  $T_1$  и  $T_2$  друг на друга, либо оставляет их на месте. В обоих случаях элемент  $w^2 = (1, 3, 2)\dots$  оставляет в целом на месте обе эти области. Порядок этого элемента делится на 3, а поэтому некоторая его степень имеет порядок  $3^s$ ; первые три буквы она переставляет циклично, оставляя в целом на месте области транзитивности; кроме того, эта степень перестановочна с элементом  $a$ . Но для каждого цикла подстановки  $a$ , если он не является тождественной подстановкой, единственным перестановочным с ним элементом является его степень порядка  $p$ . Таким образом, если  $p \neq 3$ , элемент порядка  $3^s$ , перестановочный с  $a$ , есть цикл  $(1, 2, 3)$  или  $(1, 3, 2)$  первых трех букв и тождественная подстановка — остальных. Тогда группа  $G$  содержит цикл длины 3 и к тому же трижды транзитивна, а значит, совпадает либо с  $A_n$ , либо с  $S_n$ . Мы исключили случай  $p = 3$  при  $k = 1$  или 2,  $r = 3$  или 4 (соответственно  $n = 6, 7, 9, 10$ ). Если  $p = 3$ ,  $k = 1$ , группа  $P$  сама порождена циклом длины 3, и заключение проходит. Этим рассуждением покрывается случай  $n = 6, 7$ .

Случай  $n = 9$  и  $n = 10$  должны быть рассмотрены отдельно. Все возможности, когда  $k = 1$ , уже рассмотрены, так как в этих случаях группа  $P$ , конечно, циклична. Если теперь  $k = 2$  и группа  $P$  нециклична, то  $P$  есть прямое произведение двух циклов длины  $p$ . Тогда применяем теорему 5.6.2, где  $G$  — примитивная группа,  $H$  — циклическая группа порядка  $p$  и, значит, примитивная. Получаем, что группа  $G$   $(p+4)$ - или  $(p+5)$ -кратно транзитивна. Применяя уже изложенные рассуждения для  $r = p+3$  или  $r = p+4$  и  $k = 1$ , получаем, что группа  $G$  совпадает с  $A_n$  или  $S_n$ .

Рассмотрим, наконец, случаи, когда  $k = 3, r = 4$ . Прежде всего, если группа  $P$  циклична, можно доказать, как и прежде, что существуют элементы  $(1, 2, 3)(4)\dots, (1)(2, 3, 4)\dots$ , которые перестановочны с образующим элементом  $a$  группы  $P$ , причем в действительности все восемь возможных циклов длины 3 первых 4 букв обладают этим свойством. Но они могут переставлять три области транзитивности подстановки  $a$  циклически одним из способов:  $(T_1, T_2, T_3)$  или  $(T_1, T_3, T_2)$ , и по меньшей мере две из восьми подстановок должны переставлять области  $T_i$  одинаковым образом. Перемножая эти подстановки, мы получаем элемент вида  $(1, 2, 3)(4)\dots$  или  $(1, 2)(3, 4)\dots$ , который области  $T_1, T_2, T_3$  оставляет в целом на месте. Здесь число  $p$  не менее 5,

и из элементов одного из этих двух видов, перестановочных с  $a$  и переводящих циклы подстановки  $a$  в себя, можно получить элемент такого же вида, оставляющий на месте  $3p$  тех букв, на которые действует подстановка  $a$ . Таким образом, в группе  $G$  имеется либо цикл  $(1, 2, 3)$  длины 3, либо подстановка  $(1, 2)(3, 4)$ , а из четырёхкратной транзитивности следует, что имеются также подстановки  $(1, 2)(3, 5)$  и  $(3, 4, 5)$ . Поэтому группа  $G$  содержит  $A_n$ , т. е. равна ей или совпадает с  $S_n$ . С другой стороны, если  $P$  содержит отдельный цикл из  $p$  символов, то можно применить теорему 5.6.2, в силу которой группа  $G(2p+4)$ -или  $(2p+5)$ -кратно транзитивна, следовательно, опять группа  $G$  есть или  $A_n$ , или  $S_n$ .

В последнем случае, который мы должны рассмотреть, группа  $P$  нециклична и не содержит  $p$ -цикл. Тогда группа  $P$  должна быть порядка  $p^2$ . Мы можем выбрать базис для группы  $P$ , состоящий из двух элементов:  $a = (x_1, x_2, \dots, x_p)(y_1, y_2, \dots, y_p)$  и  $b = (y_1, y_2, \dots, y_p)(z_1, z_2, \dots, z_p)$ , где  $a$  и  $b$  индуцируют один и тот же цикл на элементах  $y_1, y_2, \dots, y_p$ . В этом случае элемент  $ab^{-1}$  и его степени суть единственные элементы из  $P$ , оставляющие на месте множество  $T_2$  элементов  $y_1, y_2, \dots, y_p$ . Теперь можно выбрать элемент вида  $(1, 2, 3, 4) \dots$ , принадлежащий нормализатору группы  $P$ , так, чтобы он или оставлял на месте все три подмножества, или переставлял два из них и оставлял на месте третье. Тогда квадрат его  $u = (1, 3)(2, 4) \dots$  оставляет на месте все три области транзитивности. Следовательно, элемент  $u$  трансформирует каждый из элементов  $a, b$  и  $ab^{-1}$  в некоторую его степень и тем самым возводит  $a$  и  $b$  в одинаковую (скажем, в  $i$ -ю) степень и трансформирует любой элемент из  $P$  в его  $i$ -ю степень. Такой автоморфизм должен быть перестановочным с любым другим автоморфизмом группы  $P$  и, в частности, с автоморфизмом, индуцированным подстановкой  $w = (1)(2)(3, 4) \dots$ . Поэтому элемент  $v = w^{-1}uw = (1, 2)(3, 4) \dots$  также трансформирует любой элемент из  $P$  в его  $i$ -ю степень, а потому, естественно, оставляет на месте указанные выше области транзитивности. Но теперь элемент  $uv^{-1} = (1, 4)(2, 3) \dots$  перестановчен с любым элементом из  $P$ , оставляющим на месте рассматриваемые области транзитивности. Отсюда вытекает существование подстановки  $(1, 4)(2, 3)$ , принадлежащей группе  $G$ , а так как  $G$  четырежды транзитивна на множестве из более чем четырёх букв, то опять группа  $G$  равна или  $A_n$ , или  $S_n$ .

## 5.8. О теореме Жордана

В 1872 году Жордан [2] доказал, что конечная четырёжды транзитивная группа, в которой любые четыре буквы инвариантны только относительно единичной подгруппы, должна быть одной из следующих групп: симметрической группой четвертой или пятой

степени, знакопеременной группой шестой степени или группой Матье одиннадцатой степени.

Здесь мы обобщим эту теорему Жордана в двух направлениях. Во-первых, не будем предполагать конечность степени группы подстановок; во-вторых, вместо предположения, что 4 буквы инвариантны только относительно единичной подгруппы, будем предполагать только, что они обладают этим свойством относительно конечной группы нечетного порядка. Заключение отличается от теоремы Жордана лишь тем, что рассматриваемая группа может быть еще знакопеременной группой седьмой степени. Наша теорема гласит.

**Теорема 5.8.1.** *Четырежды транзитивная группа  $G$  конечной или бесконечной степени, в которой подгруппа, относительно которой инвариантны 4 буквы, конечна и нечетного порядка, должна быть одной из следующих групп:  $S_4$ ,  $S_5$ ,  $A_6$ ,  $A_7$  или группой Матье одиннадцатой степени.*

Случай 1. Группа  $G$  не более чем седьмой степени.

Четырежды транзитивная группа на 4 или 5 символах должна быть симметрической группой. На шести символах ее порядок должен быть равным по меньшей мере  $6 \cdot 5 \cdot 4 \cdot 3$ , т. е. она оказывается группой  $A_6$  или  $S_6$ . На семи символах ее индекс в группе  $S_7$  равен самое большое 6. Так как группа  $S_7$  не имеет подгрупп индексов 3 и 6, единственными возможными группами опять оказывается  $A_7$  или  $S_7$ . И в группе  $S_6$ , и в группе  $S_7$  существуют элементы порядка 2, оставляющие на месте по меньшей мере 4 символа, и поэтому эти группы не удовлетворяют условиям теоремы.

Рассмотрению случая, когда степень группы  $G$  более 7, мы предпошли 2 леммы.

**Лемма 5.8.1.** *Элементы  $a$  и  $b$  некоторой группы, удовлетворяющие отношениям*

$$a^2 = 1, \quad b^2 = 1, \quad (ab)^s = 1,$$

*порождают группу дизэдра порядка  $2s$ . Если число  $s = 2t - 1$  нечетно, то некоторая степень элемента  $y = ab$  трансформирует  $a$  в  $b$ . Если число  $s = 2r$  четно, то элементы  $a$  и  $b$  перестановочны с элементом  $y^r$ .*

*Доказательство.* Для  $y = ab$  имеем

$$a^2 = 1, \quad y^s = 1, \quad b = ay = y^{-1}a.$$

Если  $s = 2t - 1$ , то

$$y^{-t}ay^t = ay^{2t} = b.$$

Если  $s = 2r$ , то

$$ay^r = y^{-r}a = y^r a.$$

Начиная с этого места, мы будем обозначать буквой  $G$  (как в теореме 5.8.1) четырежды транзитивную группу степени более

чем 7, а буквой  $H$  — подгруппу нечетного порядка  $m$ , относительно которой инвариантны 4 символа.

**Лемма 5.8.2.** *Пусть группа  $G$  содержит элементы порядка 2 и все они сопряжены.*

*Тогда 1) или каждый элемент порядка 2 оставляет на месте 2 символа, 2) или каждый элемент порядка 2 оставляет на месте 3 символа.*

*Доказательство.* Так как группа  $G$  четырежды транзитивна, она содержит элемент вида

$$g = (12)(34)\dots$$

Ясно, что подстановка  $g^2$  оставляет на месте элементы 1, 2, 3, 4; следовательно, она принадлежит подгруппе  $H$  и имеет поэтому конечный нечетный порядок  $m_1$ . Тогда  $x = g^{m_1} = (12)(34)\dots$ , причем  $x^2 = 1$ . Так как порядок подгруппы  $H$  нечетный, то любой элемент  $u$  порядка 2 оставляет на месте, самое большое, 3 символа и тем самым перемещает не менее 4 символов. Ко всякому элементу вида  $u = (ab)(cd)\dots$  имеется сопряженный элемент вида

$$v = w^{-1}uw = (12)(34)\dots$$

Далее  $v = x$  или подстановка  $vx$  оставляет на месте 4 символа и имеет нечетный порядок; отсюда, согласно лемме 5.8.1, элементы  $v$  и  $x$  сопряжены. Таким образом, все элементы порядка 2 сопряжены. С другой стороны, в группе  $G$  существует элемент  $z$  вида  $z = (1)(2)(34)\dots$ , причем либо сам элемент  $z$ , либо некоторая его нечетная степень будет элементом порядка 2, не перемещающим хотя бы два символа. Следовательно, любой элемент порядка 2 оставляет на месте или 2, или 3 символа, так как они оставляют на месте не менее двух символов, но не более трех.

**Случай 2.** *Группа  $G$  степени более чем 7.*

Пусть  $a_1 = (1)(2)(34)\dots$  и  $b = (12)(34)\dots$  — два элемента порядка 2. Тогда элемент  $f = a_1b = (12)(3)(4)\dots$  — четного порядка, а  $f^2$  — нечетного порядка  $m_1$ . Следовательно, элемент  $f^{m_1} = a_3$  порядка 2; согласно лемме 5.8.1,  $a_3$  перестановочен с  $a_1$ . Положив еще  $a_2 = a_1a_3$ , мы теперь видим, что в группе  $G$  содержатся перестановочные между собой элементы порядка 2:

$$\begin{aligned} a_1 &= (1)(2)(34)\dots, \\ a_2 &= (12)(34)\dots, \\ a_3 &= (12)(3)(4)\dots \end{aligned} \tag{5.8.1}$$

Так как  $a_2$  — элемент порядка 2, то он оставляет на месте или два символа 5 и 6, или три символа 5, 6, 7. Поскольку подстановка  $a_1$  перестановочна с  $a_2$ , она переводит множество

этих символов в себя. Но подстановка  $a_1$  оставляет на месте символы 1, 2 и еще не более одного символа. Поэтому возможны два случая:

$$\begin{aligned} a_1 &= (1)(2)(34)(56)\dots, & a_1 &= (1)(2)(34)(56)(7)\dots, \\ a_2 &= (12)(34)(5)(6)\dots, \text{ или } a_2 = (12)(34)(5)(6)(7)\dots, & (5.8.2) \\ a_3 &= (12)(3)(4)(56)\dots; & a_3 &= (12)(3)(4)(56)(7)\dots. \end{aligned}$$

Первый случай имеет место, когда все элементы порядка 2 оставляют на месте два символа, второй — когда они оставляют на месте три символа. Элементы  $a_1$ ,  $a_2$ ,  $a_3$ , только что выписанные, и тождественная подстановка образуют четверную группу Клейна, которую мы обозначим через  $V$ . Остальные символы распадаются на области транзитивности для группы  $V$  по 4 символа в каждой:

$$\begin{aligned} a_1 &= (1)(2)(34)(56)(7)(hi)(jk)\dots, \\ a_2 &= (12)(34)(5)(6)(7)(hj)(ik)\dots, \\ a_3 &= (12)(3)(4)(56)(7)(hk)(ij)\dots. \end{aligned} \quad (5.8.3)$$

Здесь подразумевается, что символ 7 не обязательно присутствует в записи.

Порядок подгруппы  $K$ , переводящей множество символов  $h$ ,  $i$ ,  $j$ ,  $k$  в себя, равен  $24m$ , где  $m$  — порядок инвариантной подгруппы  $H = H(h, i, j, k)$  группы  $K$ , для которой эти символы инвариантны. Существует подгруппа  $U$ ,  $K \supset U \supset H$ , которая представляет символы  $h$ ,  $i$ ;  $j$ ,  $k$  следующим образом:

$$\begin{aligned} &(h) \\ &(hi)(jk) \\ &(hj)(ik) \\ &(hk)(ij) \\ &(hjik) \\ &(hki) \\ &(hi)(j)(k) \\ &(h)(i)(jk) \end{aligned} \quad (5.8.4)$$

Порядок подгруппы  $U$  равен  $8m$ , и поэтому силовская 2-подгруппа группы  $U$  имеет порядок 8. Подстановки, переставляющие элементы  $h$ ,  $i$ ,  $j$ ,  $k$  между собой каким-то определенным образом, составляют смежный класс по подгруппе  $H$  в  $U$ . Так как подгруппа  $H$  инвариантна в группе  $U$ , подгруппа группы  $U$  порядка 8 содержит только по одной подстановке из каждого смежного класса; она изоморфна фактор-группе  $U/H$  и, следовательно, точно представлена этими подстановками символов  $h$ ,  $i$ ,  $j$ ,  $k$ .

Группа  $V$  содержится в силовской подгруппе порядка 8 группы  $U$ . Поэтому получаем подстановки

$$\begin{aligned} a_1 &= (1)(2)(34)(56)(7)(hi)(jk)\dots, \\ a_2 &= (12)(34)(5)(6)(7)(hj)(lk)\dots, \\ a_3 &= (12)(3)(4)(56)(7)(hk)(ij)\dots, \\ u &= (1)(2)(3546)(7)(hjlk)\dots, \\ a_1u &= (1)(2)(3645)(7)(hki)\dots, \\ a_2u &= (12)(36)(45)(7)(hi)(j)(k)\dots, \\ a_3u &= (12)(35)(46)(7)(h)(i)(jk)\dots \end{aligned} \quad (5.8.5)$$

или же подстановки, получаемые из подстановок (5.8.5) заменой 5 на 6 и наоборот. Действительно, последние четыре подстановки переставляют символы 1, ..., 7 согласно следующим отношениям:

$$u^2 = a_1, \quad u^{-1}a_2u = a_3, \quad (a_2u)^2 = 1.$$

Элемент  $u$  принадлежит нормализатору группы  $V$ , а, следовательно, из символов, инвариантных относительно группы  $V$ , он оставляет на месте только символ 7 (если этот символ вообще встречается). Кроме того, элемент  $u$  должен отображать символы, инвариантные при  $a_3$ , в символы, инвариантные при  $a_2$ . Отсюда

$$u = \begin{pmatrix} 3, 4, \dots \\ 5, 6, \dots \end{pmatrix} \quad \text{или} \quad u = \begin{pmatrix} 3, 4, \dots \\ 6, 5, \dots \end{pmatrix},$$

но так как  $u^2 = a_1$ , то

$$u = (3546)\dots \quad \text{или} \quad u = (3645)\dots$$

Наконец, подстановка  $u$  должна оставлять символы 1 и 2 на месте или переставлять их между собой. Но если  $u$  переставляет 1 и 2, то элемент  $a_2u$  имеет порядок 2 и оставляет на месте символы 1, 2,  $j$ ,  $k$ . Таким образом, возможно только  $u = (1)(2)(3546)\dots$  или  $u = (1)(2)(3645)\dots$ . Отсюда следует и вид остальных трех подстановок.

Каждая другая область транзитивности группы  $V$ , подобная множеству символов  $h, i, j, k$ , дает некоторую группу  $S$ , аналогичную группе (5.8.5). В каждой из таких групп элементы вида  $(12)(36)(45)\dots$  и  $(12)(35)(46)\dots$  оставляют на месте два символа в соответствующей области транзитивности. Так как элемент порядка 2 не может оставлять на месте четыре символа, то каждой такой области транзитивности соответствует свой элемент, который переставляет первые шесть символов так же, как подстановка  $(12)(36)(45)$ . Но существует не более  $m$  подстановок, переставляющих первые шесть букв указанным образом. Сле-

довательно, если существует  $t$  таких областей транзитивности, то  $t$  — конечно,  $t \leq m$ , и группа  $G$  действует на множестве из  $n = 4t + 6$  или  $4t + 7$  символов. Если  $n = 10$  или  $11$ , то  $t = 1$ .

Четырежды транзитивной группы степени 10 не существует (кроме  $A_{10}$  и  $S_{10}$ , разумеется), так как нормализатор цикла длины 7, согласно теореме 5.7.2, действует как группа  $S_3$  на остающихся трех символах. Поэтому этот нормализатор, являющийся подпрямым произведением группы  $S_3$  и нормализатора цикла длины 7, содержит произведение цикла длины 3 и единичной подстановки. Следовательно, группа  $G$  содержит цикл длины 3, а так как она четырежды транзитивна, то содержит все циклы длины 3. Но тогда группа  $G$  содержит  $A_{10}$ .

Порядок группы  $G$  степени 11 равен  $11 \cdot 10 \cdot 9 \cdot 8m$ . Даже без предположения нечетности числа  $m$  рассмотрение нормализаторов силовских подгрупп, относительно которых инвариантны четыре символа, показывает, что  $m = 1$ . Группа порядка 8, относительно которой инвариантны три символа, содержит только один элемент порядка 2, а потому она или циклична, или изоморфна группе кватернионов. Циклическая группа имеет только 4 автоморфизма. Ее нормализатор не может быть трижды транзитивен на остающихся трех символах, так как в этом случае группа  $G$  содержала бы цикл длины 3. Следовательно, подгруппа, для которой три символа инвариантны, должна быть группой кватернионов  $Q$ . Итак, группа  $G$  является транзитивным расширением группы  $Q$ , и методом Холиоке [1] мы можем легко построить из группы  $Q$  не только четырежды транзитивную группу Матье одиннадцатой степени, но и пятикратно транзитивную группу двенадцатой степени.

Чтобы завершить доказательство нашей теоремы, мы покажем, что неравенство  $t > 1$  противоречит нечетности порядка подгруппы  $H$ . Пусть символы  $w, x, y, z$  составляют область транзитивности группы  $V$ , отличную от  $h, i, j, k$ . Из (5.8.5) имеем подстановку

$$a_2u = (12)(36)(45)(7)(hi)(j)(k) \dots$$

и отличную от нее подстановку

$$a_2u' = (12)(36)(45)(7)(wx)(y)(z) \dots$$

Каждая из этих подстановок перестановочна с  $a_1$  и трансформирует  $a_2$  в  $a_3$ , а  $a_3$  в  $a_2$ . Их произведение  $q$  оставляет на месте первые шесть (или семь) символов, а поэтому имеет нечетный порядок. Кроме того, элемент  $q$  принадлежит централизатору группы  $V$ . Согласно лемме 5.8.1, некоторая степень элемента  $q$  трансформирует  $a_2u$  в  $a_2u'$  и, следовательно, переводит символы  $j$  и  $k$ , инвариантные при  $a_2u$ , в символы  $y, z$ , инвариантные при  $a_2u'$ .

Будучи перестановочным с каждым элементом группы  $V$ , этот элемент должен отображать всю область транзитивности  $h, i, j, k$  на область транзитивности  $w, x, y, z$ . Следовательно, существует подгруппа  $C$  в  $G$ , которая оставляет на месте первые шесть (или семь) символов, содержащаяся в централизаторе группы  $V$  и к тому же транзитивна на множестве, состоящем из  $t$  областей транзитивности группы  $V$ . Элемент подгруппы  $C$ , переводящий одну из областей транзитивности группы  $V$  в себя, будучи элементом нечетного порядка, должен оставлять на месте все четыре символа. Таким образом, областями транзитивности группы  $C$  являются множества  $(1), (2), (3), (4), (5), (6), (7), T_h, T_i, T_j, T_k$ , где последние четыре множества содержат по  $t$  элементов; при этом символы  $h, i, j, k$  находятся в различных областях транзитивности группы  $C$ .

Пусть теперь  $p$  — простое число, делящее  $t$ . (Здесь мы используем предположение, что  $t > 1$ .) Пусть  $P$  — соответствующая силовская  $p$ -подгруппа группы  $C$ . Тогда относительно группы  $P$  неинвариантны все  $4t$  символов, переставляемых группой  $C$ , так как подгруппа группы  $C$ , оставляющая на месте некоторый символ, имеет индекс  $t \equiv 0 \pmod{p}$  и, следовательно, не может содержать силовскую  $p$ -подгруппу. Пусть теперь  $P_1$  — силовская  $p$ -подгруппа в группе  $H$ , оставляющая на месте символы 1, 2, 3, 4 и содержащая  $P$ . Тогда группа  $P_1$  переставляет  $4t$  символов, переставляемых группой  $C$ , и не переставляет никакие другие, кроме, может быть, случая, когда

$$p = 3, \quad t = 3^w, \quad n = 4t + 7.$$

В этом случае группа  $P_1$ , возможно, перемещает  $4t + 3$  символов. Эту возможность мы рассмотрим отдельно позднее. В основном же случае, согласно теореме 5.7.1, группа  $N_G(P_1)$  четырежды транзитивна на первых шести или семи буквах, а потому содержит группу  $A_6$  или  $A_7$  на этих символах. Но подгруппа, переводящая первые шесть (или семь) символов в себя, также содержит подстановку  $\pi$  из (5.8.5), которая не содержится в знакопеременной группе этих символов. Таким образом, в группе  $G$  содержится вся подгруппа, действующая как симметрическая группа на множестве из первых шести или семи символов, и, следовательно, некоторый элемент, оставляющий на месте первые четыре символа и переставляющий пятый и шестой символы. Это противоречит предположению о нечетности порядка подгруппы  $H$ . Остается рассмотреть случай, когда

$$t = 3^w, \quad n = 4t + 7$$

и группа  $P_1$  переставляет символы 5, 6 и 7 так же, как и  $4t$  символов, переставляемые группой  $P$ . Если  $w > 1$ , то, конечно,

5, 6 и 7 образуют область транзитивности группы  $P_1$ , и в группе  $G$  существует элемент вида

$$z = (1)(2)(3)(4)(567) \dots$$

Если же  $w = 1$ , то  $P$  — группа порядка 3 (даже если в  $P_1$  символы 5, 6, 7 попадают в одну область транзитивности с областями транзитивности 8, 9, 10 и 11, 12, 13 группы  $P$ ).

Так как имеется элемент вида  $(5)(6)(7)(8, 9, 10)(11, 12, 13) \dots$ , то найдется и элемент вида  $z$ , оставляющий на месте 8, 9, 10. Но из подстановки вида  $z = (1)(2)(3)(4)(567) \dots$  и подстановки  $u$  из (5.8.5) имеем подстановку

$$(zu)^3 = (1)(2)(35)(4)(6)(7) \dots$$

а это противоречит условию, что подгруппа  $H$ , относительно которой инвариантны четырёх символа, — нечетного порядка.

Пусть  $G$  — четырежды транзитивная группа степени 11, не совпадающая с группами  $S_{11}$  и  $A_{11}$ . Если  $G$  содержит элемент одного из видов:  $(a, b)$ ,  $(a, b)(c, d)$  или  $(a, b, c)$ , то в силу четырехкратной транзитивности группы  $G$  содержит так же все элементы такого вида и поэтому должна совпадать с  $A_{11}$  и  $S_{11}$ . Если группа  $G$  содержит цикл длины 5 или 7, то такой цикл порождает транзитивную и примитивную группу на символах, которые он переставляет. В этом случае, согласно теоремам 5.6.2 и 5.7.1, группа  $G$  должна совпадать с  $S_{11}$  или  $A_{11}$ . За исключением рассмотренных случаев, подгруппа  $V = V_{1234}$ , оставляющая на месте четыре символа, имеет порядок, делящий  $2^4 \cdot 3^2$ . Если группа  $V$  отлична от единичной, то она должна содержать силовскую 2-подгруппу или силовскую 3-подгруппу. Вследствие сделанного нами исключения в каждом из этих случаев такая силовская подгруппа должна перемещать точно шесть символов. По теореме 5.7.1 нормализатор группы  $P$  является четырежды транзитивной группой на остальных пяти символах, и, так как группа  $P$  имеет области транзитивности одного из следующих видов: три и три символа, четыре и два символа или два, два и два символа, отсюда следует, что группа  $G$  содержит цикл длины пять, а этот вариант исключен. Таким образом, единственная оставшаяся возможность заключается в том, что подгруппа  $V$ , относительно которой инвариантны четыре символа, состоит только из единицы, а группа  $G$  порядка  $11 \cdot 10 \cdot 9 \cdot 8$ .

Подгруппа  $W$ , оставляющая на месте три символа, например 9, 10, 11, регулярна и транзитивна на остальных восьми символах, а потому она является регулярным представлением одной из пяти различных групп порядка восемь. Подгруппа  $W$  содержит

элементы порядка два, скажем  $x = (12)(34)(56)(78)(9)(10)(11)$ . В подгруппе  $H$ , оставляющей на месте символы 10 и 11, содержатся девять сопряженных с  $W$  подгрупп, для каждой из которых имеется в точности один инвариантный символ. Если бы два различных элемента порядка два содержали некоторую общую транспозицию, скажем  $(i, j)$ , то их произведение было бы элементом, отличным от единицы и переставляющим не более семи символов, а это уже исключено. Но каждый из рассматриваемых элементов порядка два содержит четыре транспозиции, а транспозиций символов 1, ..., 9 существует только  $9 \cdot 8/2 = 36$ . Следовательно, группа  $W$  содержит всего один элемент порядка 2 и должна быть или циклической группой порядка 8, или группой кватернионов. Но если  $W$  — циклическая группа, то ее нормализатор содержит элемент порядка 3, который может быть только циклом  $(9, 10, 11)$ , что невозможно. Следовательно, группа  $W$  должна быть группой кватернионов  $Q$ .

Подгруппа  $H$ , для которой символы 10, 11 инвариантны, имеет порядок 72 и содержит девять групп кватернионов, из которых любые две пересекаются по единице. Тождественная подстановка и восемь остальных элементов<sup>1)</sup> образуют подгруппу  $U$  порядка 9, которая инвариантна в  $H$ . Восемь элементов группы  $U$ , отличные от единицы, сопряжены относительно группы  $Q$ , и поэтому  $U$  — элементарная абелева группа.

Исходя из установленных фактов, мы легко можем построить группу  $H$ , единственную с точностью до изоморфизма. В качестве подстановок, порождающих  $U$ , мы можем выбрать подстановки

$$u = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10)(11),$$

$$v = (1, 4, 7)(2, 5, 8)(3, 6, 9)(10)(11).$$

Тогда  $H = QU$ , где  $Q$  — группа кватернионов, порожденная подстановками

$$a = (1)(2, 4, 3, 7)(5, 6, 9, 8)(10)(11),$$

$$b = (1)(2, 5, 3, 9)(4, 8, 7, 6)(10)(11),$$

и

$$a^2 = b^2 = (1)(23)(47)(59)(68)(10)(11).$$

Подгруппа  $K$ , оставляющая на месте символ 11, порождается подгруппой  $H$  и элементом  $x$ , сопряженным с  $a^2$ , оставляющим на месте 2 и 11 и переставляющим символы 1 и 10. Такой элемент должен существовать, так как группа  $G$  четырежды тран-

<sup>1)</sup> То есть не входящих ни в одну из сопряженных групп кватернионов. — Прим. перев.

зитивна. Ясно, что  $x$  принадлежит нормализатору группы  $Q$ . Присоединение элемента  $x$  к группе  $H$  не должно давать элемента, отличного от единицы и оставляющего на месте четыре символа. Для элемента  $x$  имеются только три возможности:

$$x_1 = (1, 10)(2)(3)(11)(4, 5)(6, 8)(7, 9),$$

$$x_2 = (1, 10)(2)(3)(11)(4, 6)(5, 9)(7, 8),$$

$$x_3 = (1, 10)(2)(3)(11)(4, 7)(5, 6)(8, 9).$$

Подстановка  $(4, 5, 6)(7, 8, 9)$  трансформирует группу  $H$  в себя, а  $x_1, x_2, x_3$  — друг в друга. Поэтому, с точностью до изоморфизма, мы можем присоединить к  $H$  любой из этих трех элементов. Пусть подгруппа  $K$  получается присоединением элемента  $x_1$  к  $H$ . Тогда группа  $G$  получается присоединением к подгруппе  $H$  подстановки  $y$ , сопряженной с  $a^2$ , оставляющей на месте символы 2 и 10 и переставляющей 1 и 11. Поэтому элемент  $y$  принадлежит нормализатору подгруппы  $Q$  и подгруппы, оставляющей на месте 1 и 11. Таких элементов  $y$  может быть лишь два:

$$y_1 = (1, 11)(2)(3)(10)(4, 6)(5, 9)(7, 8),$$

$$y_2 = (1, 11)(2)(3)(10)(4, 7)(5, 6)(8, 9).$$

Элемент  $(4, 9)(5, 7)(6, 8)$  принадлежит нормализатору подгруппы  $K$  и трансформирует элементы  $y_1$  и  $y_2$  друг в друга. Следовательно, мы можем считать, что, с точностью до изоморфизма, группа  $G$  получается присоединением элемента  $y_1$  к подгруппе  $K$ . Итак,  $G = \{H, x_1, y_1\}$ . Строго говоря, мы только что доказали, что если существует четырежды транзитивная группа на 11 символах, отличная от  $A_{11}$  и  $S_{11}$ , то она изоморфна группе  $G$ . Проверка того, что группа  $G$  действительно обладает этими свойствами, предоставляет читателю в виде упражнения (упражнение 4). Группа  $G$  называется группой Матье одиннадцатой степени и обозначается  $M_{11}$ . Следует отметить следующий замечательный факт. Если рассматривать группу  $M_{11}$  как группу подстановок, оставляющую на месте символ 12, и группу  $M_{12} = \{M_{11}, z\}$ , где

$$z = (1, 12)(2)(3)(10)(11)(4, 7)(5, 6)(8, 9),$$

то мы обнаружим, что  $M_{12}$  — пятикратно транзитивная группа порядка  $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$ , а  $M_{11}$  — ее подгруппа, для которой символ 12 инвариантен.

Рассуждениями, аналогичными тем, которые проводились при построении  $M_{11}$ , можно доказать, что единственными четырежды транзитивными группами (кроме знакопеременных и симметрических) менее чем 35 степени являются группы  $M_{11}$ ,  $M_{12}$  и группы

Матые 23 и 24 степени, обозначаемые соответственно  $M_{23}$  и  $M_{24}$ . Эти последние группы  $M_{23}$  и  $M_{24}$  можно определить с помощью подстановок

$$A = (0, 1, 2, 3, \dots, 22),$$

$$B = (2, 16, 9, 6, 8)(4, 3, 12, 13, 18).$$

$$\cdot (10, 11, 22, 7, 17)(20, 15, 14, 19, 21),$$

$$C = (0, 23)(1, 22)(2, 11)(3, 15)(4, 17) \cdot$$

$$\cdot (5, 9)(6, 19)(7, 13)(8, 20)(10, 16)(12, 21)(18, 14)$$

следующим образом:  $M_{23} = \{A, B\}$  и  $M_{24} = \{A, B, C\}$ ;  $M_{23}$  — четырежды транзитивная группа степени 23 и порядка  $23 \cdot 22 \cdot 21 \cdot 19 \cdot 16 \cdot 3$ , а  $M_{24}$  — пятикратно транзитивная группа, содержащая  $M_{23}$  в качестве подгруппы, оставляющей на месте символ 24.

### 5.9. Сплетение<sup>1)</sup>. Силовские подгруппы симметрических групп

Пусть  $G$  и  $H$  — группы подстановок множеств  $A$  и  $B$  соответственно. Дадим определение сплетения групп  $G$  и  $H$ , обозначаемого  $G \wr H$ .  $G \wr H$  — это группа всех таких подстановок  $\theta$  множества  $A \times B$ , что

$$(a, b)\theta = (a\gamma_b, b\eta), \quad a \in A, \quad b \in B, \quad (5.9.1)$$

где  $\gamma_b$  — подстановка из группы  $G$  для любого  $b \in B$ , причем подстановки  $\gamma_b$  для различных элементов  $b$  выбираются независимо,  $\eta$  — подстановка из группы  $H$ . Подстановки  $\theta$ , для которых  $\eta = 1$ , образуют инвариантную подгруппу  $G^*$ , изоморфную прямому произведению  $n$  экземпляров группы  $G$ , где  $n$  — число символов во множестве  $B$ . Фактор-группа  $G/G^*$  изоморфна группе  $H$ , а подстановки  $\theta$ , для которых  $\gamma_b = 1$ , образуют подгруппу, которая изоморфна группе  $H$  и элементы которой могут служить представителями смежных классов  $G$  по  $G^*$ .

Сплетение — ассоциативная операция в том смысле, что если  $K$  — третья группа подстановок некоторого множества  $C$ , то группы  $(G \wr H) \wr K$  и  $G \wr (H \wr K)$  изоморфны, а если отождествить множества  $(A \times B) \times C$  и  $A \times (B \times C)$  с множеством  $A \times B \times C$ , то они совпадают.

<sup>1)</sup> В оригинале „wreath product“, что доеволюно означает „веночное произведение“. В ряде работ редактора для этого понятия употреблялся термин „полное произведение“ (по-французски „produit complet“). В последнее время в советской алгебраической литературе для обозначения рассматриваемого образования появился термин „сплетение“, которым мы и будем пользоваться в дальнейшем. — Прим. ред.

При помощи сплетения легко построить силовские подгруппы симметрической группы  $S_n$ . Какая наивысшая степень числа  $p$  делит  $n!$ ? Сомножителями числа  $n!$ , делящимися на  $p$ , являются числа  $p, 2p, \dots, kp$ , где  $k = [n/p]$  — наибольшее целое число, не превосходящее  $n/p$ . Следовательно,  $n!$  делится на  $p^k$  и еще на ту максимальную степень числа  $p$ , которая делит  $k!$ . Замечая, что  $[k/p] = [n/p^2]$ , и продолжая эту редукцию, мы находим, что наивысшая степень числа  $p$ , делящая  $n!$ , равна  $p^M$ , где

$$M = \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \left[ \frac{n}{p^3} \right] + \dots$$

Если выразить  $n$  в системе исчисления с основанием  $p$ :

$$n = a_0 p^u + a_1 p^{u-1} + \dots + a_{u-1} p + a_u, \quad (5.9.2)$$

где  $0 \leq a_i \leq p - 1$  для любого  $i$ , то оказывается, что

$$\begin{aligned} M = & a_0(p^{u-1} + p^{u-2} + \dots + p + 1) + \\ & + a_1(p^{u-2} + \dots + p + 1) + \dots + a_{u-1}. \end{aligned} \quad (5.9.3)$$

В частности, силовская подгруппа симметрической группы степени  $p^r$  имеет порядок  $p^{N_r}$ , где  $N_r = p^{r-1} + p^{r-2} + \dots + p + 1$ . Отсюда видно, что, построив силовские  $p$ -подгруппы для симметрических групп степеней  $p, p^2, \dots, p^u$ , мы можем легко построить силовскую  $p$ -подгруппу симметрической группы степени  $n$ , где  $n$  имеет вид (5.9.2). Для этого нужно разбить множество из  $n$  символов на такие непересекающиеся подмножества:  $a_0$  подмножество из  $p^u$  символов,  $a_1$  подмножество из  $p^{u-1}$  символов, ...,  $a_{u-1}$  подмножество из  $p$  символов,  $a_u$  отдельных элементов. Затем в каждом из этих подмножеств строится соответствующая силовская  $p$ -подгруппа и образуется их прямое произведение. Таким образом можно получить подгруппу  $P$  порядка  $p^M$ , где  $M$  имеет вид (5.9.3). Следовательно, подгруппа  $P$  и будет силовской  $p$ -подгруппой группы  $S_n$ .

Силовская  $p$ -подгруппа группы  $S_p$  символов  $1, 2, \dots, p$  имеет порядок  $p$ , и поэтому силовская  $p$ -подгруппа — циклическая группа, порожденная циклом  $a_1 = (1, 2, \dots, p)$ . Группа  $S_{p^2}$  символов  $1, 2, \dots, p^2$  имеет подгруппу, являющуюся прямым произведением циклических групп, порожденных элементами

$$\begin{aligned} a_1 &= (1, 2, \dots, p), \quad a_2 = (p+1, p+2, \dots, 2p), \dots \\ &\dots, \quad a_p = (p^2 - p + 1, \dots, p^2). \end{aligned}$$

Если выбрать еще один элемент порядка  $p$ , а именно

$$b = (1, p+1, 2p+1, \dots, p^2-p+1)(2, p+2, \dots) \dots$$

$$\dots (p, 2p, \dots, p^2),$$

то  $b^{-1}a_i b = a_{i+1}$ , где индекс  $i$  пробегает систему вычетов по модулю  $p$ . Таким образом, элементы  $b$  и  $a_i$  ( $i=1, \dots, p$ ) порождают группу  $P_2$  порядка  $p^{p+1}$ , которая является сплетением циклических групп, порожденных элементами  $b$  и  $a_1$ . Группа  $P_2$  — силовская  $p$ -подгруппа группы  $S_{p^2}$ . Вообще, пусть  $P_r$  — силовская  $p$ -подгруппа группы  $S_{p^r}$  символов  $1, \dots, p^r$ . Рассмотрим симметрическую группу  $S_{p^{r+1}}$  символов  $1, \dots, p^r, p^r+1, \dots, 2p^r, \dots, p^{r+1}$ . Тогда, выбрав элемент

$$c = [1, p^r+1, 2p^r+1, \dots, (p-1)p^r+1] \dots$$

$$\dots [j, p^r+j, \dots, (p-1)p^r+j] \dots;$$

где  $j$  принимает значения  $1, \dots, p^r$ , получаем группы  $P_r^{(i)} = c^{-i}P_r c^i$  порядка  $p^{N_r}$  символов  $ip^r+1, \dots, (i+1)p^r$ . Так как группы  $P_r^{(i)}$  ( $i=0, 1, \dots, p-1$ ) заданы на непересекающихся множествах символов, то группа, которую они порождают, является их прямым произведением. Элемент  $c$  и подгруппа  $P_r$  порождают подгруппу порядка  $p^{pN_r+1}$ . Но  $pN_r+1 = p[p^{r-1}+\dots+p+1]+1=N_{r+1}$ , и поэтому  $c$  и  $P_r$  порождают силовскую  $p$ -подгруппу  $P_{r+1}$  симметрической группы  $p^{r+1}$  символов.

Если группа  $P_r$  действует на символах  $1, \dots, p^r$ , подстановка  $c$  — цикл  $c = (u_0, u_1, \dots, u_{p-1})$ , то сплетеение  $P_r \setminus \{c\}$  переставляет символы  $(i, u_j)$ , где  $i=1, \dots, p^r$ ;  $j=0, \dots, p-1$ . Если отождествить цикл  $(i, u_j)$  с элементом  $i+jp^r$ , то только что построенная группа  $P_{r+1}$  совпадает со сплетеением  $P_r \setminus \{c\}$ . Попутно отметим, что группа  $P_r$  порождается  $r$  элементами порядка  $p$ .

Например, силовская 2-подгруппа группы  $S_8$  имеет порядок 27 и порождается подстановками  $a_1 = (1, 2)$ ,  $b_1 = (1, 3)(2, 4)$ ,  $c_1 = (1, 5)(2, 6)(3, 7)(4, 8)$ .

## Упражнения

1. Пусть  $G$  — бесконечная группа,  $H$  — ее подгруппа конечного индекса. Показать, что существует подгруппа  $K \subset H$ , инвариантная в  $G$  и имеющая в ней конечный индекс. (Указание: представить группу  $G$  как группу подстановок смежных классов по  $H$ .)

2. Показать, что существует только одна простая группа порядка 60, а именно знакопеременная группа степени 5.

3. Показать, что группа  $S_4$  имеет два точных транзитивных представления на множестве из шести символов, которые не подобны между собой.

4. Пусть даны подстановки

$$u = (1, 2, 3)(4, 5, 6)(7, 8, 9),$$

$$a = (2, 4, 3, 7)(5, 6, 9, 8),$$

$$b = (2, 5, 3, 9)(4, 8, 7, 6),$$

$$x = (1, 10)(4, 5)(6, 8)(7, 9),$$

$$y = (1, 11)(4, 6)(5, 9)(7, 8),$$

$$z = (1, 12)(4, 7)(5, 6)(8, 9).$$

Показать, что  $\{u, a, b, x, y\}$  — четырежды транзитивная группа Матье степени 11 и порядка  $11 \cdot 10 \cdot 9 \cdot 8$ , а группа  $\{M_{11}, z\}$  — пятикратно транзитивная группа Матье  $M_{12}$ , содержащая  $M_{11}$  в качестве подгруппы, оставляющей на месте символ 12.

5. Даны подстановки

$$a = (0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22),$$

$$b = (2, 16, 9, 6, 8)(3, 12, 13, 18, 4)(7, 17, 10, 11, 22)(14, 19, 21, 20, 15),$$

$$c = (0, 23)(1, 22)(2, 11)(3, 15)(4, 17)(5, 9)(6, 19)(7, 13)(8, 20)(10, 16)(12, 21)(14, 18).$$

Показать, что  $\{a, b\}$  — четырежды транзитивная группа Матье  $M_{23}$  степени 23 и порядка  $23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$  и что  $M_{24} = \{a, b, c\}$  — пятикратно транзитивная группа Матье, в которой группа  $M_{23}$  является подгруппой, оставляющей на месте символ 23.

## Г л а в а 6

### АВТОМОРФИЗМЫ

#### 6.1. Автоморфизмы алгебраических систем

В § 1.2 мы видели, что все взаимно однозначные отображения любого множества на себя образуют группу. Вообще, все взаимно однозначные отображения множества  $S$  на себя, которые сохраняют некоторые определенные свойства  $P$ , также образуют группу.

Пусть  $A$  — некоторая алгебраическая система, состоящая из элементов  $X = \{x\}$  и операций  $f_\mu$ , таких, что  $f_\mu(x_1, \dots, x_n) = y$  есть некоторый элемент множества  $A$ , если элементы  $x_1, \dots, x_n$  принадлежат  $A$ . Таких операций может быть как угодно много, но каждая из них является однозначной функцией от конечного числа  $n$  аргументов. „Законы“ или „аксиомы“ системы  $A$  задаются как отношения, включающие операции. При этом взаимно однозначное отображение  $\alpha$  множества  $X$  на себя,  $X \rightleftarrows X^\alpha$ , называется *автоморфизмом* системы  $A$ , если из соотношения

$$f_\mu(x_1, \dots, x_n) = y \text{ вытекает } f_\mu(x_1^\alpha, \dots, x_n^\alpha) = y^\alpha \quad (6.1.1)$$

для всех операций  $f_\mu$  и любых значений  $x_1, \dots, x_n$ . Произведение двух автоморфизмов есть снова автоморфизм, поэтому относительно умножения все автоморфизмы образуют группу. В частности, автоморфизмы группы образуют группу. Так как в группе определена единственная бинарная операция умножения, то для того, чтобы взаимно однозначное отображение  $\alpha$  было автоморфизмом, достаточно потребовать, чтобы из равенства  $ab = c$  следовало равенство  $a^\alpha b^\alpha = c^\alpha$ , или, более кратко,  $(ab)^\alpha = a^\alpha b^\alpha$ .

Автоморфизмы алгебраических систем являются естественным источником групп. Исторически теория групп возникла из изучения автоморфизмов алгебраических полей.

#### 6.2. Автоморфизмы групп. Внутренние автоморфизмы

Взаимно однозначное отображение  $\alpha: x \rightleftarrows x^\alpha$  группы  $G$  на себя является автоморфизмом группы  $G$  в том и только в том случае, если из соотношения  $ab = c$  вытекает соотношение  $a^\alpha b^\alpha = c^\alpha$ , или, кратко, если

$$(ab)^\alpha = a^\alpha b^\alpha. \quad (6.2.1)$$

Условие (6.2.1) определяет эндоморфизм, а в § 2.4 мы определили автоморфизм как взаимно однозначный эндоморфизм. Таким образом, два определения группового автоморфизма эквивалентны.

Любой фиксированный элемент  $a \in G$  определяет следующее отображение  $A_a$  группы  $G$  на себя:

$$A_a : x \mapsto a^{-1}xa \quad \text{для всех } x \in G. \quad (6.2.2)$$

Это отображение взаимно однозначно, так как  $axa^{-1} \mapsto a^{-1}(ax)a = x$ , и, кроме того, является автоморфизмом, так как  $a^{-1}xua = a^{-1}xa \cdot a^{-1}ua$ . Автоморфизм  $A_a$  группы  $G$  называется *внутренним автоморфизмом*. Все остальные автоморфизмы группы  $G$  называются *внешними*. Так как  $b^{-1}(a^{-1}xa)b = (ab)^{-1}x(ab)$  и  $a(a^{-1}xa)a^{-1} = x$ , ясно, что

$$A_a A_b = A_{ab}; \quad A_{a^{-1}} = A_a^{-1}. \quad (6.2.3)$$

**Теорема 6.2.1.** *Все внутренние автоморфизмы группы  $G$  образуют нормальный делитель  $I(G)$  группы  $A(G)$  всех автоморфизмов группы  $G$ . Отображение  $a \mapsto A_a$  является гомоморфизмом группы  $G$  на группу  $I(G)$ ; его ядро — центр группы  $G$ .*

*Доказательство.* Из соотношений (6.2.3) ясно, что внутренние автоморфизмы образуют подгруппу  $I(G)$  группы  $A(G)$ . Пусть  $\alpha$  — произвольный автоморфизм группы  $G$ . Тогда  $(a^{-1}xa)^\alpha = (a^\alpha)^{-1}x^\alpha a^\alpha$ . Следовательно, отображение  $\alpha^{-1}A_a\alpha$  переводит элемент  $x$  в элемент  $(a^\alpha)^{-1}x^\alpha a^\alpha$ , откуда  $\alpha^{-1}(A_a)\alpha = A_{a^\alpha}$ , и, значит,  $I(G)$  является нормальным делителем группы  $A(G)$ . Из тех же равенств (6.2.3) видно, что отображение  $a \mapsto A_a$  есть гомоморфизм группы  $G$  на группу  $I(G)$ . При этом  $A_a = 1$  тогда и только тогда, когда  $xa = ax$  при любом  $x \in G$ . Таким образом,  $A_a = 1$  тогда и только тогда, когда элемент  $a$  принадлежит центру группы  $G$ . Итак, ядро гомоморфизма  $G \rightarrow I(G)$  образует центр группы  $G$ .

Конечная абелева группа  $X$  представима как прямое произведение своих силовских подгрупп (теорема 3.2.3):

$$X = S(p_1) \times S(p_2) \times \dots \times S(p_r). \quad (6.2.4)$$

Группа  $A(X)$  всех автоморфизмов группы  $X$  должна содержать прямое произведение групп автоморфизмов  $A[S(p_i)]$ . Но так как любой автоморфизм группы  $X$  должен отображать каждую из подгрупп  $S(p_i)$ ,  $i = 1, \dots, r$ , на себя, других автоморфизмов не

существует, и потому

$$A(X) = A[S(p_1)] \times \dots \times A[S(p_r)]. \quad (6.2.5)$$

Вообще группа автоморфизмов периодической абелевой группы является декартовым произведением групп автоморфизмов силовских подгрупп.

Проблема нахождения автоморфизмов периодической абелевой группы, таким образом, сведена к нахождению автоморфизмов абелевой  $p$ -группы. Любой автоморфизм конечной абелевой  $p$ -группы  $A_p$  отображает один базис на другой базис. Обратно, пусть  $a_1, \dots, a_s$  и  $b_1, \dots, b_s$  — два базиса группы  $A_p$ , упорядоченные так, что порядок элемента  $a_i$  равен порядку элемента  $b_i$  ( $i = 1, \dots, s$ ). Последнее возможно согласно теореме 3.3.2. Тогда из разложений

$$A_p = \{a_1\} \times \{a_2\} \times \dots \times \{a_s\} = \{b_1\} \times \{b_2\} \times \dots \times \{b_s\} \quad (6.2.6)$$

видно, что отображение

$$a_i \rightarrow (a_i)\alpha = b_i \quad (i = 1, \dots, s) \quad (6.2.7)$$

есть автоморфизм  $\alpha$  группы  $A_p$ .

В циклической группе  $C = \{a\}$ ,  $a^p = 1$ , любой элемент  $a^i$  ( $i = 1, \dots, p - 1$ ) является образующим. Следовательно, существует  $p - 1$  автоморфизмов, которые можно задать отображением  $a \rightarrow (a)a_i = a^i$ . Если  $r$  — первообразный корень<sup>1)</sup> в кольце вычетов по модулю  $p$ , то отображение  $a \rightarrow (a)\beta = a^r$  определяет автоморфизм  $\beta$ . Тогда  $a \rightarrow (a)\beta^j = a^{r^j}$ . Так как  $r$  — первообразный корень, наименьшая степень  $j$  числа  $r$ , такая, что  $r^j \equiv 1 \pmod{p}$ , равна  $j = p - 1$ . Следовательно, автоморфизм  $\beta$  имеет порядок  $p - 1$ , а группа автоморфизмов  $A(C)$  — циклическая порядка  $p - 1$  с порождающим элементом  $\beta$ .

### 6.3. Голоморф группы

Как отмечалось в § 1.4, правое и левое регулярные представления группы  $G$  являются подгруппами группы  $S_G$  всех подстановок множества элементов группы  $G$ . Кроме того, если  $\alpha$  — автоморфизм группы  $G$ , то отображение  $\alpha: x \mapsto x^\alpha$  также элемент группы  $S_G$ , оставляющий на месте единицу 1 группы  $G$ .

Так как  $(g_1x)g_2 = g_1(xg_2)$ , мы имеем равенство  $L(g_1)R(g_2) = R(g_2)L(g_1)$ . Таким образом, правое и левое регулярные представления группы  $G$  поэлементно перестановочны.

<sup>1)</sup> О первообразных корнях см. Биркгоф и Маклейн [1], стр. 446, или Харди и Райт [1], стр. 236 (см. также Виноградов И. М., Основы теории чисел, ГИТТЛ, М., 1952, стр. 92. — Прим. перев.).

**Теорема 6.3.1.** Правое (левое) регулярное представление группы  $G$  является централизатором левого (правого) регулярного представления в группе  $S_G$ .

**Доказательство.** Пусть подстановка  $\pi$  из группы  $S_G$  принадлежит централизатору подгруппы  $L(G)$  и  $(1)\pi = g$ . Тогда подстановка  $\pi R(g)^{-1} = \pi^*$  принадлежит централизатору группы  $L(G)$  и оставляет на месте единицу:  $(1)\pi^* = 1$ . При этом  $(1)\pi^* L(g') = g'$ . Следовательно,  $(1)L(g')\pi^* = g'$ , т. е.  $(g')\pi^* = g'$ . Но ведь  $g'$  — произвольный элемент из группы  $G$ , поэтому  $\pi^* = 1$ , следовательно,  $\pi \in R(g)$ . Итак, централизатор подгруппы  $L(G)$  есть  $R(G)$ . Аналогично  $L(G)$  есть централизатор  $R(G)$ .

Этим указан централизатор подгруппы  $R(G)$  в группе  $S_G$ . Будем называть нормализатор подгруппы  $R(G)$  в  $S_G$  голоморфом группы  $G$ .

**Теорема 6.3.2.** Пусть  $H$  — голоморф группы  $G$ , т. е. нормализатор правого регулярного представления  $R(G)$  в группе  $S_G$ . Подгруппа группы  $H$ , оставляющая единицу группы  $G$  на месте, есть группа  $A(G)$  автоморфизмов группы  $G$ .

**Доказательство.** Пусть  $H$  — нормализатор подгруппы  $R(G)$  и  $\alpha$  — элемент из  $H$ , оставляющий единицу на месте. Тогда отображение  $R(g) \xrightarrow{\alpha} \alpha^{-1}R(g)\alpha$ , безусловно, является автоморфизмом группы  $R(G)$ , так как подгруппа  $R(G)$  инвариантна в  $H$ . Следовательно, равенство  $\alpha^{-1}R(g)\alpha = R(g^\alpha)$  определяет взаимно однозначное отображение  $g \xrightarrow{\alpha} g^\alpha$  группы  $G$  на себя. Но так как при этом  $(g_1g_2)^\alpha = g_1^\alpha g_2^\alpha$ , отображение  $g \xrightarrow{\alpha} g^\alpha$  есть автоморфизм группы  $G$ . Но ведь фактически  $\alpha$  и есть подстановка  $g \xrightarrow{\alpha} g^\alpha$  множества  $G$ . Поскольку  $(1)\alpha = 1$  и  $\alpha^{-1}R(g)\alpha = R(g^\alpha)$ , получаем, что  $(1)\alpha R(g^\alpha) = g^\alpha$  и  $(1)R(g)\alpha = g^\alpha$ , откуда  $(g)\alpha = g^\alpha$ . Таким образом, если подстановка  $\alpha$  принадлежит  $H$  и оставляет 1 на месте, то  $\alpha$  — автоморфизм группы  $G$ . Обратно, пусть соответствие  $\alpha : g \xrightarrow{\alpha} g^\alpha$  — автоморфизм группы  $G$ . Тогда  $\alpha$  — элемент группы  $S_G$ , не переставляющий единицу  $1 \in G$ . Далее,  $(x)R(g)\alpha = x^\alpha g^\alpha$  и  $(x)\alpha R(g^\alpha) = x^\alpha g^\alpha$ . Следовательно,  $\alpha^{-1}R(g)\alpha = R(g^\alpha)$ , откуда видно, что элемент  $\alpha$  принадлежит нормализатору подгруппы  $R(G)$ . Таким образом, подгруппа группы  $H$ , оставляющая 1 на месте, состоит только из автоморфизмов, причем содержит все автоморфизмы группы  $G$ . При доказательстве теоремы 6.3.1 мы показали, что только единица группы  $S_G$  оставляет  $1 \in G$  на месте и что она перестановочна со всеми элементами подгруппы  $R(G)$ . Следовательно, каждый автоморфизм группы  $G$  представлен только одним элементом группы  $H$ , оставляющей 1 на месте. Поэтому совокупность этих элементов совпадает с  $A(G)$ . Так как нормализатор группы содержит ее централизатор, то имеем включение  $H \supset L(G)$ .

## 6.4. Совершенные группы

**ОПРЕДЕЛЕНИЕ.** Группа называется совершенной, если ее центр состоит только из единицы и все ее автоморфизмы внутренние.

**Теорема 6.4.1.** Пусть совершенная группа  $G$  является нормальным делителем группы  $T$ . Тогда группа  $T$  разлагается в прямое произведение  $G \times K$  группы  $G$  и централизатора  $K$  подгруппы  $G$  в  $T$ .

*Доказательство.* Пусть

$$T = G + Gx_2 + \dots + Gx_i + \dots \quad (6.4.1)$$

Тогда  $x_i^{-1}Gx_i = G$ , так как  $G$  — инвариантная подгруппа в  $T$ . Значит, соответствие  $g \leftrightarrow x_i^{-1}gx_i = g^a$  есть автоморфизм группы  $G$ . Так как любой автоморфизм группы  $G$  является внутренним, то  $g^a = a^{-1}ga$  для некоторого элемента  $a \in G$  и всех  $g \in G$ . Тогда для любого  $g \in G$  имеем  $x_i^{-1}gx_i = a^{-1}ga$ . Отсюда вытекает, что элемент  $y_i = x_i a^{-1}$  принадлежит централизатору  $K$  подгруппы  $G$  в группе  $T$ . Но тогда  $Gx_i = x_i G = x_i a^{-1}G = y_i G = Gy_i$ , и мы можем выбрать  $y_i$  в качестве представителей смежных классов по подгруппе  $G$ . Поэтому любой смежный класс по  $G$  в  $T$  содержит элемент из централизатора  $K$ . Следовательно,  $T = G \cup K = GK = KG$ , так как подгруппа  $G$  инвариантна. Но из того, что центр группы  $G$  равен 1, следует, что  $K \cap G = 1$ . А так как любой элемент из  $K$  перестановочен с любым элементом из  $G$ , то  $T = G \times K$ .

**Следствие 6.4.1.** Гомоморф  $H$  совершенной группы  $G$  есть прямое произведение  $R(G) \times L(G)$ .

Это следует из того, что  $L(G)$  есть централизатор  $R(G)$  в группе  $H$ .

## 6.5. Нормальные, или полуправильные, произведения

**Теорема 6.5.1.** Пусть даны две группы  $H$  и  $K$ , причем каждому элементу  $h \in H$  соответствует автоморфизм группы  $K$ :

$$k \leftrightarrow k^h \text{ при любом } k \in K, \quad (6.5.1)$$

подчиненный условию

$$(k^{h_1})^{h_2} = k^{h_1 h_2}, \quad h_1, h_2 \in H. \quad (6.5.2)$$

Тогда символы  $[h, k]$ ,  $h \in H$ ,  $k \in K$ , образуют группу относительно следующего правила умножения:

$$[h_1, k_1] \cdot [h_2, k_2] = [h_1 h_2, k_1^{h_2} k_2]; \quad (6.5.3)$$

эта группа называется нормальным произведением группы  $K$  на группу  $H$ , или полуправильным произведением  $K$  на  $H$ .

*Доказательство.* Так как  $k^h \in K$  для любых  $k$  и  $h$ , то произведение (6.5.3) вполне определено.

1) Умножение (6.5.3) ассоциативно, так как, согласно (6.5.2) и (6.5.3), имеем

$$([h_1, k_1] \cdot [h_2, k_2]) \cdot [h_3, k_3] = [h_1 h_2, k_1^{h_2} k_2] \cdot [h_3, k_3] = \\ = [(h_1 h_2) h_3, (k_1^{h_2} k_2)^{h_3} k_3] = [h_1 h_2 h_3, k_1^{h_2 h_3} k_2^{h_3} k_3], \quad (6.5.4)$$

а с другой стороны,

$$[h_1, k_1] \cdot ([h_2, k_2] \cdot [h_3, k_3]) = [h_1, k_1] [h_2 h_3, k_2^{h_3} k_3] = \\ = [h_1 h_2 h_3, k_1^{h_2 h_3} k_2^{h_3} k_3]. \quad (6.5.5)$$

2) Единицей является элемент  $[1, 1]$ , так как

$$[1, 1][h, k] = [1h, 1^h k] = [h, k], \\ [h, k][1, 1] = [h1, k^1 1] = [h, k],$$

где  $k^1 = k$  согласно условию (6.5.2).

3) Произвольный элемент  $[h, k]$  обладает левым обратным элементом  $[h^{-1}, (k^{-1})^{h^{-1}}]$ , так как

$$[h^{-1}, (k^{-1})^{h^{-1}}] \cdot [h, k] = [h^{-1}h, k^{-1}k] = [1, 1]. \quad (6.5.6)$$

Следовательно, символы  $[h, k]$ , перемножаемые по правилу (6.5.3), образуют группу  $G$ .

**Теорема 6.5.2.** Если  $G$  есть нормальное произведение  $K$  на  $H$ , то элементы вида  $[h, 1]$  группы  $G$  образуют подгруппу, изоморфную группе  $H$ , а элементы вида  $[1, k]$  образуют нормальный делитель, изоморфный группе  $K$ . Кроме того, автоморфизм (6.5.1) группы  $K$ , рассматриваемой как подгруппа группы  $G$ , индуцируется трансформированием элементом  $h = [h, 1]$  из группы  $H \subset G$ , так как

$$[h, 1]^{-1} [1, k] [h, 1] = [1, k^h]. \quad (6.5.7)$$

Более того,  $G = H \cup K$ , так как

$$[h, 1][1, k] = [h, k]. \quad (6.5.8)$$

*Доказательство.* Заметим, что соответствия  $h \leftrightarrow [h, 1]$  и  $k \leftrightarrow [1, k]$  являются изоморфизмами между группами  $H$  и  $K$  и соответствующими подгруппами группы  $G$  [это следует из правила (6.5.3) и того, что  $k^1 = k$ ]. Равенства (6.5.7) и (6.5.8) прямо вытекают из правила умножения (6.5.3). Равенство (6.5.7) показывает, что  $K$  есть инвариантная подгруппа и что автоморфизм (6.5.1) совпадает с трансформированием элементом  $h = [h, 1]$ . Далее,  $H \cap K = [1, 1] = 1$ , а равенство (6.5.8) показывает, что

элементы из  $H$  могут быть взяты в качестве представителей смежных классов по нормальному делителю  $K$ .

**Теорема 6.5.3.** Группа  $G$  является нормальным произведением группы  $K$  на группу  $H$  тогда и только тогда, когда  $K$  есть инвариантная подгруппа группы  $G$ , а  $H$  — подгруппа группы  $G$ , элементы которой могут служить представителями смежных классов по  $K$ . Другими словами,

- 1)  $K$  — нормальный делитель группы  $G$ ,
- 2)  $H$  — подгруппа группы  $G$ ,
- 3)  $K \cap H = 1$ ,
- 4)  $H \cup K = G$ .

**Доказательство.** Мы уже видели, что эти свойства имеют место, если  $G$  — нормальное произведение  $K$  на  $H$ . Обратно, пусть эти свойства имеют место. Тогда из свойств 1), 3), 4), применяя теорему 2.3.3, получаем, что любой элемент  $G$  однозначно представим в виде

$$g = hk. \quad (6.5.9)$$

Так как подгруппа  $K$  инвариантна, то

$$h^{-1}kh = k^h \in K, \quad (6.5.10)$$

причем ясно, что  $k \mapsto k^h$  — автоморфизм группы  $K$ . Далее, из соотношения (6.5.10) получаем, что

$$(k^{h_1})^{h_2} = k^{h_1 h_2}. \quad (6.5.11)$$

Для двух элементов  $g_1 = h_1 k_1$  и  $g_2 = h_2 k_2$  группы  $G$  имеем следующее правило умножения:

$$g_1 g_2 = h_1 k_1 h_2 k_2 = h_1 h_2 (h_2^{-1} k_1 h_2) \cdot k_2 = h_1 h_2 \cdot k_1^{h_2} k_2. \quad (6.5.12)$$

Оно совпадает с правилом (6.5.3). Поэтому  $G$  — нормальное произведение  $K$  на  $H$ .

Отметим, что сопоставление некоторого автоморфизма группы  $K$  элементу из  $H$  определяет гомоморфизм группы  $H$  в группу автоморфизмов группы  $K$ . Если образом группы  $H$  является тождественный автоморфизм группы  $K$ , т. е.  $k^h = k$  для всех элементов  $h$  и  $k$ , то полупрямое произведение сводится к обычному прямому произведению групп  $H$  и  $K$ .

## Упражнения

1. Показать, что группа диэдра порядка 8 изоморфна своей группе автоморфизмов.

2. Показать, что группа автоморфизмов элементарной абелевой группы порядка  $p^r$  имеет порядок  $(p^r - 1)(p^r - p) \dots (p^r - p^{r-1})$ .

3. Найти внешний автоморфизм симметрической группы  $S_6$ , обладающий свойством переводить два класса сопряженных элементов порядка 3 друг в друга.

4. Показать, что если порядок группы делится на  $p^2$ , где  $p$  — простое число, то порядок ее группы автоморфизмов делится на  $p$ . (Указание: если в группе не существует внутреннего автоморфизма порядка  $p$ , то следует показать, что силовская  $p$ -подгруппа абелева и является прямым сомножителем группы  $G$ .)

5. Автоморфизм  $\alpha$  группы  $G$  называется центральным, если для любого элемента  $x \in G$  имеет место включение  $x^{-1}(x)\alpha \in Z$ , где  $Z$  — центр группы  $G$ . Доказать, что группа центральных автоморфизмов, которые являются внутренними, изоморфна центру фактор-группы  $G/Z$ .

6. Пусть группа  $G$  задана определяющими отношениями  $a^8 = b^8 = c^4 = 1$ ,  $b^{-1}ab = a^5$ ,  $c^{-1}ac = a^5$ ,  $c^{-1}bc = a^6b$ . Доказать, что подгруппа  $\{a, b\}$  представима как полупрямое произведение подгрупп  $\{a\}$  и  $\{b\}$  и что группа  $G$  — полупрямое произведение подгрупп  $\{a, b\}$  и  $\{c\}$ . Отсюда можно заключить, что порядок группы  $G$  равен 256, а элементы ее имеют вид  $a^ib^jc^k$ .

7. Пусть  $G$  — группа из упр. 6. Доказать, что  $\alpha: a \rightarrow a^5, b \rightarrow b, c \rightarrow c$  — внешний автоморфизм группы  $G$ , который переводит каждый класс сопряженных элементов группы  $G$  в себя.

## Г л а в а 7

### СВОБОДНЫЕ ГРУППЫ

#### 7.1. Определение свободной группы

Пусть нам дано множество элементов  $S = \{s_1, \dots, s_n\}$ , причем не предполагается, что число  $n$  конечно или даже счетно. Но когда это будет нам нужно, мы будем считать множество индексов  $i$  элементов  $s_i$  вполне упорядоченным. Введем символы  $s_i^1$  и  $s_i^{-1}$ , где  $s_i^1 = s_i$ , а  $s_i^{-1}$  — новый символ.

Слово — это пустая (обозначается 1) или конечная последовательность  $a_1 a_2 \dots a_t$ , где каждый символ  $a_i$  есть один из символов  $s_i^\epsilon$ ,  $\epsilon = \pm 1$ ,  $i = 1, \dots, n$ .

Слово называется *редуцированным*, если оно либо пустое, либо в его записи  $a_1 \dots a_t$  нет ни одной пары рядом стоящих символов  $a_i, a_{i+1}$  ( $i = 1, \dots, t - 1$ ) вида  $s_j^\epsilon, s_j^{-\epsilon}$ , где  $\epsilon = \pm 1$ .

Два слова  $f_1$  и  $f_2$  будем называть *соседними*, если они имеют вид  $f_1 = g s_j^\epsilon s_j^{-\epsilon} h$ ,  $f_2 = gh$ .

Два слова  $f$  и  $g$  *эквивалентны* (обозначается  $f \sim g$ ), если существует такая последовательность слов  $f_1 = f$ ,  $f_2, \dots, f_m = g$ , что слова  $f_i, f_{i+1}$  — соседние при  $i = 1, \dots, m - 1$ . Ясно, что отношение  $f \sim g$  рефлексивно, симметрично и транзитивно. Все слова, эквивалентные слову  $f$ , образуют класс эквивалентных слов, который мы обозначим через  $[f]$ .

**Лемма 7.1.1.** *Любой класс содержит одно и только одно редуцированное слово.*

*Доказательство.* Если слово  $f = a_1 \dots a_t$  содержит подслово  $a_i a_{i+1} = s_j^\epsilon s_j^{-\epsilon}$ , то соседнее с ним слово  $a_1 \dots a_{i-1} a_{i+2} \dots a_t$  состоит из меньшего числа символов. После не более чем  $t/2$  шагов сокращения мы придем к редуцированному слову, эквивалентному слову  $f$ . Этим показано, что класс  $[f]$  содержит, по меньшей мере, одно редуцированное слово.

Далее, исходя из слова  $f = a_1 a_2 \dots a_t$ , мы определяем следующую систему преобразований, которую назовем  $W$ -процессом:

$W_0 = 1$  — пустое слово,

$W_1 = a_1$ ,

$W_{i+1} = W_i a_{i+1}$ , если  $W_i$  не редуцированное слово вида  $X a_{i+1}^{-1}$ ,

$W_{i+1} = X$ , если  $W_i$  — редуцированное слово вида  $X a_{i+1}^{-1}$ .

Тогда, по индукции, легко видеть, что слова  $W_0, W_1, \dots, W_t$  являются редуцированными и что  $W_t = f$ , если слово  $f$  редуцировано. Пусть теперь

$$\begin{aligned}f_1 &= a_1 \dots a_r a_{r+1} \dots a_t, \\f_2 &= a_1 \dots a_r s_j^{-e} s_j^e a_{r+1} \dots a_t,\end{aligned}$$

и пусть  $W_0^1, W_1^1, \dots, W_t^1$  обозначают слова  $W$ -процесса, примененного к  $f_1$ , а  $W_0^2, \dots, W_{t+2}^2$  — соответствующие слова для слова  $f_2$ . Покажем, что  $W_t^1 = W_{t+2}^2$ . Имеют место равенства  $W_0^1 = W_0^2, \dots, W_r^1 = W_r^2$ , так как до  $r$ -го шага  $W$ -процессы совпадают. Дальше же возможны два случая.

1) Слово  $W_r^1 = W_r^2$  редуцировано и имеет вид  $Xs_j^{-e}$ . Так как слово  $Xs_j^{-e}$  редуцировано, то слово  $X$  не может быть вида  $Ys_j^e$ . Тогда для слова  $f_2$  имеем  $W_{r+1}^2 = X, W_{r+2}^2 = Xs_j^{-e} = W_r^2 = W_r^1$ .

2) Слово  $W_r^1 = W_r^2$  редуцировано, но не имеет вида  $Xs_j^{-e}$ . Тогда  $W_{r+1}^2 = W_{r+1}^1 s_j^e, W_{r+2}^2 = W_r^2 = W_r^1$ .

Следовательно, в обоих случаях  $W_{r+2}^2 = W_r^1$ , и по индукции мы заключаем, что  $W_{r+2+i}^2 = W_{r+i}^1$ , так как для всех последующих шагов процессы совпадают. Таким образом,  $W$ -процесс преобразует два соседних слова в одно и то же редуцированное слово. Следовательно, он и любые два эквивалентных слова переведет в одно и то же редуцированное слово. При этом  $W$ -процесс не изменяет редуцированного слова. Следовательно, в классе эквивалентных слов не может быть двух различных редуцированных слов.

Мы можем теперь определить произведение классов эквивалентных слов, относительно которого они будут образовывать группу. Мы назовем ее свободной группой  $F$ , порожденной множеством  $S$ .

**Теорема 7.1.1** Для произвольной пары классов слов  $[f_1], [f_2]$  над множеством  $S$  определим произведение следующим образом:  $[f_1][f_2] = [f_1 f_2]$ . Это произведение вполне определено, и относительно него классы эквивалентных слов над множеством  $S$  образуют группу — свободную группу  $F$ , порожденную множеством  $S$ .

**Доказательство.** Если  $f_1 \sim f'_1, f_2 \sim f'_2$ , то  $f_1 f_2 \sim f'_1 f'_2$ . Действительно, сперва можно показать, что  $f_1 f_2 \sim f'_1 f_2$ , заменяя  $f_1$  последовательно соседними словами, ведущими от  $f_1$  к  $f'_1$ . Аналогично доказывается, что  $f'_1 f_2 \sim f'_1 f'_2$ , откуда следует, что  $f_1 f_2 \sim f'_1 f'_2$ , т. е.  $[f'_1 f'_2] = [f_1 f_2]$ . Поэтому произведение  $[f_1 f_2] = [f_1][f_2]$  зависит только от перемножаемых классов, но не от

их представителей. При таком умножении класс, содержащий пустое слово, представляет собой единичный элемент, так как  $[1][f] = [f][1] = [f]$ . Кроме того, если  $f = a_1 \dots a_t$  и  $h = a_t^{-1} \dots a_1^{-1}$ , то  $[f][h] = [fh] = [1]$  и  $[h][f] = [hf] = [1]$ . Поэтому класс  $[a_t^{-1} \dots a_1^{-1}]$  есть обратный класс для класса  $[a_1 \dots a_t]$ . Далее мы обнаруживаем, что  $([f_1][f_2])[f_3] = [f_1 f_2 f_3] = [f_1]([f_2][f_3])$ , т. е. ассоциативный закон выполняется. Таким образом, классы слов образуют группу, называемую *свободной группой*  $F$ , порожденной множеством  $S$ . Чтобы отметить последнее обстоятельство, эту свободную группу часто обозначают через  $F_S$ .

Удобно писать  $f_1 = f_2$ , если слова  $f_1$  и  $f_2$  эквивалентны и, следовательно, представляют один и тот же элемент группы  $F$ . Мы будем писать  $f_1 \equiv f_2$  для обозначения равенства слов  $f_1$  и  $f_2$ . Удобно в качестве представителя класса выбирать редуцированное слово. Если слово  $f = a_1 \dots a_t$  редуцированное, то мы говорим, что оно редуцировано к этому виду.

В произвольной группе  $G$  множество элементов  $X: x_1, \dots, x_n$  порождает подгруппу  $H$ , состоящую из всех конечных произведений  $b_1 b_2 \dots b_t$ , где каждый элемент  $b_j$  вида  $x_j^\epsilon$ ,  $\epsilon = \pm 1$ . Нетрудно проверить, что эти конечные произведения действительно образуют подгруппу. Вообще говоря, элемент подгруппы  $H$  может быть записан в виде указанного конечного произведения многими способами. Кроме того, очевидно, что все элементы группы  $G$  порождают группу  $G$ . Следовательно, произвольную группу  $G$  можно рассматривать как группу, порожденную некоторым множеством элементов  $X$ , при этом пишут  $G = \{X\}$ . Следующая теорема показывает, почему свободные группы интересны не только сами по себе, но и как орудие исследования произвольных групп.

**Теорема 7.1.2.** Пусть группа  $G$  порождается множеством элементов  $X: x_1, \dots, x_n$ , а  $F$  — свободная группа с образующими  $S: s_1, \dots, s_n$ . Тогда существует гомоморфизм  $F \rightarrow G$ , определяемый отображениями  $s_i \rightarrow x_i$  для всех  $i$ .

**Доказательство.** Пусть  $f = a_1 \dots a_t$  — любое слово над множеством  $S$ . Рассмотрим элемент  $g = b_1 \dots b_t \in G$ , где  $b_i = x_j^\epsilon$ , если  $a_i = s_j^\epsilon$ . Тогда отображение  $f \rightarrow g$  переводит каждое слово над множеством  $S$  в некоторый элемент группы  $G$ . Ясно, что соседние, а поэтому и эквивалентные слова над  $S$  отображаются в один и тот же элемент группы  $G$ . Следовательно, отображение  $f \rightarrow g$  есть фактически отображение элементов свободной группы  $F$  на элементы группы  $G$ . При этом из того, что  $f_1 \rightarrow g_1$  и  $f_2 \rightarrow g_2$ , следует, что  $f_1 f_2 \rightarrow g_1 g_2$ . Значит, отображения  $s_i \rightarrow x_i$  определяют гомоморфизм свободной группы  $F$  на группу  $G$ .

Из теорем о гомоморфизмах получаем следствие.

**Следствие 7.1.1.** *Произвольная группа  $G$  с заданным множеством образующих  $X$  изоморфна фактор-группе свободной группы  $F$  с таким же количеством образующих элементов.*

Дадим другое определение свободной группы.

**ОПРЕДЕЛЕНИЕ:** *Свободная группа  $F$ , порожденная множеством элементов  $S$ , — это группа со следующими свойствами:*

- 1) *Группа  $F$  порождается множеством элементов  $S$ .*
- 2) *Если  $G$  — произвольная группа, порожденная множеством элементов  $X$ , и если дано взаимно однозначное соответствие между множествами  $S$  и  $X$ ,  $S \rightleftarrows X$ , то существует гомоморфизм группы  $F$  на группу  $G$ ,  $F \rightarrow G$ , продолжающий отображение  $S$  на множество  $X$ .*

Что второе определение свободной группы законно, ясно из теоремы 7.1.2. Действительно, свободная группа  $F_S$ , по первому определению, обладает этими свойствами. Кроме того, если  $F'$  — группа, имеющая эти свойства, то гомоморфизм  $F' \rightarrow F_S$  есть изоморфизм, так как его ядро состоит из единицы.

Однако следует отметить, что второе определение обладает рядом недостатков. Прежде всего, это неконструктивное определение, которое без приведенного выше действительного построения не дает возможности утверждать, что существует группа, удовлетворяющая требованиям 1) и 2), а если такая группа и существует, то ниоткуда не следует, что в ней нет никаких нетривиальных отношений. Кроме того, с более широкой точки зрения понятие „свободной“ системы, системы, в которой не выполняются никакие отношения, кроме отношений, вытекающих из аксиом, прочно укоренилось, хотя теорема, аналогичная теореме 7.1.2, может не иметь места.

## 7.2. Подгруппы свободных групп. Метод Шрейера

Природа подгрупп всегда играет фундаментальную роль при изучении групп. Теорема же 7.1.2 указывает на особую роль инвариантных подгрупп в свободных группах. Нильсен [1] и Шрейер [3] доказали, что подгруппы свободных групп сами свободны. Доказательство Нильсена проходит только для конечно порожденных групп, однако оно было обобщено Леви [1] и другими на произвольные свободные группы. Нильсен оперировал непосредственно элементами подгруппы, а Шрейер — смежными классами по подгруппе. Первое доказательство, которое мы дадим<sup>1)</sup>, представляет собой упрощение доказательства Шрейера.

<sup>1)</sup> См. М. Холл, Радо [1]. Дальнейшие результаты можно найти в работах М. Холла [4, 5].

Множество  $G$  элементов свободной группы  $F$  называется *шрейеровской системой*, если для любого элемента  $g \in G$  имеет место

- 1)  $g = a_1 a_2 \dots a_t$  — редуцированное слово,
- 2) слово  $a_1 a_2 \dots a_{t-1}$  также принадлежит  $G$ .

Мы будем говорить, что множество  $G$  — *двусторонняя шрейеровская система*, если наряду с 1) и 2) имеет место следующее свойство:

- 3) слово  $a_2 \dots a_t$  также принадлежит  $G$ .

Заметим, что шрейеровская система всегда содержит единичный элемент.

Пусть  $F$  — свободная группа, порожденная множеством  $S$ ,  $U$  — ее подгруппа. Рассмотрим левое разложение группы  $F$  по подгруппе  $U$ :

$$F = U \cdot 1 + U g_2 + \dots + U g_i + \dots \quad (7.2.1)$$

Представителем смежного класса  $U$  мы всегда будем выбирать единицу. Мы увидим, что целесообразно выбирать систему представителей остальных смежных классов так, чтобы они удовлетворяли некоторым определенным отношениям.

**Лемма 7.2.1.** (Обобщенная лемма ШРЕЙЕРА.) *Если  $U$  — подгруппа свободной группы  $F$ , то в качестве системы представителей левых смежных классов по подгруппе  $U$  можно выбрать некоторую шрейеровскую систему. Если  $U$  — инвариантная подгруппа группы  $F$ , то может быть выбрана система представителей, образующая двустороннюю шрейеровскую систему.*

**Доказательство.** Пусть множество образующих  $S : s_1, \dots, s_n$  группы  $F$  и обратных к ним элементов некоторым образом вполне упорядочено. Если число  $n$  конечно, это может быть сделано, например, так:  $s_1 < s_1^{-1} < s_2 < s_2^{-1} < \dots < s_n < s_n^{-1}$ . Но здесь вовсе не предполагается, что множество  $S$  конечно или даже счетно; предполагается лишь, что множество  $S \cup S^{-1}$  может быть вполне упорядочено.

Полное упорядочение множества  $S \cup S^{-1}$  может быть продолжено в *лексикографическое упорядочение*. А именно для двух элементов  $f$  и  $g$  группы  $F$  мы следующим образом определим отношение „ $<$ “:  $f < g$ , если редуцированные представления

$$\begin{aligned} f &= a_1 \dots a_t, \\ g &= b_1 \dots b_u \end{aligned}$$

этих элементов таковы, что выполняется одно из следующих свойств:

- 1)  $t < u$ ,

2)  $t = u, a_1 < b_1$ ,

3)  $t = u; a_1 = b_1, \dots, a_t = b_t; a_{t+1} < b_{t+1}$ ;

здесь символы  $a_i$  и  $b_j$  принадлежат множеству  $S \cup S^{-1}$ . Так определенный лексикографический порядок, конечно, является простым и даже полным порядком, причем выполняются следующие полезные свойства.

Если  $f < g$  и слово  $gh$  редуцировано, то  $fh < gh$ . Если  $f < g$  и элемент  $hg$  редуцирован, то  $hf < hg$ . Это следует из определения лексикографического порядка.

Чтобы доказать лемму, выберем в качестве представителя  $g_i$  смежного класса  $Ug_i$  первый элемент этого класса в смысле лексикографического упорядочения элементов группы  $F$ . Утверждается, что так выбранные представители  $g_i$  образуют шрейеровскую систему и даже двустороннюю шрейеровскую систему, если подгруппа  $U$  инвариантна. Так как единица есть первый элемент группы  $F$ , то она выбирается в качестве представителя смежного класса  $U$ . Пусть  $g = a_1 \dots a_{t-1} a_t$  — представитель класса  $Ug$ , т. е. наименьший элемент этого класса<sup>1)</sup>. Пусть  $h$  — наименьший элемент в классе, содержащем элемент  $h^* = a_1 \dots a_{t-1}$ . Если  $h = b_1 \dots b_t$ , то  $h \leq a_1 \dots a_{t-1}$ . Но  $ha_t \in Ug$ , поэтому  $g \leq ha_t$ . С другой стороны,  $ha_t \leq a_1 \dots a_{t-1} a_t = g$ . Значит,  $g = ha_t$ , а отсюда элемент  $h = h^* = a_1 \dots a_{t-1}$  есть также представитель смежного класса. Таким образом, элементы  $g_i$  образуют шрейеровскую систему. Если  $U$  — нормальный делитель, то пусть элемент  $a_2 \dots a_t$  находится в классе  $Uf = fU$  с наименьшим элементом  $f$ . Тогда  $f \leq a_2 \dots a_t$ , и элемент  $a_1 f$  принадлежит классу  $a_1 \dots a_t U = gU = Ug$ . Отсюда  $g \leq a_1 f$ . Но мы также имеем неравенство  $a_1 f \leq a_1 a_2 \dots a_t = g$ . Таким образом,  $g = a_1 f$  и  $f = a_2 \dots a_t$ . Следовательно, элементы  $g_i$  образуют двустороннюю шрейеровскую систему. Заметим, что доказанная лемма только гарантирует существование шрейеровской системы представителей левых смежных классов. Но для одной и той же подгруппы возможно существование более чем одной шрейеровской системы представителей для смежных классов.

**Основная теорема. Теорема 7.2.1.** Любая подгруппа свободной группы свободна.

**Доказательство.** Пусть  $F$  — свободная группа, порожденная множеством  $S$ ,  $U$  — некоторая ее подгруппа. Тогда, согласно лемме Шрейера, можно выбрать шрейеровскую систему  $G$  представителей левых смежных классов по  $U$ :

$$F = U \cdot 1 + Ug_2 + \dots + Ug_t + \dots \quad (7.2.2)$$

<sup>1)</sup> „Наименьший“ здесь и в дальнейшем понимается в смысле определенного выше лексикографического порядка. — Прим. ред.

Начнем доказательство с леммы, которая имеет место для произвольной, не обязательно свободной группы  $F$ . Пусть  $F$  — группа, порожденная множеством  $S$ ,  $U$  — подгруппа группы  $F$  и (7.2.2) — левое разложение группы  $F$  по подгруппе  $U$ .

Если элемент  $f$  группы  $F$  принадлежит смежному классу  $Ug$  в (7.2.2), мы определяем функцию  $\Phi(f)$  на группе, полагая  $\Phi(f)=g_i$ . Ясно, что  $\Phi(uf)=\Phi(f)$ , если  $u \in U$ , и что  $\Phi(f)=1$  тогда и только тогда, когда  $f \in U$ .

Пусть  $f=a_1a_2 \dots a_t$ , где  $a_i \in S \cup S^{-1}$ . Полагаем  $f_0=1$ ,  $f_1=a_1$ ,  $f_2=a_1a_2$ , ...,  $f_t=a_1a_2 \dots a_t=f$  и, далее,  $h_0=\Phi(f_0)=1$ ,  $h_1=\Phi(f_1)$ , ...,  $h_t=\Phi(f)$ . Представим элемент  $fh_t^{-1}$  в виде

$$fh_t^{-1}=h_0a_1h_1^{-1} \cdot h_1a_2h_2^{-1} \cdot h_2 \dots h_{t-1}^{-1} \cdot h_{t-1}a_th_t^{-1}. \quad (7.2.3)$$

Если  $f \in U$ , то это выражение равно  $f$ , так как тогда  $h_t=1$ .

Далее, так как  $h_i=\Phi(h_i)=\Phi(f_i)=\Phi(f_{i-1}a_i)=\Phi(h_{i-1}s_a^{\epsilon})$ , где  $a_i=s_a^{\epsilon}$ ,  $\epsilon=\pm 1$ ,  $h_i \in G$ , то в равенстве (7.2.3) нам достаточно знать значения функции  $\Phi$  только для аргументов вида  $gs^{\epsilon}$ , где  $g \in G$ ,  $s^{\epsilon} \in S \cup S^{-1}$ . Положим  $\varphi(gs^{\epsilon})=\Phi(gs^{\epsilon})$ , где функция  $\varphi(f)$  определена только для аргументов вида  $f=gs^{\epsilon}$ .

**Лемма 7.2.2.** *Пусть в произвольной группе  $F$  элемент  $g$  пробегает множество представителей левых смежных классов по подгруппе  $U$  из разложения (7.2.2), элемент  $s$  — множество образующих группы  $F$ , а  $\varphi(gs^{\epsilon})$  есть представитель класса, содержащего элемент  $gs^{\epsilon}$ . Тогда элементы вида  $gs\varphi(gs)^{-1}$  являются образующими подгруппы  $U$ .*

*Доказательство.* Если  $f \in U$ , то  $h_t=1$  и, согласно равенству (7.2.3), элемент  $f$  представляется в виде произведения элементов  $h_{t-1}a_th_t^{-1}$ . Поскольку  $h_i=\Phi(h_{i-1}a_i)$ , элемент  $h_{t-1}a_th_t^{-1}$  имеет вид  $gs^{\epsilon}\varphi(gs^{\epsilon})^{-1}$ , где  $h_{t-1}=g$  и  $a_i=s^{\epsilon}$ , так как  $h_i=\varphi(gs^{\epsilon})$ . Но элемент  $gs^{\epsilon}$  принадлежит смежному классу  $U\varphi(gs^{\epsilon})$ , откуда следует, что для любого элемента  $gs^{\epsilon}$  элемент  $gs^{\epsilon}\varphi(gs^{\epsilon})^{-1} \in U$ . Заметим, что если  $\varphi(g_js^{\epsilon})=g_k$ , то  $\varphi(g_k s^{-\epsilon})=g_j$ . Следовательно, если  $g_js^{\epsilon}\varphi(g_js^{\epsilon})^{-1}=g_js^{\epsilon}g_k^{-1}$ , то обратным к нему элементом будет элемент  $g_k s^{-\epsilon} g_j^{-1}=g_k s^{-\epsilon} \varphi(g_k s^{-\epsilon})^{-1}$ , который имеет такой же вид, но с противоположным показателем степени при  $s$ . Следовательно, элементы вида  $gs\varphi(gs)^{-1}$  порождают подгруппу  $U$ .

**Следствие 7.2.1.** *Если  $F$  — группа с конечным числом образующих и  $U$  — подгруппа конечного индекса, то подгруппа  $U$  также имеет конечное число образующих.*

Это утверждение следует из того, что число возможностей выбора элементов  $g$  и  $s$ , встречающихся в выражениях  $gs\varphi(gs)^{-1}$ , конечно.

В дальнейшем будем предполагать, что  $F$  — свободная группа, причем представители ее смежных классов по  $U$  образуют шрейеровскую систему  $G$ .

Нам понадобятся следующие свойства функции  $\varphi(gs^e)$ :

- 1)  $\varphi(gs^e) \in G$ ,
- 2) если  $gs^e \in G$ , то  $\varphi(gs^e) = gs^e$ ,
- 3)  $\varphi[\varphi(gs^e)s^{-e}] = g$ .

Введем общие обозначения, положив  $v = gs^e\varphi(gs^e)^{-1}$  и  $u = gs\varphi(gs)^{-1}$ . Теперь всякий элемент  $u$  всегда является элементом  $v$  с показателем степени  $+1$ , а элемент  $v$  либо равен некоторому  $u$ , либо некоторому  $u^{-1}$ . При этом, если  $v = g_i s^{-1} \varphi(g_i s^{-1})^{-1}$ , положим  $\varphi(g_i s^{-1}) = g_j$ . Тогда, согласно третьему свойству,  $v^{-1} = g_j s g_i^{-1} = g_j s \varphi(g_j s)^{-1} = u$ ; аналогично  $u^{-1} = v$ .

**Лемма 7.2.3.** Слово  $v = gs^e\varphi(gs^e)^{-1}$  или редуцировано, или равно 1.

**Доказательство.** Пусть  $v = g_j s_a^e \varphi(g_j s_a^e)^{-1} = g_j s_a^e g_k^{-1}$ , где  $g_k = \varphi(g_j s_a^e)$ . Слова  $g_j$  и  $g_k^{-1}$  оба редуцированы. Следовательно, если слово  $v$  допускает сокращение, то или последняя буква слова  $g_j$  равна  $s_a^{-e}$ , или первая буква в  $g_k^{-1}$  равна  $s_a^{-e}$ . Если имеет место первый случай, то  $g_j = a_1 \dots a_{t-1} s_a^{-e}$  — редуцированное представление элемента  $g_j$ . Тогда элемент  $g_j s_a^e = a_1 \dots a_{t-1}$  равен некоторому  $g$ , и, согласно свойству 2 функции  $\varphi$ ,  $g_k = \varphi(g_j s_a^e) = g_j s_a^e$ , поэтому  $v = g_j s_a^e g_k^{-1} = 1$ . Если имеет место второй случай, то аналогично  $g_j = \varphi(g_k s_a^{-e}) = g_k s_a^{-e}$ , и снова  $v = 1$ .

В случае когда  $v = gs^e\varphi(gs^e)^{-1} \neq 1$ , назовем  $s^e$  значимым сомножителем слова  $v$ . Пусть  $v = g_j s_a^e \varphi(g_j s_a^e)^{-1} = g_k s_b^e \varphi(g_k s_b^e)^{-1} \neq 1$ . Если слова  $g_j$  и  $g_k$  имеют равную длину, то  $g_j = g_k$ ,  $s_a = s_b$ , так как элемент  $v$  не допускает сокращения. Если слова  $g_j$  и  $g_k$  разной длины, например  $g_k$  длиннее, то слово  $g_j s_a^e$  как начальная часть слова  $g_k$  само равно некоторому  $g$ , поэтому  $\varphi(g_j s_a^e) = g_j s_a^e$ , откуда  $v = 1$ , что противоречит предположению. Таким образом, элемент  $v \neq 1$  имеет единственное представление в виде  $gs^e\varphi(gs^e)^{-1}$ , и, в частности, его значимый сомножитель однозначно определен.

**Лемма 7.2.4.** При сокращении в произведении  $v_1 v_2$ , где  $v_1 \neq 1$ ,  $v_2 \neq 1$ ,  $v_2 \neq v_1^{-1}$ , значимые сомножители в словах  $v_1$  и  $v_2$  не исчезают.

**Доказательство.** Пусть  $v_1 = g_i s_a^e g_j^{-1}$ ,  $g_j = \varphi(g_i s_a^e)$ ,  $v_2 = g_k s_b^{\eta} g_l^{-1}$ ,  $g_l = \varphi(g_k s_b^{\eta})$ . Слова  $v_1$  и  $v_2$  оба не допускают сокращения, а так как  $v_2 \neq v_1^{-1}$ , равенства  $g_k = g_j$  и  $s_b^{-\eta} = s_a^e$  не

могут оба выполняться. Будем доказывать лемму от противного. Предположим, что сокращению подлежит значимый фактор. Если сокращение достигает сначала  $s_b^\eta$ , то слово  $g_j$  начинается словом  $g_k s_b^{-\eta}$ , откуда  $\varphi(g_k s_b) = g_k s_b$  и  $v_2 = 1$ , что противоречит условию. Аналогично если сокращение достигает сначала  $s_a^e$ , то  $g_j s_a^{-e}$  есть начальная часть слова  $g_k$  и  $v_1 = 1$ , что тоже противоречит условию. Если сокращение достигает  $s_a^e$  и  $s_b^\eta$  одновременно, то тогда  $g_k = g_j$ ,  $s_b^\eta = s_a^{-e}$  и  $v_2 = v_1^{-1}$ , что опять противоречит условию.

Мы можем теперь закончить доказательство основной теоремы.

**Лемма 7.2.5.** *Если  $v_i \neq 1$  ( $i=1, \dots, m$ ),  $v_{i+1} \neq v_i^{-1}$  ( $i=1, \dots, m-1$ ), то произведение  $v_1 v_2 \dots v_m \neq 1$ .*

*Доказательство.* Повторным применением леммы 7.2.4 мы получаем, что сокращение между  $v_i$  и  $v_{i+1}$  не может затронуть ни одного значимого сомножителя. Следовательно, произведение  $v_1 \dots v_m$ , представленное как редуцированное произведение символов, содержит все первоначальные значимые сомножители, а поэтому не равно единице.

Рассмотрим теперь элементы  $u = gs\varphi(gs)^{-1} \neq 1$ . По лемме 7.2.5, все их произведения не равны единице, и все элементы  $u \neq 1$  порождают подгруппу  $U$ . Мы покажем, что  $U$  — свободная подгруппа. Элементы  $u \neq 1$  можно считать свободными образующими подгруппы  $U$ , если убедиться в том, что ни одно из произведений этих элементов, являющихся редуцированными словами в  $U$ , не равно единице, т. е. эти произведения, рассматриваемые как слова, составленные из образующих множества  $S$ , не могут быть редуцированы к единице. Но всякое слово  $v \neq 1$  равно либо  $u$ , либо  $u^{-1}$ . Следовательно, редуцированное слово от элементов  $u \neq 1$  имеет вид  $v_1 v_2 \dots v_m$ ,  $v_i \neq 1$ , где  $v_{i+1} \neq v_i^{-1}$ , как в лемме 7.2.5, и поэтому не равно единице. Итак, мы доказали лемму 7.2.6.

**Лемма 7.2.6.** *Элементы  $u = gs\varphi(gs)^{-1} \neq 1$  составляют систему свободных образующих подгруппы  $U$ .*

Таким образом, мы нашли свободные образующие подгруппы  $U$  и тем самым доказали, что она свободная подгруппа.

Использованное в лемме 7.2.4 понятие значимого сомножителя играет главную роль в приведенном доказательстве теоремы 7.2.1. Мы можем обобщить это понятие, дав независимое определение значимого сомножителя.

Рассмотрим множество  $Y$  такое, что  $Y \cap Y^{-1} = 0$ . Будем говорить, что множество  $Y$  обладает значимыми сомножителями, если

для любого элемента  $y \in Y$  мы можем выбрать из редуцированных представлений элементов  $y$  и  $y^{-1}$

$$\begin{aligned}y &= a_1 \dots a_i \dots a_t, \\y^{-1} &= a_t^{-1} \dots a_i^{-1} \dots a_1^{-1}\end{aligned}$$

такую пару символов  $a_i$  и  $a_i^{-1}$ , что в любом произведении

$$zw, \quad z \neq w^{-1}, \quad z, w \in Y \cup Y^{-1}$$

сокращению не подлежат значимые сомножители слов  $z$  и  $w$ . Другими словами, множество  $Y$  обладает значимыми сомножителями, если для этих сомножителей в множестве  $Y \cup Y^{-1}$  выполняется лемма 7.2.4. Значимые сомножители множества называют *центральными* значимыми сомножителями, если для слова  $u$  нечетной длины значимым сомножителем является его центральный член, а для слова  $u$  четной длины значимым сомножителем является один из двух его центральных членов.

**Теорема 7.2.2.** *Если множество  $Y$  обладает значимыми сомножителями, то оно является системой свободных образующих для порожденной им подгруппы. Если  $G$  — шрейеровская система и каждый ее элемент  $g$  — наикратчайшее слово в смежном классе  $Ug$ , то для элементов  $s$  вида  $s = gs\varphi(gs)^{-1} \neq 1$  множество элементов  $s$  образует множество центральных значимых сомножителей.*

**Доказательство.** По определению значимых сомножителей, для элементов  $v_1, v_2 \in Y \cup Y^{-1}$  имеет место утверждение леммы 7.2.4. Но тогда также выполняется лемма 7.2.5. Следовательно, слово, записываемое в буквах  $u$  и  $u^{-1}$ , может быть равно единице только в том случае, если после сокращения в элементах  $u$  оно становится единичным словом.

Таким образом, множество элементов  $u$  представляет собой систему свободных образующих группы, которую они порождают.

Если  $G$  — шрейеровская система представителей  $g$  смежных классов по подгруппе  $U$  и ни один смежный класс не содержит элементов, более коротких, чем  $g$ , то длины элементов  $g$  и  $\varphi(gs)$  могут отличаться самое большое на 1, так как  $gs \in U\varphi(gs)$ ,  $\varphi(gs)s^{-1} \in Ug$ . Таким образом, символ  $s$ , являющийся значимым сомножителем (лемма 7.2.4), есть центральный значимый сомножитель, так как в слове  $s = gs\varphi(gs)^{-1}$  он находится между двумя словами с разностью длин, равной, самое большое, 1.

Мы можем теперь доказать обращение леммы 7.2.6 и основной теоремы.

**Теорема 7.2.3.** Пусть  $G$  — шрейеровская система в свободной группе  $F$ , порожденной множеством  $S$  свободных образующих, и  $\varphi(h)$  — функция, определенная для аргументов вид  $h = gs^e$ ,  $e = \pm 1$ ,  $g \in G$ ,  $s \in S$ , со следующими свойствами:

- 1)  $\varphi(gs^e) \in G$ ;
- 2) если  $gs^e \in G$ , то  $\varphi(gs^e) = gs^e$ ;
- 3)  $\varphi[\varphi(gs^e)s^{-e}] = g$ .

Тогда множество элементов  $u = gs\varphi(gs)^{-1} \neq 1$  представляет собой систему свободных образующих некоторой подгруппы  $U$  группы  $F$ , а шрейеровская система является при этом множеством представителей левых смежных классов группы  $F$  по подгруппе  $U$ .

**Доказательство.** Введем общее обозначение  $v = gs^e\varphi(gs^e)^{-1}$ . При условиях теоремы выполняются утверждения лемм 7.2.3, 7.2.4 и 7.2.5, так как в их доказательствах были использованы лишь свойства (1) — (3) функции  $\varphi$ . Из леммы 7.2.5 вытекает, что элементы вида  $u = gs\varphi(gs)^{-1} \neq 1$  являются свободными образующими некоторой подгруппы  $U$  группы  $F$ .

Чтобы показать, что шрейеровская система  $G$  представляет собой систему представителей левых смежных классов по подгруппе  $U$ , определим функцию  $\Phi(f)$  для любого слова  $f$  на множеством  $S \cup S^{-1}$ . Пусть

$$f = a_1 a_2 \dots a_t, \quad a_i \in S \cup S^{-1}, \quad i = 1, \dots, t.$$

Положим  $h_0 = 1$ ,

$$h_i = \varphi(h_{i-1} a_i), \quad i = 1, \dots, t,$$

$$h_t = \Phi(f).$$

Легко доказываются следующие основные свойства функции  $\Phi(f)$ :

$$1) \Phi(a_1 \dots a_i a_{i+1} \dots a_t) = \Phi(a_1 \dots a_i s^e s^{-e} a_{i+1} \dots a_t).$$

По определению, элементы  $h_i$ ,  $i = 1, \dots, t$ , принадлежат системе  $G$ . Следовательно, подсчитывая значения правой части, последовательно получаем  $h_i$ ,  $\varphi(h_i s^e)$  и  $\varphi[\varphi(h_i s^e) s^{-e}] = h_i$  в силу свойства (3). Процесс вычисления значений функции  $\Phi$  одинаков для обеих сторон равенства и, следовательно, приводит к одному и тому же результату. Таким образом, значения функции  $\Phi(f)$  одинаковы для любой пары слов, представляющих один и тот же элемент группы  $F$ .

$$2) \Phi(g) = g.$$

Действительно, если  $g = a_1 \dots a_t$  — редуцированное слово, равное элементу из системы  $G$ , то любое слово, являющееся началом слова  $g$ , опять принадлежит системе  $G$ , и в силу свойства (2)  $h_i = a_1 \dots a_i$  ( $i = 1, \dots, t$ ).

3)  $\Phi(f_1 f_2) = \Phi[\Phi(f_1) f_2]$ .

В самом деле, пусть  $f = f_1 f_2$ ,  $f_1 = a_1 \dots a_i$ ,  $f_2 = a_{i+1} \dots a_t$ . Тогда значение  $h_i = \Phi(f_1)$  принадлежит множеству  $G$ , откуда  $\Phi(h_i) = h_i$ . Поэтому при вычислении значения  $\Phi(h_i f_2)$  мы получаем сначала элемент  $h_i$ , а далее элементы, равные соответственно элементам  $a_{i+1}, \dots, a_t$ ,  $h_i = \Phi(f_1 f_2)$ .

4)  $\Phi(gs^e) = \varphi(gs^e)$ .

Из определения функции  $\Phi$  мы имеем  $\Phi(gs^e) = \varphi(\Phi(g)s^e)$ , но ведь  $\Phi(g) = g$ , значит  $\Phi(gs^e) = \varphi(gs^e)$ .

5)  $\Phi[gs^e \varphi(gs^e)^{-1}] = 1$ .

Это свойство вытекает из следующей цепочки равенств:

$$\begin{aligned}\Phi[gs^e \varphi(gs^e)^{-1}] &= \Phi[\Phi(gs^e) \varphi(gs^e)^{-1}] = \\ &= \Phi[\varphi(gs^e) \cdot \varphi(gs^e)^{-1}] = \Phi(1) = 1.\end{aligned}$$

6) Если  $f \in U$ , то  $\Phi(f) = 1$ .

Доказательство получается из повторного применения свойств (3) и (5).

7) Если  $\Phi(f) = g$ , то  $f \in Ug$ .

В очевидном равенстве  $f = a_1 a_2 \dots a_t = (1 \cdot a_1 \cdot h_1^{-1})(h_1 a_2 h_2^{-1}) \dots (h_{t-1} a_t h_t^{-1}) h_t$  каждый элемент  $h_{i-1} a_i h_i^{-1} = gs^e \varphi(gs^e)^{-1} \in U$ ,  $i = 1, \dots, t$ , где  $h_i = \Phi(f) = g$ . В частности, если  $\Phi(f) = 1$ , то  $f \in U$ .

8) Если  $g_i \neq g_j$ , то элементы  $g_i$  и  $g_j$  лежат в разных смежных классах по подгруппе  $U$ .

В противном случае  $g_i = w g_j$ , где  $w \in U$ , откуда  $g_i = \Phi(g) = \Phi[\Phi(w) g_j] = \Phi(g_j) = g_j$ .

Таким образом, мы показали, что все смежные классы  $U_g$  различны и содержат все элементы свободной группы  $F$ . При доказательстве теоремы 7.2.3 мы доказали даже более сильное утверждение. Сформулируем его в виде теоремы.

**Теорема 7.2.4.** Пусть даны шрейеровская система  $G$  и функция  $\varphi(gs^e)$ , определенная в теореме 7.2.3. Этих данных достаточно, чтобы решить вопрос, принадлежит ли произвольный элемент  $f$  подгруппе  $U$ , определяемой системой  $G$  и функцией  $\varphi$ , или нет.

**Доказательство.** Мы можем выразить значение  $\Phi(f)$  через элементы системы  $G$  и функцию  $\varphi$  и воспользоваться признаком, что  $\Phi(f) = 1$  тогда и только тогда, когда  $f \in U$ . Так как функция  $\varphi$  и система  $G$  определяют подгруппу  $U$  столь недвусмысленным образом, мы будем считать, что функция  $\varphi$  и система  $G$  представляют подгруппу  $U$ , и говорить, что  $U = U[G, \varphi(gs^e)]$  есть *стандартное представление* подгруппы  $U$ .

Здесь, естественно, возникают два вопроса:

1) Как связаны между собой различные стандартные представления одной и той же группы?

2) Сколько подгрупп можно представить через данную шрейеровскую систему?

Мы последовательно ответим на оба вопросы.

**Теорема 7.2.5.** Подгруппы  $U_1 = U_1[G_1, \varphi_1(gs^e)]$  и  $U_2 = U_2[G_2, \varphi_2(gs^e)]$  совпадают тогда и только тогда, когда существует такое взаимно однозначное соответствие  $g^1 \leftrightarrow g^2$  (включая  $1 \leftrightarrow 1$ ) между шрейеровскими системами  $G_1$  и  $G_2$ , что из  $g^1 \leftrightarrow g^2$  вытекает  $\varphi_1(g^1s^e) \leftrightarrow \varphi_2(g^2s^e)$  при любом  $s^e$ .

**Доказательство.** Если  $U_1 = U_2 = U$ , то каждый смежный класс по подгруппе  $U$  имеет по представителю из  $G_1$  и  $G_2$ . Таким образом, если  $Ug^1 = Ug^2$ , то ясно, что соответствие  $g^1 \leftrightarrow g^2$ , включая  $1 \leftrightarrow 1$ , взаимно однозначно. Поскольку элементы  $g^1s^e$  и  $g^2s^e$  лежат в одном смежном классе, имеет место равенство  $\varphi_1(g^1s^e) = \varphi_2(g^2s^e)$ .

Обратно, пусть дано взаимно однозначное соответствие  $g^1 \leftrightarrow g^2$  (включая  $1 \leftrightarrow 1$ ), влекущее за собой  $\varphi_1(g^1s^e) \leftrightarrow \varphi_2(g^2s^e)$ . Тогда для любого аргумента  $f$  имеет место соответствие  $\Phi_1(f) \leftrightarrow \Phi_2(f)$ , в частности, равенство  $\Phi_1(f) = 1$  выполняется тогда и только тогда, когда  $\Phi_2(f) = 1$ . Но последнее означает, что подгруппы  $U_1$  и  $U_2$  состоят из одних и тех же элементов  $f$  и, следовательно, совпадают. Более того, индукцией по длине слова  $g^1$  можно доказать, что  $Ug^1 = Ug^2$ .

Прежде чем отвечать на второй вопрос, мы отметим несколько свойств функции  $\varphi$ . Отображения  $\pi(s) : g \rightarrow \varphi(gs)$  и  $\pi(s^{-1}) : g \rightarrow \varphi(gs^{-1})$  для всех  $g \in G$  и некоторого фиксированного образующего элемента  $s$  переводят множество  $G$  в себя. В силу свойства (3) функции  $\varphi$  произведения  $\pi(s)\pi(s^{-1})$  и  $\pi(s^{-1})\pi(s)$  оба равны единице. Поэтому отображения  $\pi(s)$  и  $\pi(s^{-1})$  являются подстановками (взаимно однозначными отображениями); при этом они взаимно обратны друг к другу. Кроме того, в силу свойства (2) некоторые значения функции  $\varphi$  обязательно зависят от системы  $G$ , но не зависят от подгруппы  $U$ . Пусть снова образующий элемент  $s$  фиксирован, а элемент  $g \in G$  произволен. Множество элементов  $g$  можно разбить следующим образом на два класса  $C(s)$  и  $C^*(s)$ :

$g \in C(s)$  тогда и только тогда, когда  $gs \in G$ ;

$g \in C^*(s)$  тогда и только тогда, когда  $gs \notin G$ .

Пусть  $N(s)$  — мощность класса  $C(s)$ , а  $M(s)$  — мощность класса  $C^*(s)$ . Тогда

$$N(s) + M(s) = N,$$

где  $N$  — мощность множества  $G$ . Аналогично определяем

$g \in C(s^{-1})$  тогда и только тогда, когда  $gs^{-1} \in G$ ,

$g \in C^*(s^{-1})$  тогда и только тогда, когда  $gs^{-1} \notin G$ ;

при этом  $N(s^{-1})$  — мощность множества  $C(s^{-1})$ ,  $M(s^{-1})$  — мощность множества  $C^*(s^{-1})$ . Снова имеем

$$N(s^{-1}) + M(s^{-1}) = N.$$

Если теперь элементы  $g_i$  и  $g_j$  таковы, что  $g_i s = g_j$ , т. е.  $g_j s^{-1} = g_i$ , то  $g_i \in C(s)$  и  $g_j \in C(s^{-1})$ . Этим устанавливается взаимно однозначное соответствие между множествами  $C(s)$  и  $C(s^{-1})$ , поэтому

$$N(s) = N(s^{-1}).$$

Если число  $N$  конечно, то отсюда следует, что

$$M(s) = M(s^{-1}).$$

Если же  $N$  бесконечно, последнее равенство может оказаться неверным для произвольной шрейеровской системы. Например, возьмем шрейеровскую систему  $1, s, s^2, \dots, s^l, \dots$ . Для нее  $M(s) = 1, M(s^{-1}) = 0$ . С другой стороны, если функция  $\varphi$  существует для данной шрейеровской системы  $G$ , то отображение  $\pi(s)$  переводит множество  $C(s)$  в множество  $C(s^{-1})$  и, будучи подстановкой, также отображает множество  $C^*(s)$  в множество  $C^*(s^{-1})$ . Следовательно, равенство  $M(s) = M(s^{-1})$  является необходимым условием существования функции  $\varphi$ .

**Теорема 7.2.6.** Пусть  $G$  — такая шрейеровская система, что  $M(s) = M(s^{-1})$  для любого образующего  $s$ . Тогда можно указать функцию  $\varphi(gs^e)$ , обладающую следующими тремя свойствами:

- 1) элемент  $\varphi(gs^e)$  принадлежит системе  $G$ ;
- 2) если  $gs^e \in G$ , то  $\varphi(gs^e) = gs^e$ ;
- 3)  $\varphi[\varphi(gs^e)s^{-e}] = g$ .

Для фиксированного  $s$  функцию  $\varphi$  в самом общем виде можно определить следующим образом:

а)  $\varphi(gs) = gs$ , если элемент  $gs$  принадлежит  $G$ ;

б) если элемент  $gs$  не принадлежит системе  $G$ , то значения  $\varphi(gs)$  выбираем произвольно, но так, чтобы отображение  $\pi(s) : g \rightarrow \varphi(gs)$  было взаимно однозначным на множестве  $G$ ;

в) определив значения  $\varphi(gs)$  для всех элементов  $g \in G$ , определяем значения  $\varphi(gs^{-1})$  так, чтобы отображение  $\pi(s^{-1}) : g \rightarrow \varphi(gs^{-1})$  было подстановкой, обратной к  $\pi(s)$ .

**Доказательство.** Если для любого образующего  $s$  имеет место равенство  $M(s) = M(s^{-1})$  на  $G$ , то теорема не только утверждает существование  $\varphi(gs^e)$ , но также описывает наиболее общий метод построения такой функции, если только сформули-

рованное определение законно. Поэтому мы должны доказать законность конструкции. Для данного образующего элемента  $s$ , очевидно, имеем:

1) элемент  $\varphi(gs)$  принадлежит множеству  $G$ ;

2) если элемент  $gs$  принадлежит  $G$ , то  $\varphi(gs) = gs$ .

Если для некоторого элемента  $g_i$  имеем  $g_i s = g_j \in G$ , то положим  $\varphi(g_i s) = g_j$ , где  $g_j s^{-1} = g_i$ . Тогда соответствие  $g \rightarrow \varphi(gs)$  отображает класс  $C(s)$  на класс  $C(s^{-1})$ . Оставшиеся  $M(s)$  элементов  $g$  системы  $G$  должны быть отображены на оставшиеся  $M(s^{-1})$  элементов  $g$ . Так как  $M(s) = M(s^{-1})$ , то возможно взаимно однозначное отображение  $g \leftrightarrow g'$  множества  $C^*(s)$  на множество  $C^*(s^{-1})$ . Мы полагаем  $g' = \varphi(gs)$ . Тогда соответствие  $\pi(s) : g \rightarrow \varphi(gs)$  есть подстановка, отображающая класс  $C(s)$  на класс  $C(s^{-1})$  и класс  $C^*(s)$  на класс  $C^*(s^{-1})$ .  $\pi(s)$  — подстановка, и, следовательно, если определить отображение  $\pi(s^{-1}) : g \rightarrow \varphi(gs^{-1})$  как обратное к отображению  $\pi(s)$ , мы получим значения  $\varphi(gs^{-1})$ . Ясно, что элементы  $\varphi(gs^{-1})$  принадлежат множеству  $G$ . Кроме того, так как подстановка  $\pi(s)$  отображает множество  $C(s)$  на  $C(s^{-1})$ , выполняется следующее свойство:

3) если элемент  $gs^{-1} \in G$ , то  $\varphi(gs^{-1}) = gs^{-1}$ .

Таким образом, свойства (1) и (2) имеют место для любого элемента  $g \in G$  при фиксированном  $s$  или  $s^{-1}$ . Наконец, свойство (3)  $\varphi[\varphi(gs^e)s^{-e}] = g$  имеет место, так как подстановки  $\pi(s)$  и  $\pi(s^{-1})$  взаимно обратны.

В теоремах 7.2.5 и 7.2.6 подстановки  $\pi(s)$  играли главную роль. Если  $g = a_1 a_2 \dots a_t$ , то подстановка  $\pi(a_1) \pi(a_2) \dots \pi(a_t)$  переводит 1 в элемент  $g$ , и, следовательно, подстановки  $\pi(s)$  порождают группу, транзитивную на множестве  $G$ . Как мы сейчас докажем, уже одни эти подстановки однозначно определяют подгруппу  $U$ .

**Теорема 7.2.7.** Пусть  $F$  — свободная группа на множестве  $S$  свободных образующих, каждому символу  $s \in S$  соответствует одна подстановка  $\pi(s)$  на множестве символов  $1, y_2, \dots, y_i, \dots$  и группа, порожденная подстановками  $\pi(s)$ , транзитивна на этом множестве символов. Каждому элементу  $f$  из группы  $F$ , где  $f = a_1 a_2 \dots a_t$ , поставим в соответствие подстановку  $\pi(f) = \pi(a_1) \pi(a_2) \dots \pi(a_t)$ . Тогда такие элементы  $f$ , для которых подстановки  $\pi(f)$  не перемещают 1, образуют подгруппу  $U$ . Если  $g_1 = 1, g_2, \dots, g_i, \dots$  — некоторая шрейеровская система представителей левых смежных классов по подгруппе  $U$ , мы можем отождествить слова  $g_i$  с символами  $y_i$ , считая, что  $g_i \rightarrow y_i$ , если подстановка  $\pi(g_i)$  переводит 1 в  $y_i$ . Тогда подстановки  $\pi(s)$  на множестве символов  $y_i$  подобны описанным в теоремах 7.2.5 и 7.2.6 подстановкам  $\pi(s)$  на множестве элементов  $g_i$ .

*Доказательство.* Ясно, что элементы  $f$ , которым соответствуют подстановки  $\pi(f)$ , оставляющие на месте 1, образуют подгруппу  $U$  группы  $F$ . Согласно теореме 5.3.1, мы можем рассматривать подстановки  $\pi(f)$  как представление группы  $F$  множеством смежных классов по подгруппе  $U$ , заменяя 1 подгруппой  $U$ , а символы  $y_i$  — соответствующими левыми смежными классами по подгруппе  $U$ . Отсюда следует, что каждый символ  $y_i$  однозначно соответствует некоторому левому смежному классу  $Ug_i$ , для которого подстановка  $\pi(g_i)$  отображает 1 в  $y_i$ . При таком представлении подстановка  $\pi(s)$  переводит смежный класс  $Ug$  в смежный класс  $Ugs$ , или, что то же,  $U\varphi(gs)$ . Так, если мы заменяем смежный класс  $Ug_i$  его представителем  $g_i$ , подстановка  $\pi(s)$  совпадает с подстановкой  $\pi(s)$  из теорем 7.2.5 и 7.2.6; этим мы установили подобие исходной группы подстановок на символах  $y_i$  с группой подстановок на шрейеровской системе  $G$ .

Для подгруппы  $U$  конечного индекса в свободной группе с конечным числом образующих мы можем указать несколько точных значений для числа образующих подгруппы  $U$  и для суммы их длин.

**Теорема 7.2.8.** Пусть  $U = U[G, \varphi(gs^e)]$  — подгруппа конечного индекса  $n$  свободной группы  $F$ , с  $r$  свободными образующими  $s_1, s_2, \dots, s_r$ . Тогда:

- 1) подгруппа  $U$  имеет  $1 + n(r - 1)$  свободных образующих;
- 2) если  $L$ -сумма длин элементов шрейеровской системы  $G$ , то сумма длин свободных образующих  $u = gs\varphi(gs)^{-1} \neq 1$  подгруппы  $U$  равна  $K = (2L + n)r - 2L$ .

*Доказательство.* Мы уже доказывали, что множество свободных образующих подгруппы  $U$  состоит из элементов

$$u_{ia} = g_i s_a \varphi(g_i s_a)^{-1}, \quad i = 1, \dots, n; \quad a = 1, \dots, r,$$

которые не равны единице. Более того, по лемме 7.2.3 элементы  $u_{ia}$  или не допускают сокращений, или равны единице. Отсюда

$$\sum_{i=1}^n \{L(g_i) + L(s_a) + L[\varphi(g_i s_a)]\} = 2L + n,$$

так как при фиксированном  $s_a$  элементы  $\varphi(g_i s_a)$  суть некоторая перестановка элементов  $g_i$ . Следовательно, до сокращения мы имеем  $nr$  образующих  $u_{ia}$  общей длины  $r(2L + n)$ . Из этих двух чисел мы должны вычесть соответственно число элементов  $u_{ia}$ , равных единице, и длины  $L(g_i) + L(s_a) + L(g_i s_a)$  этих элементов. Когда элемент  $u_{ia}$  равен единице? Слова  $g_i, s_a$  и  $\varphi(g_i s_a)^{-1}$  сокращению не поддаются. Значит, сокращение должно допускать их произведение, но, в силу леммы 7.2.3,  $u_{ia} = 1$  тогда и только

тогда, когда  $s_a$  сокращается с  $g_i$  или с  $\varphi(g_i s_a)^{-1}$ . В первом случае  $g_i$  оканчивается символом  $s_a^{-1}$ ,  $g_i = g_j s_a^{-1}$ , где элемент  $g_j \in G$  не редуцируется. Во втором случае элемент  $\varphi(g_i s_a) = g_k$  кончается символом  $s_a$ , и тогда  $g_k = g s_a$ . Таким образом, для данного символа  $s_a$  число элементов  $u_{ia}$ , равных единице, равно числу элементов из  $G$ , оканчивающихся на  $s_a$  или  $s_a^{-1}$ . Но каждый элемент  $g \in G$ , кроме  $g = 1$ , оканчивается некоторым символом  $s_a$  или  $s_a^{-1}$ , а поэтому учитывается точно один раз в этом процессе. Следовательно, всего существует  $n - 1$  элементов  $u_{ia}$ , равных единице, и, значит, свободных образующих подгруппы  $U$  всего  $nr - (n - 1) = n(r - 1) + 1$ . Теперь подсчитаем сумму их длин. Во-первых, если  $g_i = g_j s_a^{-1}$ , то  $\varphi(g_i s_a) = g_j$ , и потому  $L(g_i) + L(s_a) + L[\varphi(g_i s_a)] = 2L(g_i) = 2L(g_j s_a^{-1})$ . Во-вторых, если  $g_i s_a = g_k$ , то  $L(g_i) + L(s_a) + L[\varphi(g_i s_a)] = 2L(g_i s_a)$ . Таким образом, при данном  $s_a$  в слове  $u_{ia} = 1$  мы посчитали дважды длину каждого элемента  $g$ , оканчивающегося на  $s_a$  или  $s_a^{-1}$ . Следовательно, для всех  $s_a$  мы дважды посчитали в словах  $u_{ia} = 1$  длину каждого элемента  $g$ , кроме  $g = 1$ . Но  $L(1) = 0$ , и потому, если вычесть точно  $2L$ , то получим, что общая длина свободных образующих подгруппы  $U$  равна  $(2L + n)r - 2L$ .

Наконец, применяя теорему 7.2.7, мы можем указать рекуррентную формулу для числа подгрупп индекса  $n$  в группе  $F_r$ .

**Теорема 7.2.9.** Число  $N_{n,r}$  подгрупп индекса  $n$  в группе  $F_r$  рекуррентно выражается так:  $N_{1,r} = 1$ ,

$$N_{n,r} = n(n!)^{r-1} - \sum_{i=1}^{n-1} (n-i)!^{r-1} N_{i,r}.$$

**Доказательство.** Равенство  $N_{1,r} = 1$  просто означает, что группа  $F_r$  является единственной подгруппой индекса 1.

Зададим  $r$  подстановок  $P_1, \dots, P_r$  на символах  $1, x_2, \dots, x_n$ . Вообще говоря, эти подстановки не порождают транзитивную группу на всех этих символах. Введем в рассмотрение область транзитивности, содержащую символ 1. Пусть она состоит из символов  $1, b_2, \dots, b_t$ . Оставив в стороне остальные буквы  $x$ , мы можем рассматривать  $\pi(s_1), \dots, \pi(s_r)$ , как подстановки на символах  $1, b_2, \dots, b_t$ . Согласно теореме 7.2.7, они вполне определяют одну-единственную подгруппу индекса  $t$ . Оставшиеся  $n-t$  символов могут переставляться подстановками  $P_1, \dots, P_r, [(n-t)!]^r$  различными способами. Кроме того, если мы заменим символы  $1, b_2, \dots, b_t$  любым другим набором символов  $1, c_2, \dots, c_t$  и допустим, что оставшиеся  $n-t$  символов могут переставляться как угодно, то мы придем к той же самой

подгруппе индекса  $t$ . Таким образом, с одной и той же подгруппой индекса  $t$  ассоциируются

$(n-1)(n-2)\dots(n-t+1)[(n-t)!]^r = (n-1)![(n-t)!]^{r-1}$  различных наборов подстановок  $P_1, \dots, P_r$ . Следовательно,

$$\sum_{t=1}^n (n-1)![(n-t)!]^{r-1} N_{t,r} = (n!)^r,$$

где  $(n!)^r$  — это число всех возможных подстановок  $P_1, \dots, P_r$ , соответствующих подгруппе определенного индекса. Выделяя в полученной сумме последнее слагаемое и деля на  $(n-1)!$ , мы получаем искомую рекурсивную формулу.

### 7.3. Свободные образующие подгруппы свободных групп.

#### Метод Нильсена

В предыдущем параграфе для изучения свойств подгруппы  $U$  свободной группы  $F$  рассматривались смежные классы по подгруппе  $U$  в группе  $F$ . В этом параграфе мы будем непосредственно оперировать с элементами подгруппы  $U$ .

Пусть  $A = \{a_i\}$  — семейство элементов свободной группы  $F$ , где индекс  $i$  пробегает множество индексов  $I$ . Предположим, что множество  $A$  состоит из свободных образующих группы, которую оно порождает. Последнюю мы обозначим через  $[A]$ . Если элемент  $f \in [A]$ , то через  $L_A(f)$  мы обозначим длину редуцированного слова  $f$  в символах  $a_i$  и  $a_i^{-1}$ .

Пусть  $X$  — множество свободных образующих свободной группы  $F$ . Мы будем говорить, что множество  $A$  элементов группы  $F$  обладает *свойством Нильсена* по отношению к множеству свободных образующих  $X$  в том и только в том случае, если

1)  $A \cap A^{-1} = 0$  ( $A^{-1}$  — множество элементов вида  $a^{-1}$ , где  $a \in A$ ),

2) для  $a, b \in A \cup A^{-1}$  из неравенства  $L_X(ab) < L_X(a)$  следует  $b = a^{-1}$ ,

3) для  $a, b, c \in A \cup A^{-1}$  из неравенства  $L_X(abc) \leq L_X(a) - L_X(b) + L_X(c)$  следует, что или  $b = a^{-1}$ , или  $b = c^{-1}$ .

**Теорема 7.3.1.** *Если множество  $A$  обладает свойством Нильсена по отношению к множеству  $X$  свободных образующих группы  $F$ , то оно состоит из свободных образующих подгруппы  $[A]$ , которую оно порождает. Свойство Нильсена эквивалентно существованию центральных значимых сомножителей в множестве  $A$ .*

**Доказательство.** Достаточно доказать, что свойство Нильсена эквивалентно существованию центральных значимых сомножите-

лей, так как по теореме 7.2.2 отсюда будет следовать, что множество  $A$  состоит из свободных образующих подгруппы  $[A]$ .

Предположим, что множество  $A$  обладает свойством Нильсена. Тогда в силу свойства 2), если  $b \neq a^{-1}$ ,  $L_X(ab) \geq L_X(a)$  и  $L_X(b^{-1}a^{-1}) \geq L_X(b^{-1})$ , откуда  $L_X(ab) \geq L_X(b)$ . Если бы при редуцировании слова  $ab$  более половины одного сомножителя скажем  $b$ , сократилось с  $a$ , мы бы имели  $a = uv^{-1}$ ,  $b = vw$ .  $L_X(v) > L_X(w)$  и  $L_X(ab) = L_X(uw) < L_X(u) + L_X(v) = L_X(a)$ . Но этого случиться не может, и при редуцировании слова  $ab$  сокращается, самое большое, половина слова  $a$  (или  $b$ ). Следовательно для элемента нечетной длины его центральный член можно рассматривать как значимый сомножитель. Если элемент  $b$  четной длины, возможно, его первая половина  $v$  сократится при умножении  $a$  и  $b$  при  $b \neq a^{-1}$ . Если бы также и вторая половина слова  $b$  сократилась при редуцировании слова  $bc$  при  $b \neq c^{-1}$ , то мы бы имели  $a = uv^{-1}$ ,  $b = vw$ ,  $c = w^{-1}z$  и  $L_X(abc) = L_X(uz) \leq L_X(u) + L_X(z) = L_X(a) - L_X(b) + L_X(c)$ , что противоречит третьему требованию свойства Нильсена. Следовательно, ни одна из половин слова  $b$  (ни  $v$ , ни  $w$ ) не может сократиться ни в каком произведении, и поэтому один из центральных членов слова  $b$  можно взять в качестве центрального значимого сомножителя. Таким образом, из свойства Нильсена следует существование центральных значимых сомножителей.

Обратно, если для множества  $A$  ( $A \cap A^{-1} = 0$ ) центральные значимые сомножители существуют, то в слове  $ab$ , самое большое, половина слова  $b$  сокращается с частью слова  $a$  такой же длины при  $b \neq a^{-1}$ , поэтому верно неравенство  $L_X(ab) \geq L_X(a) + L_X(b) - \frac{2 \cdot 1}{2} L_X(b) = L_X(a)$ , удовлетворяющее второму требованию свойства Нильсена. Далее, в произведении  $abc$  при  $b \neq a^{-1}$ ,  $b \neq c^{-1}$  сокращение между  $a$  и  $b$  и между  $b$  и  $c$  прекращается, не доходя до значимого сомножителя слова  $b$ ; поэтому  $L_X(abc) > L_X(a) + L_X(b) + L_X(c) - 2L_X(b)$ , т. е. третье требование свойства Нильсена выполнено. Нетрудно доказать, что одно лишь это третье требование эквивалентно существованию значимых сомножителей. Задавшись словом  $b$ , возьмем в качестве  $a \neq b^{-1}$  элемент, который сокращает наибольшее число членов слова  $b$  при умножении  $a$  на  $b$ , а в качестве элемента  $c \neq b^{-1}$  возьмем элемент, который сокращает справа наибольшее число членов слова  $b$  при умножении  $b$  на  $c$ . Третье требование утверждает, что не все члены слова  $b$  сокращаются, и любой оставшийся член может быть выбран в качестве значащего сомножителя для  $b$ .

**Теорема 7.3.2.** Рассматривается конечное множество  $B$  элементов  $\beta_1, \dots, \beta_m$  в свободной группе  $F$  с данным мно-

жеством  $X$  свободных образующих. Утверждается, что конечным числом шагов следующих трех типов:

1° вычеркивание тех  $\beta_i$ , которые равны 1,

2° замена  $\beta_i$  элементом  $\beta_i^{-1}$ ,

3° замена  $\beta_j$  элементом  $\beta_i\beta_j$ ,  $i \neq j$ ,

мы можем перейти от множества  $B$  к другому множеству  $A: a_1, \dots, a_n, n \leq m$ , такому, что оно порождает ту же самую подгруппу, что и  $B$ , и обладает свойством Нильсена по отношению к множеству  $X$ . Следовательно, множество  $A$  есть система свободных образующих для подгруппы  $[A] = [B]$ .

*Доказательство.* Легко видеть, что любая замена описанного типа переводит множество в другое множество, порождающее ту же самую подгруппу. Первый тип изменения уменьшает число элементов, а второй и третий — оставляет его без изменения. Заметим, что, комбинируя преобразования типов 2° и 3°, можно заменить элемент  $\beta_j$  элементом  $\beta_i^\varepsilon\beta_j^\eta$  или  $\beta_j^\eta\beta_i^\varepsilon$ ,  $\varepsilon = \pm 1$ ,  $\eta = \pm 1$ , и оставить все другие элементы из  $B$  неизменными.

Если два элемента из  $B$  равны или взаимно обратны, то мы можем один из них заменить единицей, а затем эту единицу вычеркнуть. Эта операция уменьшает количество элементов  $\beta_i$ ; следовательно, она не может применяться более чем  $m$  раз. Если при  $a, b \in B \cup B^{-1}, b \neq a^{-1}$ , мы имеем  $L_X(ab) < L_X(a)$ , то  $b \neq a$ , так как всегда  $L_X(a^2) > L_X(a)$ . В этом случае мы можем заменить элемент  $\beta = a^\varepsilon$  словом  $ab$  и тем самым уменьшить сумму длин элементов  $\beta_i$ . Число подобных преобразований конечно. Поэтому конечным числом шагов можно достигнуть выполнения условий (1) и (2) свойства Нильсена. Труднее удовлетворить третьему требованию свойства Нильсена.

Независимо от того, бесконечно множество  $X$  или нет, множество  $Y$  тех образующих из  $X$ , которые встречаются в записи элементов множества  $B$ , безусловно, конечно. Упорядочим элементы группы  $F$ , порожденные множеством  $Y$ , по длине; для слов одинаковой длины установим произвольный фиксированный порядок. Число элементов заданной длины конечно. Следовательно, при указанном порядке любой элемент имеет только конечное число предшествующих.

Если слово  $\beta$  имеет четную длину  $2k$ , запишем его в виде  $\beta = \gamma\delta^{-1}$ , где каждое из слов  $\gamma$  и  $\delta$  имеет длину  $k$ . Если  $\beta \neq 1$ , то  $\delta \neq \gamma$ . Так как  $\beta^{-1} = \delta\gamma^{-1}$ , то, заменяя в случае необходимости  $\beta$  на  $\beta^{-1}$ , мы всегда можем достигнуть того, чтобы в определенном порядке первая часть слова предшествовала второй. Если  $\beta_i = \gamma\delta^{-1}$  и  $\beta_j = \delta\zeta$ , мы заменяем  $\beta_j$  словом  $\beta_i\beta_j = \gamma\zeta$ . Ана-

логично, если  $\beta_k = w\delta^{-1}$ , мы заменяем  $\beta_k$  словом  $\beta_k\beta_i^{-1} = w\gamma^{-1}$ . Следовательно, если  $\beta_i = \gamma\delta^{-1}$ , то мы можем преобразовать элементы  $\beta$  так, чтобы никакой элемент  $\beta$ , отличный от  $\beta_i$ , не начинался со слова  $\delta$  или не кончался словом  $\delta^{-1}$ . Так как мы при этом заменяем некоторые члены  $\delta$  другими членами  $\gamma$  той же длины, но предшествующими первым в установленном порядке, то указанный процесс оборвется через конечное число шагов. Важно отметить, что если мы начинаем с кратчайшего слова  $\beta$  четной длины, а затем преобразуем все более и более длинные слова четной длины, то процесс оборвется через конечное число шагов. Действительно, оперируя с элементами  $\beta_i$  равной длины, мы последовательно заменяем первую половину слова предшествующими словами, и, таким образом, процесс обрывается через конечное число шагов. Действуя над элементами  $\beta$  большей длины, чем длина слова  $\beta_i = \gamma\delta^{-1}$ , мы не встретим слов, начинающихся со слова  $\delta$  и оканчивающихся словом  $\delta^{-1}$ . Естественно, если на некотором этапе нарушается или условие  $A \cap A^{-1} = 0$ , или условие  $L_X(ab) \geq L_X(a)$ , то мы делаем подходящее преобразование, либо уменьшая число элементов  $\beta$ , либо уменьшая их совокупную длину, а затем вновь переходим к замене половин слов, которые не изменяют ни числа слов  $\beta$ , ни их совокупной длины. Этот процесс оборвется после конечного числа шагов, после чего мы получим множество  $A$  элементов  $\alpha_1, \dots, \alpha_n$ ,  $n \leq m$ . Утверждается, что множество  $A$  обладает свойством Нильсена по отношению к системе свободных образующих  $X$ . Требования  $A \cap A^{-1} = 0$  и  $L_X(ab) \geq L_X(a)$ , при  $b \neq a^{-1}$ ,  $a, b \in A \cup A^{-1}$ , конечно, выполняются, так как в противном случае мы могли бы уменьшить или число, или совокупную длину слов  $\beta_i$ . Рассмотрим теперь произведение  $abc$ , где  $b \neq a^{-1}$ ,  $b \neq c^{-1}$ . Если элемент  $b$  нечетной длины  $2k+1$ , то, самое большое,  $k$  первых членов слова  $b$  сократятся со словом  $a$  и, самое большое,  $k$  последних членов слова  $b$  сократятся со словом  $c$ ; поэтому справедливо неравенство  $L_X(abc) > L_X(a) - L_X(b) + L_X(c)$ . Если слово  $b$  четной длины, то оно имеет вид  $\gamma\delta^{-1}$  или  $\delta\gamma^{-1}$ , причем при установленной выше упорядоченности  $\gamma$  предшествует слову  $\delta$ . Так как второе требование выполняется, не более половины слова  $b$  сокращается с  $a$  и не более половины с  $c$ . Но или слово  $a$  не оканчивается словом  $\delta^{-1}$ , или слово  $c$  не начинается с  $\delta$ , а потому половина слова  $b$  (или  $\delta$ , или  $\delta^{-1}$ ) полностью не может сократиться; таким образом, само слово  $b$  не может полностью сократиться, откуда и следует неравенство  $L_X(abc) > L_X(a) - L_X(b) + L_X(c)$ , доказывающее третье требование свойства Нильсена для множества  $A$ .

**Теорема 7.3.3.** Две свободные группы изоморфны тогда и только тогда, когда они имеют равномощные системы свободных образующих. Свободная группа  $F_r$  с конечным числом  $r$  образующих свободно порождается произвольным множеством из  $r$  элементов, порождающим эту группу.

**Доказательство.** Пусть  $F_X$  и  $F_Y$  — свободные группы с множествами свободных образующих  $X$  и  $Y$  соответственно.

Если множества  $X$  и  $Y$  имеют одинаковую мощность, то существует взаимно однозначное соответствие между элементами множеств  $X$  и  $Y$ , которое может быть продолжено до взаимно однозначного соответствия между группами  $F_X$  и  $F_Y$ , которое, очевидно, является изоморфизмом.

Обратно, предположим, что группы  $F_X$  и  $F_Y$  изоморфны. Тогда эти группы имеют равное количество подгрупп индекса 2. Любая подгруппа индекса 2 является ядром гомоморфизма на группу порядка 2. Такой гомоморфизм однозначно определяется множеством образующих, отображаемых в единицу. Итак, число подгрупп индекса 2 свободной группы  $F_Z$  на множестве  $Z$  свободных образующих равно числу непустых подмножеств множества  $Z$ . Это число несчетно, если множество  $Z$  бесконечно, и равно  $2^r - 1$ , если  $Z$  конечно и состоит из  $r$  элементов. Таким образом, если свободные группы  $F_X$  и  $F_Y$  изоморфны, то отсюда следует, что множества  $X$  и  $Y$  или оба бесконечны, или оба конечны, причем в последнем случае состоят из равного числа элементов. Если же  $X$  и  $Y$  бесконечны, то группы  $F_X$  и  $F_Y$  имеют те же мощности, что и множества  $X$  и  $Y$  соответственно. Но так как группы  $F_X$  и  $F_Y$  равномощны, множества  $X$  и  $Y$  также равномощны.

Предположим теперь, что свободная группа  $F_r$  на множестве  $X$ :  $x_1, x_2, \dots, x_r$ , порождается также элементами  $\beta_1, \beta_2, \dots, \beta_r$ . Тогда, согласно теореме 7.3.2, после конечного числа преобразований вида  $1^\circ, 2^\circ, 3^\circ$  множества  $\beta_1, \beta_2, \dots, \beta_r$ , мы получим систему свободных образующих  $\alpha_1, \dots, \alpha_s$ ,  $s \leq r$ , группы  $F_r$ . Но тогда имеет место равенство  $s = r$ , и поэтому ни одно преобразование типа  $1^\circ$  не было использовано.

Легко убедиться непосредственно в следующем. Пусть множество  $B$  переходит в множество  $B'$  с помощью преобразований типа  $2^\circ, 3^\circ$ . Тогда, если  $B$  состоит из свободных образующих, тем же свойством обладает и  $B'$ , и обратно. Следовательно, так как множество  $\alpha_1, \dots, \alpha_r$  — система свободных образующих группы  $F_r$ , то и элементы  $\beta_1, \beta_2, \dots, \beta_r$  — свободные образующие группы  $F_r$ .

Этим теорема доказана. Но можно точнее охарактеризовать множество элементов  $\alpha_1, \alpha_2, \dots, \alpha_r$ . Для элементов  $\alpha_i$  выполняется свойство Нильсена и поэтому они обладают центральными значимыми сомножителями (теорема 7.3.1). Кроме того, для

каждого элемента  $x_i (i = 1, \dots, r)$  имеем  $x_i = \gamma_1 \dots \gamma_m$ , где каждый элемент  $\gamma$  совпадает или с некоторым  $\alpha_i$ , или с некоторым  $\alpha_i^{-1}$ , причем  $\gamma_i \gamma_{i+1} \neq 1$ . Произведение элементов  $\gamma_i$  в сокращенном виде содержит все центральные сомножители. Значит, произведение состоит только из одного множителя  $\gamma$ , совпадающего с  $x_i$ . Таким образом,  $x_i$  равен или  $\alpha_j$ , или  $\alpha_j^{-1}$ . Следовательно, если мы будем дальше применять преобразования второго типа, множество  $\alpha_1, \dots, \alpha_r$  совпадет с множеством  $x_1, \dots, x_r$ , с точностью до порядка следования. Таким образом, мы знаем, опять-таки с точностью до порядка следования, как получить произвольное множество свободных образующих  $\beta_1, \dots, \beta_r$  группы  $F_r$  из элементов  $x_1, \dots, x_r$ . А это значит, что мы знаем автоморфизмы группы  $F_r$ .

**Теорема 7.3.4.** *Все автоморфизмы свободной группы  $F_r$  с конечным множеством  $X: x_1, x_2, \dots, x_r$  свободных образующих порождаются следующими автоморфизмами:*

- 1)  $P_{ij}: x_i \rightarrow x_j, x_j \rightarrow x_i, x_k \rightarrow x_k, k \neq i, j;$
- 2)  $V_i: x_i \rightarrow x_i^{-1}, x_j \rightarrow x_j, j \neq i;$
- 3)  $W_{ij}: x_j \rightarrow x_i x_j, i \neq j, x_k \rightarrow x_k, k \neq j,$

где числа  $i \neq j$  независимо друг от друга пробегают значения  $1, \dots, r$ .

**Доказательство.** Ясно, что каждое из этих отображений определяет автоморфизм группы  $F_r$ , так как оно переводит множество  $X$  в множество из  $r$  элементов, которые снова порождают группу  $F_r$ . Мы должны показать, что любой автоморфизм группы  $F_r$  является произведением автоморфизмов, указанных в формулировке теоремы. Как уже было доказано выше, в наиболее общей форме автоморфизм группы  $F_r$  получается заменой множества  $X: x_1, \dots, x_r$  множеством образующих  $B: \beta_1, \dots, \beta_r$ , причем множество  $B$  получается из множества  $X$  конечным числом преобразований:

$$B = B_1, B_2, \dots, B_{N-1}, B_N = X,$$

где множество  $B_i$  получается из  $B_{i+1}$  преобразованием типа  $2^\circ$  или  $3^\circ$  (см. теорему 7.2.3) при  $i = 1, \dots, N - 2$ , а переход от  $B_{N-1}$  к  $B_N$  осуществляется подстановкой множества  $X$  и, следовательно, может быть представлен как произведение транспозиций  $P_{ij}$  (см. § 5.4). Таким образом, каждый из переходов от  $B_{i+1}$  к  $B_i$ ,  $i = 1, \dots, N - 2$ , оказывается или автоморфизмом типа  $V_i$ , или автоморфизмом вида  $W_{ij}$ , заданным на множестве элементов  $B_{i+1}$ . Мы должны доказать, что эти автоморфизмы могут быть представлены в виде произведений автоморфизмов  $V_i$  и  $W_{ij}$ , заданных на множестве  $X$ .

Пусть

$$Y : y_1, \dots, y_r,$$

$$Z : z_1, \dots, z_r,$$

$$W : w_1, \dots, w_r$$

— три множества свободных образующих группы  $F_r$ , где

$$1) \quad z_i = y_i^{-1}, \quad z_j = y_j, \quad j \neq i$$

или

$$2) \quad z_j = y_i y_j, \quad z_k = y_k, \quad k \neq j$$

и

$$3) \quad w_m = z_m^{-1}, \quad w_n = z_n, \quad n \neq m$$

или

$$4) \quad w_n = z_m z_n, \quad w_t = z_t, \quad t \neq n.$$

Здесь переходы  $Y$  в  $Z$  и  $Z$  в  $W$  суть автоморфизмы типов  $V_i$  или  $W_{ij}$ . Мы должны доказать, что автоморфизмы (3) и (4) можно представить в виде произведения автоморфизмов типа  $V_i$  и  $W_{ij}$  на множестве  $Y$ . Для этого нужно рассмотреть несколько сравнительно простых случаев. Мы рассмотрим только два наиболее трудных.

Пусть даны отображения (2)  $z_j = y_i y_j$  и (3)  $w_m = z_m^{-1}$  при  $m = j$ . Мы должны выразить автоморфизм (3), отображающий элемент  $y_i y_j$  в элемент  $y_j^{-1} y_i^{-1}$  и оставляющий на месте  $y_k$ , если  $k \neq j$ . Это отображение эквивалентно преобразованию, при котором элемент  $y_j$  переходит в элемент  $y_i^{-1} y_j^{-1} y_i^{-1}$ , а все остальные элементы из  $Y$  переходят в себя. Но такое преобразование является произведением следующих отображений:

$$y_j \rightarrow y_i^{-1} y_j \rightarrow y_i^{-1} y_j^{-1} \rightarrow y_i^{-1} y_j^{-1} y_i^{-1}, \text{ т. е.}$$

$$W_{ij}^{-1}(y) V_j(y) W_{ij}(y).$$

Рассмотрим второй случай. Пусть мы имеем отображения (2)  $z_j = y_i y_j$  и (4)  $w_n = z_m z_n$  при  $m = j, n = i$ . Здесь автоморфизм (4) заменяет  $z_j = y_i y_j$  элементом  $y_i y_j$ , а  $z_i = y_i$  — элементом  $y_i y_j y_i$ , причем остальные элементы  $z_k = y_k$  остаются на месте. Но это преобразование совпадает с отображением

$$y_i \rightarrow y_i y_j y_i,$$

$$y_j \rightarrow y_i^{-1}.$$

Но это отображение равно произведению  $W_{ij}^{-1}(y) W_{ji}(y) W_{ij}(y)$ , так как при этом

$$y_i \rightarrow y_i \rightarrow y_j y_i \rightarrow y_i y_j y_i,$$

$$y_j \rightarrow y_i^{-1} y_j \rightarrow y_i^{-1} \rightarrow y_i^{-1}.$$

Следовательно, любой автоморфизм типа  $V_i$  или  $W_{ij}$  на множестве  $Z$  может быть выражен в виде произведения тех же типов автоморфизмов на множестве  $Y$ . Теперь мы можем закончить доказательство теоремы индукцией по  $N$ . Предположим по индукции, что замена  $B_{N-2}$  множеством  $B_1$  есть произведение автоморфизмов типов  $V_i$  и  $W_{ij}$  на множестве  $B_{N-2}$ . Принимая  $B_{N-1}$  в качестве  $Y$ , а  $B_{N-2}$  в качестве  $Z$ , мы сможем выразить отображение  $B_{N-2}$  на  $B_1$  через произведение автоморфизмов типов  $V_i$  и  $W_{ij}$  на множестве  $B_{N-1}$ . Отображение  $B_{N-1}$  на  $B_{N-2}$  есть автоморфизм того же типа на множестве  $B_{N-1}$ . Следовательно, замена  $B_{N-1}$  множеством  $B_1$  есть произведение автоморфизмов типов  $V_i$  и  $W_{ij}$  на множестве  $B_{N-1}$ . Кроме того, эти автоморфизмы тех же типов на множестве  $X$ , так как  $B_{N-1}$  есть просто перестановка множества  $X$ . Таким образом, теорема доказана.

Если множество  $A$  обладает свойством Нильсена по отношению к системе свободных образующих  $X$  группы  $F_X$ , то множество  $A$  можно рассматривать с различных точек зрения как „минимальное“ множество образующих подгруппы  $[A]$ .

**Теорема 7.3.5.** *Если множество  $A$  обладает свойством Нильсена по отношению к  $X$  и*

$$f = a_1 a_2 \dots a_t, \quad a_i \in A \cup A^{-1}, \quad a_i a_{i+1} \neq 1,$$

то

$$L_X(f) \geq \frac{1}{2} L_X(a_1) + t - 2 + \frac{1}{2} L_X(a_t)$$

и

$$L_X(f) \geq L_X(a_i \dots a_j), \quad 1 \leq i \leq j \leq t.$$

Более того, если множество  $X$  конечно и элементы из множества  $A$  упорядочены по длинам  $\alpha_1, \alpha_2, \dots, \alpha_r, \dots, \beta_1, \beta_2, \dots, \beta_s$  — любое другое множество свободных образующих подгруппы  $[A]$ , также упорядоченное по длинам, то

$$L_X(\beta_n) \geq L_X(\alpha_n), \quad n = 1, 2, \dots$$

**Доказательство.** В слове  $f = a_1 a_2 \dots a_t$  каждый элемент  $a_i$  имеет центральный сомножитель, который не сокращается при редуцировании слова  $f$ . Следовательно, в редуцированном представлении элемента  $f$  останутся, по меньшей мере, первая половина слова  $a_1$ , центральные сомножители слов  $a_2, \dots, a_{t-1}$  и вторая половина слова  $a_t$ , т. е.  $L_X(f) \geq \frac{1}{2} L_X(a_1) + t - 2 + \frac{1}{2} L_X(a_t)$ . При редуцировании слова  $a_1 a_2 \dots a_{t-1} a_t$  сокращению между редуцированной формой слова  $a_1 \dots a_{t-1}$  и  $a_t$  подлежат  $k$  членов слова  $a_{t-1}$  и  $k$  членов слова  $a_t$ , где  $k \leq \frac{1}{2} L_X(a_{t-1})$ ,  $k \leq L_X(a_t)$ , так как центральные сомножители не сокращаются. Таким обра-

зом,  $L_X(f) = L_X(a_1 \dots a_{t-1}) + L_X(a_t) - 2k$ . Но  $2k \leq L_X(a_t)$ , откуда  $L_X(a_1 \dots a_t) \geq L_X(a_1 \dots a_{t-1})$ . Аналогично  $L_X(a_1 \dots a_t) \geq L_X(a_2 \dots a_t)$ . Повторяя эти рассуждения, получаем  $L_X(a_1 \dots a_t) \geq L_X(a_t \dots a_j)$ .

Если множество  $X$  конечно, существует только конечное число элементов данной длины, и поэтому, записывая элементы множества  $A$  в порядке возрастания длин, мы сможем исчерпать все множество  $A$ . Пусть  $\alpha_1, \alpha_2, \dots, \alpha_i, \dots$  — элементы множества  $A$ , упорядоченные по возрастанию длин, а  $\beta_1, \dots, \beta_r, \dots$  — другое множество образующих, упорядоченное аналогичным образом. Пусть  $\beta_1(\alpha), \dots, \beta_n(\alpha)$  — выражения первых  $n$  элементов  $\beta_i$  через свободные образующие  $\alpha_i \in A$ , и пусть  $\alpha_r$  — последний среди  $\alpha_i$  элемент, встречающийся в этих выражениях. Утверждается, что  $r \geq n$ . Предположим обратное, т. е. что  $r < n$ . Тогда по модулю коммутатора  $K$  подгруппы  $[A]$  мы имеем

$$\begin{aligned}\beta_1 &\equiv \alpha_1^{e_{11}} \dots \alpha_r^{e_{1r}} \pmod{K}, \\ &\dots \dots \dots \dots \dots \dots \\ \beta_n &\equiv \alpha_1^{e_{n1}} \dots \alpha_r^{e_{nr}} \pmod{K}.\end{aligned}$$

При  $r < n$  обязательно существуют<sup>1)</sup> целые числа  $u_1, \dots, u_n$ , не все равные нулю, но такие, что

$$\begin{aligned}e_{11}u_1 + \dots + e_{n1}u_n &= 0, \\ &\dots \dots \dots \dots \dots \\ e_{1r}u_1 + \dots + e_{nr}u_n &= 0.\end{aligned}$$

Но тогда  $\beta_1^{u_1} \dots \beta_n^{u_n} \in K$ , где числа  $u_1, \dots, u_n$  не все равны нулю, а это противоречит утверждению, что элементы  $\beta_i$  образуют систему свободных образующих подгруппы  $[A]$ . Итак,  $r \geq n$ . Пусть элемент  $\alpha_r$  действительно встречается в слове  $\beta_j(\alpha)$  при некотором  $j \leq n$ . Тогда, как доказано в первой части теоремы,  $L_X(\beta_j) \geq L_X(\alpha_r)$ . Но  $L_X(\beta_n) \geq L_X(\beta_j)$  и  $L_X(\alpha_r) \geq L_X(\alpha_n)$ , так как  $r \geq n$ . Поэтому  $L_X(\beta_n) \geq L_X(\alpha_n)$ .

## Упражнения

- Пусть  $F$  — свободная группа, порожденная символами  $x$  и  $y$ . Показать, что вполне характеристическая подгруппа группы  $F$ , содержащая элемент  $x^2uy^{-1}$ , совпадает с группой  $F$  или имеет в ней индекс 9.
- Пусть  $F$  — свободная группа с двумя образующими. Найти все ее подгруппы индекса 3.

<sup>1)</sup> Биркгоф и Маклейн [1], стр. 48. См. в § 9.2 о свойствах коммутатора подгруппы.

3. Пусть  $F$  — свободная группа, порожденная элементами  $a, b$  и  $c$ . Найти множество свободных образующих подгруппы индекса 8, порожденной квадратами всех элементов группы  $F$ .

4. Пусть  $A_1, A_2, \dots, A_m$  — элементы свободной группы, данные в редуцированной форме, ни один из которых не равен единице, и такие, что  $A_1 A_2 \dots A_m = 1$ . Показать, что для некоторого  $i$  слово  $A_i$  полностью сокращается в произведении  $A_{i-1} A_i A_{i+1}$ .

5. Дано редуцированное слово  $g = a_1 a_2 \dots a_t \neq 1$  в свободной группе  $F$ . Показать, что  $F$  имеет подгруппу  $H$  индекса  $t+1$ , не содержащую элемента  $g$ . (Указание: выбрать следующие представители смежных классов по  $H$ : 1,  $a_1, a_1 a_2, \dots, a_1 a_2 \dots a_t$ .)

6. Показать, что если  $g = g(x_1, \dots, x_r)$  есть некоторое слово от образующих  $x_1, \dots, x_r$ , не являющееся единицей в свободной группе, порожденной свободными образующими  $x_1, \dots, x_r$ , то существует некоторая конечная группа  $G$ , порожденная элементами  $x_1, \dots, x_r$ , в которой  $g$  не является единицей (см. упр. 5 этой главы и упр. 1 к гл. 5).

## Г л а в а 8

### СТРУКТУРЫ И КОМПОЗИЦИОННЫЕ РЯДЫ

#### 8.1. Частично упорядоченные множества

ОПРЕДЕЛЕНИЕ. Частично упорядоченным множеством называется такое множество  $S$ , в котором для некоторых пар элементов  $a$  и  $b$  определено такое отношение  $a \sqsupseteq b$  (читается „ $a$  содержит  $b$ “), что:

- P1.  $a \sqsupseteq a$ ;
- P2. Если  $a \sqsupseteq b$  и  $b \sqsupseteq c$ , то  $a \sqsupseteq c$ ;
- P3. Если  $a \sqsupseteq b$  и  $b \sqsupseteq a$ , то  $a = b$ .

ОПРЕДЕЛЕНИЕ. Верхней гранью подмножества  $T$  частично упорядоченного множества  $S$  называется элемент  $x \in S$ , такой, что  $x \sqsupseteq t$  для любого элемента  $t$  из  $T$ . Аналогично нижняя грань подмножества  $T$  — это такой элемент  $y \in S$ , что  $t \sqsupseteq y$  для любого элемента  $t$  из  $T$ .

ОПРЕДЕЛЕНИЕ. Наименьшая верхняя грань (н. в. г.) подмножества  $T$  частично упорядоченного множества  $S$  есть элемент  $x$ , обладающий следующими двумя свойствами:

- 1)  $x$  есть верхняя грань множества  $T$ ,

- 2) если  $z$  — любая верхняя грань множества  $T$ , то  $z \sqsupseteq x$ .

Аналогично наибольшая нижняя грань (н. н. г.) подмножества  $T$  есть элемент  $y$ , обладающий следующими двумя свойствами:

- 1)  $y$  есть нижняя грань множества  $T$ ,

- 2) если  $z$  — любая нижняя грань для  $T$ , то  $y \sqsupseteq z$ .

Вообще говоря, подмножество  $T$  не обязательно имеет наименьшую верхнюю грань или наибольшую нижнюю грань. Но если  $T$  обладает наименьшей верхней гранью  $x$ , то она единственна, так как, по определению, две наименьшие верхние грани должны содержать друг друга, а значит (Р3) должны совпадать. То же можно сказать о наибольшей нижней грани.

Если частично упорядоченное множество  $S$  также обладает свойством

P4: для любой пары элементов  $a$  и  $b$  имеет место либо  $a \sqsupseteq b$ , либо  $b \sqsupseteq a$ , то мы говорим, что  $S$  есть просто упорядоченное множество, или цепь.

Иногда вместо  $a \sqsupseteq b$  мы будем писать  $b \sqsubseteq a$ . Мы будем писать  $a \sqsupset b$ , если  $a \sqsupseteq b$ , но  $a \neq b$ .  $b \subset a$  равносильно  $a \sqsupset b$ . Введем еще

одно полезное обозначение  $a > b$  (читается „ $a$  покрывает  $b$ “), которое означает, что из отношений  $a \supset b$  и  $a \sqsupseteq x \sqsupseteq b$  вытекает, что или  $x = a$ , или  $x = b$ .  $b < a$  означает то же, что  $a > b$ .

**ПРИМЕР.** Пусть  $S$  — множество элементов  $a, b, c, d, e, f$  с отношениями включения, указанными на диаграмме;  $x \sqsupseteq y$ , если

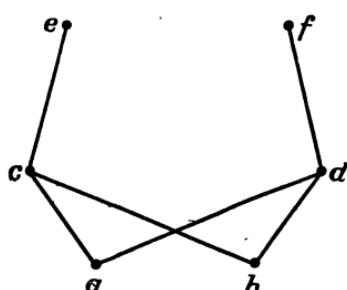


Рис. 3. Частично упорядоченное множество.

точка  $x$  расположена выше  $y$  и эти точки соединены. Здесь подмножество, состоящее из элементов  $c$  и  $d$ , не имеет верхней грани. Оно имеет две нижние грани ( $a$  и  $b$ ), но ни одной наибольшей нижней грани.

## 8.2. Структуры

**ОПРЕДЕЛЕНИЕ.** Структурой будем называть частично упорядоченное множество, в котором каждая пара элементов  $a$  и  $b$  обладает наименьшей верхней гранью, называемой также объединением  $a \cup b$ , и наибольшей нижней гранью, или пересечением  $a \cap b$ .

Так как каждый из элементов  $a \cup b$  и  $a \cap b$  определяется однозначно, объединение и пересечение — вполне определенные бинарные операции в структуре.

**ТЕОРЕМА 8.2.1.** В структуре выполняются следующие законы:

- L1.  $x \cap x = x$ ,  $x \cup x = x$ . Идемпотентность.
- L2.  $x \cap y = y \cap x$ ,  $x \cup y = y \cup x$ . Коммутативность.
- L3.  $x \cap (y \cap z) = (x \cap y) \cap z$ ,  
 $x \cup (y \cup z) = (x \cup y) \cup z$ . Ассоциативность.
- L4.  $x \cap (x \cup y) = x$ ,  $x \cup (x \cap y) = x$ . Закон поглощения.

**Доказательство.** Законы L1, L2, L4 непосредственно вытекают из определений н. в. г. и н. н. г. Докажем свойство L3. Положим  $y \cap z = u$ ,  $x \cap u = w$ . Здесь  $w$  есть нижняя грань элементов  $x$  и  $u$ , а значит, и элементов  $x$ ,  $y$  и  $z$ . Но любая нижняя грань  $x$ ,  $y$  и  $z$  содержится в  $u$ , а значит, и в пересечении  $x \cap u = w$ . Поэтому  $w$  оказывается н. н. г. элементов  $x$ ,  $y$  и  $z$ . Аналогично  $(x \cap y) \cap z$  есть н. н. г. элементов  $x$ ,  $y$  и  $z$ , откуда следует, что  $x \cap (y \cap z) = (x \cap y) \cap z$ . Подобным же образом каждый из элементов  $x \cup (y \cup z)$  и  $(x \cup y) \cup z$  является н. в. г. элементов  $x$ ,  $y$  и  $z$ .

**ТЕОРЕМА 8.2.2.** Законы L1—L4 вполне характеризуют структуру.

**Доказательство.** Во всякой системе, удовлетворяющей законам L1—L4, равенство  $x \cap y = y$  имеет место в том и только

в том случае, если  $x \cup y = x$ . Если мы в такой системе введем отношение включения, положив  $x \sqsupseteq y$  тогда и только тогда, когда  $x \sqcap y = y$ , то эта система окажется частично упорядоченным множеством относительно так введенного отношения включения. Действительно, из равенства  $a \sqcap a = a$  вытекает свойство Р1. Если  $a \sqcap b = b$  и  $b \sqcap c = c$ , то  $a \sqcap c = a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c = b \sqcap c = c$ , что означает выполнение требования Р2. Если  $a \sqcap b = b$  и  $b \sqcap a = a$ , то  $a = b$ , так как  $a \sqcap b = b \sqcap a$ , т. е. требование Р3 также удовлетворено. Таким образом, при таком определении включения наша система является частично упорядоченным множеством. Далее,  $a \sqcap (a \sqcap b) = (a \sqcap a) \sqcap b = a \sqcap b$  и  $b \sqcap (a \sqcap b) = a \sqcap b$ , откуда элемент  $a \sqcap b$  есть нижняя грань элементов  $a$  и  $b$ . Но если  $a \sqsupseteq x$  и  $b \sqsupseteq x$ , то  $a \sqcap x = x$  и  $b \sqcap x = x$ , откуда  $(a \sqcap b) \sqcap x = a \sqcap (b \sqcap x) = a \sqcap x = x$ , следовательно,  $a \sqcap b$  есть н. н. г. элементов  $a$  и  $b$ . Аналогично, если  $y \sqsupseteq a$  и  $y \sqsupseteq b$ , то  $a \cup y = y$  и  $b \cup y = y$ , откуда  $y = (a \cup b) \cup y$ . Отсюда получаем, что  $a \cup b$  не только верхняя грань, но и наименьшая верхняя грань для  $a$  и  $b$ .

Некоторые структуры обладают другими свойствами. Здесь мы укажем те из них, которые нам понадобятся.

**ОПРЕДЕЛЕНИЕ.** Говорят, что структура  $L_1$  изоморфна структуре  $L_2$ , если существует взаимно однозначное соответствие  $x_i \leftrightarrow y_i$  между элементами  $x_i$  из  $L_1$  и  $y_i$  из  $L_2$ , такое, что  $x_i \sqsubset x_j \leftrightarrow y_i \sqsubset y_j$  и  $x_i \cup x_j \leftrightarrow y_i \cup y_j$ .

**ОПРЕДЕЛЕНИЕ.** Структура  $L$  называется полной, если любое ее подмножество имеет наибольшую нижнюю грань и наименьшую верхнюю грань.

Если множество всех элементов структуры  $L$  обладает наименьшей верхней гранью, то она называется *единичным элементом*, если же она обладает наибольшей нижней гранью, она называется *нулевым элементом*.

**ОПРЕДЕЛЕНИЕ.** Структура  $L$  называется дистрибутивной, если в ней выполняется свойство

$$\text{Д1. } a \sqcap (b \cup c) = (a \sqcap b) \cup (a \sqcap c).$$

**ОПРЕДЕЛЕНИЕ.** Структура  $L$  называется модулярной<sup>1)</sup>, если в ней выполняется свойство

$$\text{М. Если } a \sqsupseteq b, \text{ то } a \sqcap (b \cup c) = b \cup (a \sqcap c).$$

Говорят, что структура или, более обще, частично упорядоченное множество, удовлетворяет *условию минимальности*, если любая убывающая цепь  $a_1 \supset a_2 \supset a_3 \supset \dots$  обрывается после конечного числа шагов, и *условию максимальности*, если любая возрастающая цепь  $a_1 \subset a_2 \subset a_3 \subset \dots$  обрывается после конечного числа шагов.

<sup>1)</sup> Модулярные структуры называются также дедекиндовыми структурами.

**ОПРЕДЕЛЕНИЕ.** В структуре  $L$  конечная цепь  $x = x_0 \sqsupseteq x_1 \sqsupseteq \dots \sqsupseteq x_d = y$  называется максимальной, если  $x_i > x_{i+1}$  при  $i = 0, 1, \dots, d-1$ , т. е.  $x = x_0 > x_1 > \dots > x_d = y$ . Число  $d$  называется ее длиной.

**ОПРЕДЕЛЕНИЕ.** Элемент  $x$  структуры  $L$  имеет конечную размерность  $d$  (обозначается  $d(x)$ ), если структура  $L$  имеет нулевой элемент 0, любая цепь от  $x$  до нуля конечна и  $d$  — длина самой длинной максимальной цепи от  $x$  до 0.

### 8.3. Модулярные и полумодулярные структуры

В любой структуре множество таких элементов  $x$ , что  $a \sqsupseteq \sqsupseteq x \sqsupseteq b$ , есть подструктура, называемая частным  $a/b$ . Частные  $a \cup b/b$  и  $a/a \cap b$  называются перспективными друг другу. Если частное  $a_i/b_i$  перспективно частному  $a_{i+1}/b_{i+1}$  при  $i = 1, \dots, n-1$ , то мы говорим, что частное  $a_1/b_1$  проективно частному  $a_n/b_n$ .

**Теорема 8.3.1.** В модулярной структуре перспективные частные изоморфны.

**Доказательство.** Пусть  $a \cup b/b$  и  $a/a \cap b$  — перспективные частные в модулярной структуре. Для любого элемента  $x$  из  $a/a \cap b$  определяем элемент  $y(x) = x \cup b$ . Для любого элемента  $y$  из  $a \cup b/b$  определяем элемент  $x(y) = y \cap a$ . Первое отображение переводит элементы частного  $a/a \cap b$  в элементы частного  $a \cup b/b$ , а второе отображает  $a \cup b/b$  в  $a/a \cap b$ . Если  $x \in a/a \cap b$ , то  $x[y(x)] = (x \cup b) \cap a$ . Поскольку  $a \sqsupseteq x$ , мы можем применить модулярный закон  $a \cap (x \cup b) = x \cup (a \cap b) = x$  в силу того, что  $x \sqsupseteq a \cap b$ . Следовательно,  $x[y(x)] = x$ . Аналогично, если  $y \in a \cup b/b$ , получаем  $y[x(y)] = y$ . Таким образом, отображения  $x \rightarrow y(x)$  и  $y \rightarrow x(y)$  есть взаимно однозначные и взаимно обратные отображения двух рассматриваемых частных друг на друга. Кроме того, это соответствие сохраняет операции пересечения и объединения. Действительно, для элементов  $x_1$  и  $x_2$  из частного  $a/a \cap b$  имеем  $y(x_1 \cup x_2) = (x_1 \cup x_2) \cup b = (x_1 \cup b) \cup (x_2 \cup b) = y(x_1) \cup y(x_2)$ . Далее,  $x_1 = x(y_1)$ ,  $x_2 = x(y_2)$ , откуда  $x_1 \cap x_2 = x(y_1) \cap x(y_2) = (y_1 \cap a) \cap (y_2 \cap a) = y_1 \cap y_2 \cap a = x(y_1 \cap y_2)$ . А теперь  $y(x_1 \cap x_2) = y[x(y_1 \cap y_2)] = y_1 \cap y_2 = y(x_1) \cap y(x_2)$ . Итак, обе операции сохраняются при отображении  $x \rightarrow y(x)$ . Из того, что соответствие однозначно, следует, что операции сохраняются также при отображении  $y \rightarrow x(y)$ . Это можно было бы проверить и непосредственно вполне аналогичным образом.

**Следствие 8.3.1.** В модулярной структуре проективные частные изоморфны.

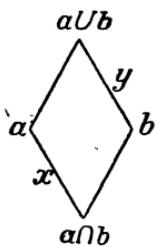


Рис. 4. Перспективные частные.

**Теорема 8.3.2.** Если в модулярной структуре элемент  $x$  имеет конечную размерность  $d(x)$ , то все максимальные цепи от  $x$  до 0 имеют одну и ту же длину.

**Доказательство** будем вести индукцией по числу  $d(x)$ . Если  $d(x)=1$ , то  $x > 0$  — единственная цепь от  $x$  до 0. Пусть  $x=x_0>x_1>\dots>x_d=0$  — одна максимальная цепь от  $x$  до 0, а  $x=y_0>y_1>\dots>y_s=0$  — другая. Если  $y_1=x_1$ , то, по предположению индукции, максимальные цепи, начиная с  $x_1$  и  $y_1$ , имеют одну и ту же длину  $d-1$ , откуда  $s-1=d-1$ , т. е.  $s=d$ . Если  $x_1 \neq y_1$ , то положим  $z_2=x_1 \sqcap y_1$ . Тогда частные  $x/x_1$  и  $y_1/z_2$ ,  $x/y_1$  и  $x_2/z_2$  попарно перспективны. Но частные  $x/x_1$  и  $x/y_1$  не имеют промежуточных элементов, поэтому  $x_1 > z_2$ ,  $y_1 > z_2$ . Так как все максимальные цепи от  $x_1$  до 0 имеют длину  $d-1$ , все максимальные цепи от  $z_2$  до 0 имеют длину  $d-2$ . Следовательно, цепь от  $y_1$  через  $z_2$  к 0 имеет длину  $d-1$ , а теперь по индукции мы заключаем, что такую же длину имеет цепь  $y_1 > y_2 > \dots > 0$ . Следовательно, цепь  $x=y_0>y_1>\dots>y_s=0$  имеет длину  $d=s$ .

В качестве следствия из этой теоремы мы получаем, что условие Жордана — Дедекинда для цепей имеет место в модулярных структурах.

**Условие Жордана — Дедекинда для цепей.** Все конечные максимальные цепи между двумя элементами имеют одинаковую длину.

Если  $a \sqsupseteq b$ , мы можем взять элемент  $b$  в качестве нулевого элемента в структуре  $a/b$  и применить предыдущую теорему.

В модулярной структуре размерность подчинена важному соотношению.

**Теорема 8.3.3.** В структуре, в которой все элементы имеют конечную размерность, соотношение

$$d(x) + d(y) = d(x \sqcup y) + d(x \sqcap y)$$

имеет место тогда и только тогда, когда структура модулярна.

**Доказательство.** В модулярной структуре частные  $x \sqcup y/x$  и  $y/x \sqcap y$  изоморфны. Длина максимальной конечной цепи каждой из этих подструктур соответственно равна  $d(x \sqcup y) - d(x)$  и  $d(y) - d(x \sqcap y)$ . Но из изоморфизма следует, что эти числа равны, откуда мы имеем

$$d(x) + d(y) = d(x \sqcup y) + d(x \sqcap y). \quad (\text{M})$$

Обратно, пусть имеет место равенство (M). Пусть  $A \sqsupseteq B$ ; рассмотрим выражения  $A \sqcap (B \sqcup C)$  и  $B \sqcup (A \sqcap C)$ . Выписываем

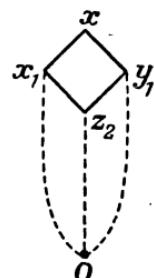


Рис. 5.  
Условие  
Жордана —  
Дедекинда.

последовательно такие включения:

$$\begin{aligned}B &\subseteq A, \\B &\subseteq B \cup C, \\B &\subseteq A \cap (B \cup C), \\A \cap C &\subseteq A, \\A \cap C &\subseteq C \subseteq B \cup C, \\A \cap C &\subseteq A \cap (B \cup C), \\B \cup (A \cap C) &\subseteq A \cap (B \cup C).\end{aligned}$$

Теперь, чтобы показать равенство  $B \cup (A \cap C) = A \cap (B \cup C)$ , достаточно, используя равенство (M), показать равенство соответствующих размерностей:

$$\begin{aligned}d[B \cup (A \cap C)] &= d(B) + d(A \cap C) - d(B \cap A \cap C) = \\&= d(B) + d(A \cap C) - d(B \cap C) = \\&= d(B \cup C) - d(C) + d(A \cap C) = \\&= d(B \cup C) + d(A) - d(A \cup C) = \\&= d(A) + d(B \cup C) - d(A \cup B \cup C) = \\&= d[A \cap (B \cup C)].\end{aligned}$$

Следовательно,  $A \cap (B \cup C) = B \cup (A \cap C)$ , и модулярность структуры доказана.

С помощью отношения покрытия  $A > B$  можно определить два свойства полумодулярности, которые выполняются в некоторых структурах.

**ОПРЕДЕЛЕНИЕ.** Нижняя полумодулярность. *Структура называется нижне полумодулярной, если из включений  $A > B$  и  $A > C$  ( $B \neq C$ ) следует, что  $B > B \cap C$  и  $C > B \cap C$ .*

Верхняя полумодулярность. *Структура называется верхне полумодулярной, если из включений  $A < B$  и  $A < C$  ( $B \neq C$ ) следует, что  $B < B \cup C$  и  $C < B \cup C$ .*

Ясно, что эти два вида полумодулярности дуальны друг другу и в силу теоремы 8.3.1 являются следствиями свойства модулярности. Мы покажем, что структура конечной размерности со свойствами нижней и верхней полумодулярности модулярна.

**ТЕОРЕМА 8.3.4.** *Если в полумодулярной структуре  $L$   $A \sqsupseteq B$  и существует конечная максимальная цепь между  $A$  и  $B$ , то все конечные максимальные цепи между  $A$  и  $B$  имеют равную длину.*

*Доказательство* в основном совпадает с доказательством теоремы 8.3.2. Пусть  $L$  — нижне полумодулярная структура. Если

существует максимальная цепь длины один между  $A$  и  $B$ , то  $A > B$  и других целей от  $A$  до  $B$  не существует. Проведем индукцию по длине максимальной цепи между  $A$  и  $B$ . Предположим, что

$$A = A_0 > A_1 > A_2 > \dots > A_r = B$$

— максимальная цепь длины  $r$  от  $A$  до  $B$ , причем теорема верна для цепей, имеющих длину, меньшую чем  $r$ . Пусть

$$A = U_0 > U_1 > U_2 > \dots > U_s = B$$

— другая максимальная цепь от  $A$  до  $B$ . Тогда, если  $U_1 = A_1$ , максимальная цепь от  $A_1 = U_1$  до  $B$ , по предположению индукции, должна иметь длину  $r - 1$ , и теорема доказана. Если же  $U_1 \neq A_1$ , то в силу нижней полумодулярности

$$A_1 > U_1 \cap A_1, \quad U_1 > U_1 \cap A_1.$$

Обозначив  $U_1 \cap A_1 = V_2$ , мы получим следующие цепи:

$$A = A_0 > A_1 > A_2 > \dots > A_r = B,$$

$$A = A_0 > A_1 > V_2 > \dots > V_m = B,$$

$$A = U_0 > U_1 > V_2 > \dots > V_m = B,$$

$$A = U_0 > U_1 > U_2 > \dots > U_s = B.$$

По предположению индукции длины цепей от  $A_1$  до  $B$  равны, т. е.  $m = r$ , следовательно, первые две цепи имеют равные длины. Вторая и третья имеют длину  $m$ , а по предположению индукции длины цепей от  $U_1$  до  $B$  равны, откуда  $m = s$ . Следовательно, все четыре цепи имеют одну и ту же длину, и теорема доказана для нижне полумодулярных структур. Дуальные рассуждения приводят к тому же результату для верхне полумодулярных структур.

Из этой теоремы видно, что в полумодулярной структуре размерность  $d(A)$  элемента  $A$  — это длина всех максимальных цепей между  $A$  и нулевым элементом 0. В конечномерных полумодулярных структурах размерности элементов связаны неравенствами.

**Теорема 8.3.5.** *Пусть  $L$  — структура конечной размерности. Если она верхне полумодулярна, то (1)  $d(X \cup Y) + d(X \cap Y) \leq d(X) + d(Y)$ . Если же она нижне полумодулярна, то (2)  $d(X \cup Y) + d(X \cap Y) \geq d(X) + d(Y)$ . Обратно, из неравенства (1) следует верхняя полумодулярность, но из (2) нижняя полумодулярность не следует.*

**Доказательство.** В силу теоремы 8.3.4, если структура  $L$  полумодулярна и если  $R \supset S$ , то  $d(R) - d(S)$  — длина максимальной цепи между  $R$  и  $S$ , так как все максимальные цепи от нулевого элемента до  $R$  имеют одинаковую длину. Поэтому размер-

ность элемента  $R$  равна длине максимальной цепи от  $R$  до нуля, содержащей элемент  $S$ . Мы используем этот факт в доказательстве.

Пусть  $L$  — верхне полумодулярная структура. Условимся писать  $A \geq B$ , если  $A = B$  или  $A > B$  (читается: „ $A$ , самое большое, покрывает  $B$ “). Если теперь

$$X \cap Y = U_0 \leq U_1 \leq U_2 \leq \dots \leq U_m = X,$$

$$X \cap Y = V_0 \leq V_1 \leq V_2 \leq \dots \leq V_n = Y,$$

то мы утверждаем, что  $U_i \cup V_j \geq U_{i-1} \cup V_j$  и  $U_i \cup V_j \geq U_i \cup V_{j-1}$  для всех  $i = 1, \dots, m$ ;  $j = 1, \dots, n$ . Будем это доказывать индукцией по  $i + j$ . Наименьшее значение для  $i + j$  равно 2; для этого значения утверждение следует из верхней полумодулярности:

$$U_1 \cup V_1 \geq U_1 = U_1 \cup V_0 \text{ и } U_1 \cup V_1 \geq V_1 = U_0 \cup V_1.$$

Далее,  $U_i \cup V_j = (U_i \cup V_{j-1}) \cup (U_{i-1} \cup V_j)$ , а, по предположению индукции,  $U_i \cup V_{j-1} \geq U_{i-1} \cup V_{j-1}$  и  $U_{i-1} \cup V_j \geq U_{i-1} \cup V_{j-1}$ , следовательно, в силу верхней полумодулярности  $U_i \cup V_j \geq U_i \cup V_{j-1}$  и  $U_i \cup V_j \geq U_{i-1} \cup V_j$ , что и требовалось доказать. Отсюда, учитывая, что  $V_n = Y$  при  $j = n$ , мы получаем

$$Y \leq U_1 \cup Y \leq U_2 \cup Y \leq \dots \leq U_m \cup Y = X \cup Y.$$

Таким образом, длина максимальной цепи от  $Y$  до  $X \cup Y$  не превосходит  $m$ . Но, как мы установили ранее, это означает, что

$$d(X \cup Y) - d(Y) \leq m = d(X) - d(X \cap Y),$$

откуда следует неравенство (1) для верхне полумодулярной структуры. В силу дуальности неравенство (2) имеет место в нижне полумодулярной структуре. Этим доказано прямое утверждение теоремы.

**Лемма 8.3.1.** *Если в структуре конечной размерности имеет место неравенство (1), то из  $U > V$  следует, что  $d(U) = d(V) + 1$ .*

*Доказательство.* Пусть  $0 = U_0 \leq U_1 \leq U_2 \leq \dots \leq U_{t-1} \leq \dots \leq U_t = U$  — максимальная цепь от 0 до  $U$ . Между 0 и  $U_i$  не существует цепи длины, большей чем  $i$ , так как в противном случае мы могли бы построить более длинную цепь между 0 и  $U$ . Следовательно,  $d(U) = t$  и  $d(U_i) = i$  при  $i = 0, 1, \dots, t-1$ . Далее, так как  $U > V$ , имеем,  $d(U) \geq d(V) + 1$ , и поэтому  $t-1 \geq d(V)$ . Выберем  $U_j$  так, чтобы  $U_j \subseteq V$ ,  $U_{j+1} \not\subseteq V$  (такое  $j$  среди чисел  $0, 1, \dots, t-1$  должно найтись). Тогда  $U_{j+1} \cup V = U$ ,  $U_{j+1} \cap V = U_j$ . В силу неравенства (1)  $d(U_{j+1} \cup V) + d(U_{j+1} \cap V) \leq d(V) + d(U_{j+1})$ , откуда  $t+j \leq d(V) + j + 1$ , или  $t-1 \leq d(V)$ , а значит,  $d(V) = t-1$ ,  $d(U) = t = d(V) + 1$ .

Теперь, учитывая эту лемму и неравенство (1), предположим, что  $A < B$ ,  $A < C$  и  $B \neq C$ . Тогда  $A = B \cap C$ ,  $d(B) = d(A) + 1$ ,  $d(C) = d(A) + 1$ . Применяем неравенство (1):  $d(B \cup C) + d(B \cap C) \leq d(B) + d(C)$ , откуда  $d(B \cup C) \leq d(A) + 2$ . Но  $B \cup C \neq B$ ,  $C$ , поэтому  $d(B \cup C) = d(B) + 1 = d(C) + 1$ , откуда  $B \cup C > B$ ,  $B \cup C > C$ , т. е. структура  $L$  верхне полумодулярна. Так как понятие размерности  $d(X)$  элемента  $X$  определяется как длина максимальной цепи от 0 до  $X$  и принцип двойственности к нему неприменим, из неравенства (2) не следует, что структура  $L$  нижне полумодулярна. Пятиэлементная структура с элементами  $0$ ,  $T$ ,  $A_1$ ,  $B_1 \subset B_2$ , такими, что  $A_1 \cap B_1 = A_1 \cap B_2 = 0$ ,  $A_1 \cup B_1 = A_1 \cup B_2 = T$ , удовлетворяет неравенству (2), но не является нижне полумодулярной.

**Теорема 8.3.6.** *Структура конечной размерности модулярна тогда и только тогда, когда она одновременно нижне и верхне полумодулярна.*

**Доказательство.** Мы уже видели, что из модулярности следуют оба вида полумодулярности. Но если имеют место свойства верхней и нижней полумодулярности, то в силу теоремы 8.3.5 мы имеем, что  $d(X \cup Y) + d(X \cap Y) = d(X) + d(Y)$ , а согласно теореме 8.3.3 это свойство равносильно модулярности.

**Теорема 8.3.7.** *Подгруппы конечной  $p$ -группы образуют нижне полумодулярную структуру.*

**Доказательство.** Объединение и пересечение подгрупп, определенные в § 1.4, действительно удовлетворяют аксиомам структуры, причем отношением порядка является включение. Если  $A > B$ ,  $A > C$ , где  $A$ ,  $B$ ,  $C$  — подгруппы конечной  $p$ -группы, то  $B$  и  $C$  являются максимальными подгруппами группы  $A$  и по теореме 4.3.2 имеют индекс  $p$ . Согласно теореме 1.5.5 о неравенствах для индексов, значения  $[B : B \cap C]$  и  $[C : B \cap C]$  не превосходят  $p$ , а значит, равны 1 или  $p$ . Таким образом, если  $B \neq C$ , то  $B > B \cap C$  и  $C > B \cap C$ .

## 8.4. Главные и композиционные ряды

Мы применим теперь совокупность результатов предшествующих параграфов к исследованию структуры подгрупп произвольных групп. Рассмотрим цепочку подгрупп группы  $G$ :

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_n, \quad (8.4.1)$$

где каждая подгруппа  $A_i$  — нормальный делитель в подгруппе  $A_{i-1}$ , что мы обозначим так:

$$A_i \triangleleft A_{i-1}, \quad i = 1, \dots, n. \quad (8.4.2)$$

Группы  $A_i$  называются *субинвариантными* в группе  $G$ , а цепочка (8.4.1) называется *нормальным рядом*, или *нормальной цепочкой*<sup>1)</sup>.

Цепочке подгрупп (8.4.1) мы ставим в соответствие последовательность фактор-групп

$$A_{i-1}/A_i, \quad i = 1, \dots, n. \quad (8.4.3)$$

Если каждая подгруппа  $A_i$  инвариантна в группе  $G$ , мы называем ряд (8.4.1) *инвариантным рядом*, или *инвариантной цепью*. Если  $A_i \triangleleft A_{i-1}$ ,  $i = 1, \dots, n$ , то отсюда еще не следует, что  $A_i \triangleleft G$ , и поэтому требования инвариантности ряда сильнее, чем требования (8.4.2). Нормальный ряд, в котором каждый член  $A_i$  является максимальной инвариантной подгруппой группы  $G$ , содержащейся в  $A_{i-1}$ , будем называть *главным*. Нормальный ряд, в котором каждый член  $A_i$  является максимальной инвариантной подгруппой в  $A_{i-1}$ , будем называть *композиционным*. В терминах теории структур, если включения в ряду (8.4.1) являются покрытиями, инвариантный ряд называется *главным*, а нормальный — *композиционным*. Можно дополнительно требовать, чтобы группы  $A_i$  были допустимы относительно некоторого множества операторов  $\Omega$ .

Мы сможем интерпретировать общие теоремы о модулярных структурах или как теоремы о подгруппах, или как теоремы об отношениях конгруэнтности на лупах, или, более обще, как теоремы об отношениях конгруэнтности в алгебре<sup>2)</sup>, перестановочных с операциями алгебры. Основной теоремой, которая позволит нам получить самый сильный результат о группах, является теорема 2.4.1. Теоретико-структурные теоремы при этом опираются на модулярный закон, и это проявляется в алгебрах различными способами. Таким образом, при различных предположениях относительно алгебр из одной и той же теоремы о структурах получаются различные теоремы. Для теории подгрупп нам понадобится вспомогательная теорема о модулярности. Будем говорить, что подгруппы  $A$  и  $B$  группы  $G$  *перестановочны*, если  $AB = BA$ . Легко проверить, что в этом случае  $A \cup B = AB = BA$  и множество  $BA = AB$  является подгруппой. Из теоремы 2.3.3 следует, что подгруппы  $A$  и  $B$  перестановочны, если одна из них инвариантна; очевидно, вполне достаточно их инвариантности в группе  $A \cup B$ .

<sup>1)</sup> Автор называет инвариантный ряд нормальным. Переводчик предпочел пользоваться терминологией, принятой в советской алгебраической литературе. — Прим. перев.

<sup>2)</sup> Алгебры понимаются здесь в смысле Г. Биркгофа, т. е. как множество  $M$ , на котором задана некоторая совокупность многолистных функций со значениями в  $M$ . — Прим. перев.

**Теорема 8.4.1.** Пусть  $A, B, C$  — подгруппы группы  $G$ , причем  $A \supseteq B$ . Тогда для того, чтобы имело место равенство  $A \cap (B \cup C) = B \cup (A \cap C)$ , достаточно, чтобы подгруппы  $B$  и  $C$  были перестановочны.

**Доказательство.** Как отмечалось в доказательстве теоремы 8.2.5, из включения  $A \supseteq B$  следует, что

$$B \cup (A \cap C) \subseteq A \cap (B \cup C).$$

Достаточно доказать обратное включение. Элемент из группы  $A \cap (B \cup C)$ , являясь одновременно элементом подгрупп  $A$  и  $B \cup C$ , имеет вид  $a = bc$ , где  $a \in A$ ,  $b \in B$ ,  $c \in C$ . При этом, так как  $B$  и  $C$  перестановочны, все элементы из  $B \cup C$  записываются в виде  $bc$ . Отсюда  $c = b^{-1}a \in A$ , так как  $B \subseteq A$ . Поэтому  $c \in A \cap C$ , следовательно,  $bc \in B \cup (A \cap C)$ . Таким образом,  $A \cap (B \cup C) \subseteq B \cup (A \cap C)$ , и теорема доказана. Она справедлива также для подгрупп с обратными элементами, где перестановочность  $B$  и  $C$  означает  $B \cup C = BC$ . Для заключения, что  $b^{-1}a = b^{-1}(bc) = c$ , требуется только выполнение закона о существовании обратного элемента,

**Теорема 8.4.2.** (Теорема об уплотнении<sup>1)</sup>.) Пусть  $U = A_0 \supseteq \supseteq A_1 \supseteq \dots \supseteq A_n = V$  и  $U = B_0 \supseteq B_1 \supseteq \dots \supseteq B_m = V$  — две конечные цепи от  $U$  до  $V$  в модулярной структуре. Тогда можно уплотнить обе цепочки дополнительными элементами  $A_{i-1} = A_{i,0} \supseteq \supseteq A_{i,1} \supseteq \dots \supseteq A_{i,m} = A_i$ ,  $i = 1, \dots, n$ , и  $B_{j-1} = B_{j,0} \supseteq B_{j,1} \supseteq \dots \supseteq B_{j,n} = B_j$ ,  $j = 1, \dots, m$ , так, чтобы факторы  $A_{i,j-1}/A_{i,j}$  и  $B_{j,i-1}/B_{j,i}$  были проективны.

**Доказательство.** Положим  $A_{i,j} = A_i \cup (A_{i-1} \cap B_j)$ ,  $B_{j,i} = B_j \cup (B_{j-1} \cap A_i)$ ,  $i = 1, \dots, n$ ;  $j = 1, \dots, m$ . Здесь фактор  $A_{i,j-1}/A_{i,j}$  перспективен фактору

$$A_{i-1} \cap B_{j-1}/(A_{i-1} \cap B_j) \cup (A_i \cap B_{j-1}), \quad (8.4.4)$$

так как из включения  $B_j \subseteq B_{j-1}$  мы получаем

$$(A_{i-1} \cap B_{j-1}) \cup A_i \cup (A_{i-1} \cap B_j) = A_i \cup (A_{i-1} \cap B_{j-1}). \quad (8.4.5)$$

<sup>1)</sup> Оригинальная теорема Жордана — Гёльдера была расширена и обобщена целым рядом авторов. Она была доказана Жорданом [1] и Гёльдером [1]. Обобщения для групп с операторами были установлены Э. Нёттер [1] и В. Круллем [1, 2]. Теорема об уплотнении была доказана Шрейером [4] и Цассенхаузом [1]. Теоретико-структурная формулировка, данная здесь, является модификацией формулировки Орэ [2]. Обобщение на частично упорядоченные множества было сделано Орэ [1] и Маклейном [3].

Кроме этого, применяя свойство модулярности, получаем, что

$$\begin{aligned} & (A_{i-1} \cap B_{j-1}) \cup [A_i \cup (A_{i-1} \cap B_j)] = \\ & = (A_{i-1} \cap B_j) \cup (A_{i-1} \cap B_{j-1} \cap A_i) = \\ & = (A_{i-1} \cap B_j) \cup (A_i \cap B_{j-1}). \end{aligned} \quad (8.4.6)$$

Аналогично, фактор  $B_{j,i-1}/B_{j,i}$  перспективен фактору (8.4.4), и теорема доказана.

Эта теорема вместе с ее доказательством справедлива для нормальных рядов произвольной группы  $G$ , причем, если  $G$  — группа с областью операторов  $\Omega$ , то в качестве подгрупп рассматриваются только допустимые подгруппы. Сюда естественным образом относится случай группы без операторов, т. е. случай, когда область операторов  $\Omega$  состоит из одного тождественного оператора.

**Теорема 8.4.3.** (Теорема об уплотнении для групп.) Пусть  $G$  — группа с областью операторов  $\Omega$ , и пусть  $G = A_0 \supseteq A_1 \supseteq \dots \supseteq A_n = H$  и  $G = B_0 \supseteq B_1 \supseteq \dots \supseteq B_m = H$  — два нормальных ряда допустимых подгрупп от  $G$  до  $H$ . Тогда можно уплотнить оба ряда дополнительными допустимыми субинвариантными группами:

$$A_{i-1} = A_{i,0} \supseteq A_{i,1} \supseteq \dots \supseteq A_{i,m} = A_i, \quad i = 1, \dots, n,$$

и

$$B_{j-1} = B_{j,0} \supseteq B_{j,1} \supseteq \dots \supseteq B_{j,n} = B_j, \quad j = 1, \dots, m,$$

так, чтобы фактор-группы

$$A_{i,j-1}/A_{i,j} \text{ и } B_{j,i-1}/B_{j,i}$$

были операторно изоморфны.

**Доказательство.** В силу теоремы 2.4.1 перспективные (следовательно, и проективные) фактор-группы допустимых подгрупп операторно изоморфны. Следовательно, чтобы показать, что доказательство теоремы 8.4.2 применимо и в данном случае, мы должны установить, что в факторах  $X/Y$ , фигурирующих в доказательстве,  $Y \triangleleft X$  и что применение модулярного закона в выражении (8.4.6) законно. Так как объединение и пересечение допустимых подгрупп — допустимые подгруппы, то все подгруппы, встречающиеся в доказательстве, допустимы. Далее, группа  $A_{i,j} = A_i \cup (A_{i-1} \cap B_j)$  инвариантна в группе  $A_{i,j-1} = A_i \cup (A_{i-1} \cap B_{j-1})$ , так как каждая из групп  $A_i$  и  $A_{i-1} \cap B_j$  трансформируется в себя элементами подгруппы  $A_{i-1} \cap B_{j-1}$ . Аналогично  $B_{j,i} \triangleleft B_{j,i-1}$ . Группы  $A_{i-1} \cap B_j$  и  $A_i \cap B_{j-1}$ , а следовательно, и их объединение являются нормальными делителями в группе  $A_{i-1} \cap B_{j-1}$ , откуда фактор (8.4.4) является фактор-группой. Так как группа  $A_i$  инвариантна в  $A_{i-1}$ , в выражении (8.4.6)  $A_i$  перестановочна с лю-

бой подгруппой из  $A_{i-1}$  и, в частности, с подгруппой  $A_{i-1} \cap B_j$ . Следовательно, по теореме 8.4.1, к выражению (8.4.6) можно применить модулярный закон. Таким образом, теорема доказана.

В главных или композиционных рядах (для группы с операторами или без операторов) дальнейшие уплотнения невозможны, а потому в качестве следствия из теоремы об уплотнении получается следующая

**Теорема 8.4.4. (Теорема Жордана — Гельдера.)** *Если  $G = A_0 \supset A_1 \supset \dots \supset A_n = H$  и  $G = B_0 \supset B_1 \supset \dots \supset B_m = H$  — два главных (или композиционных) ряда группы  $G$  с областью операторов  $\Omega$ , то  $m = n$  и фактор-группы  $A_{i-1}/A_i$  операторно изоморфны фактор-группам  $B_{j-1}/B_j$  в некотором порядке.*

Равенство  $m = n$  является, конечно, следствием взаимно однозначного соответствия между фактор-группами, отличными от единичных.

В случае инвариантных рядов все подгруппы, будучи инвариантными, допустимы относительно всех внутренних автоморфизмов  $x \rightarrow a^{-1}xa$ , и мы можем включить все внутренние автоморфизмы в область операторов  $\Omega$ . Изоморфизм, сохраняющийся при всех внутренних автоморфизмах, называется *центральным*. Таким образом, следствием из теоремы об уплотнении является следующая

**Теорема 8.4.5.** *В уплотнениях инвариантных рядов соответствующие фактор-группы центрально изоморфны.*

Если теперь соответствие  $x \rightarrow (x)\alpha$  есть центральный автоморфизм группы, то

$$a^{-1}(x)\alpha a = (a^{-1}xa)\alpha = ((a)\alpha)^{-1}(x)\alpha(a)\alpha,$$

откуда элемент  $(a)\alpha a^{-1}$  перестановочен с любым  $(x)\alpha$  и, следовательно, принадлежит центру  $Z$  группы. Поэтому для любого центрального автоморфизма  $\alpha$  и для любого элемента  $a$  из группы имеем  $(a)\alpha = az$ ; здесь  $z$  — элемент центра, зависящий от  $a$ . Обратно, как легко видеть, автоморфизм такого вида является центральным.

## 8.5. Прямые разложения

Предположим, что в модулярной структуре имеются  $m$  элементов  $A_1, \dots, A_m$  таких, что для элементов  $\bar{A}_i = A_1 \cup \dots \cup A_{i-1} \cup A_{i+1} \cup \dots \cup A_m$  ( $i = 1, \dots, m$ ) выполняются отношения  $A_i \cap \bar{A}_i = 0$  ( $i = 1, \dots, m$ ). Тогда мы будем говорить, что элемент  $A = A_1 \cup \dots \cup A_m$  является *прямым объединением* элементов  $A_1, \dots, A_m$ , и будем записывать его в виде

$$A = A_1 \times A_2 \times \dots \times A_m. \quad (8.5.1)$$

Для групп это имеет место, если  $A$  есть прямое произведение подгрупп  $A_1, \dots, A_m$ .

**Теорема 8.5.1.** (Теорема Орэ.) Пусть  $L$  — любая модулярная структура конечной размерности. Если некоторый элемент  $T$  структуры  $L$  имеет два разложения  $T = A_1 \times \dots \times A_m$ ,  $T = B_1 \times \dots \times B_n$ , где  $A_i$  и  $B_j$  далее неразложимы в прямое объединение, то  $m = n$ , а элементы  $A_i$  и  $B_j$  попарно проективны.

**Доказательство.** Мы покажем, что любой элемент  $A_i$  (скажем,  $A_1$ ) можно заменить некоторым проективным ему элементом  $B_j$ , т. е.  $T = A_1 \times A_2 \times \dots \times A_m = B_j \times A_2 \times \dots \times A_m$ . Это и будет основной частью нашего доказательства. Заменив  $A_1$  элементом  $B_j$ , мы затем во втором разложении заменим  $A_2$  элементом  $B'_k$  и т. д. В процессе замен никогда не будем пользоваться элементом  $B_j$  дважды, так как это противоречило бы требованию, что пересечение любой компоненты с объединением остальных равно нулю. Элементов  $B_j$  должно быть достаточно, чтобы заменить все компоненты  $A_i$ , причем ясно, что в силу включений  $B_j \subseteq T$  лишних элементов  $B_j$  не должно быть. Поэтому  $m = n$ . Напомнив, что  $\bar{A}_i = A_1 \cup \dots \cup A_{i-1} \cup A_{i+1} \cup \dots \cup A_m$ ,  $i = 1, \dots, m$ , и  $\bar{B}_j = B_1 \cup \dots \cup B_{j-1} \cup B_{j+1} \cup \dots \cup B_n$ ,  $j = 1, \dots, n$ , проведем основное доказательство индукцией по размерности элемента  $T$ , исходя из того, что для размерности 1 утверждение тривиально.

Случай 1.  $A_1 \cup \bar{B}_j = \bar{A}_1 \cup B_j = T$  для некоторого  $j$ .  
Тогда

$$\begin{aligned} d(A_1) &= d(T) - d(\bar{B}_j) + d(A_1 \cap \bar{B}_j) = \\ &= d(B_j) + d(A_1 \cap \bar{B}_j) \geq d(B_j), \end{aligned}$$

и аналогично  $d(B_j) \geq d(A_1)$ . Поэтому  $d(A_1) = d(B_j)$ . Таким образом,  $d(A_1 \cap \bar{B}_j) = d(\bar{A}_1 \cap B_j) = 0$  и, следовательно,  $T = A_1 \times \bar{B}_j = \bar{A}_1 \times B_j$ , т. е. элементы  $A_1$  и  $B_j$  можно заменять друг другом.

Случай 2. Пусть  $A_1 \cup \bar{B}_j \subset T$  для некоторого  $j$  (скажем, для  $j = 1$ ). Введем обозначения  $D_h = A_1 \cup \bar{B}_h$ ,  $Q_h = D_h \cap B_1$ ,  $h = 1, \dots, n$ . Если  $D_1 = A_1 \cup \bar{B}_1 \not\supseteq B_1$ , то  $D_1 \not\supseteq \bar{B}_1 \cup B_1 = T$ , что противоречит условию. Следовательно,  $Q_1 = D_1 \cap B_1 \subset B_1$  и  $d(Q_1) < d(B_1)$ . Элемент  $T$  является прямым объединением элементов  $B_j$ ; поэтому объединение элементов  $Q_h$  также является прямым, поскольку  $Q_h \subseteq B_h$ ,  $h = 1, \dots, n$ .

Положим  $C = \bigcup_{h=1}^n Q_h$ . Поскольку элементы  $T$  и  $C$  являются прямыми объединениями, причем  $Q_1 \subset B_1$ ,  $d(T) = d(B_1) + \dots$

$\dots + d(B_n)$ , имеем

$$d(C) = d(Q_1) + \dots + d(Q_n) < d(T). \quad (8.5.2)$$

Так как элемент  $C$  строго содержится в  $T$ , мы можем предположить, согласно индукции по размерности, что теорема верна для  $C$ .

Положим  $U_r = Q_1 \cup \dots \cup Q_r$ . Мы хотим показать, что  $U_r = M_r \cap N_r$ , где  $M_r = B_1 \cup \dots \cup B_r$ ,  $N_r = D_1 \cap \dots \cap D_r$ . Применяя опять индукцию. При  $r=1$  это верно, так как тогда  $U_1 = Q_1$ , а, по определению,  $U_1 = B_1 \cap D_1$ . Предположим, что  $U_j = M_j \cap N_j$ . Тогда  $U_{j+1} = U_j \cup Q_{j+1} = (M_j \cap N_j) \cup (B_{j+1} \cap D_{j+1})$ , где  $D_{j+1} \supseteq \bar{B}_{j+1} \supseteq M_j \supseteq M_j \cap N_j$ . Согласно модулярному закону,  $U_{j+1} = D_{j+1} \cap [(M_j \cap N_j) \cup B_{j+1}]$ . Здесь  $B_{j+1} \subseteq \bar{B}_h \subseteq D_h$ ,  $h=2, \dots, j$ , откуда  $B_{j+1} \subseteq N_j$ . Наконец,  $U_{j+1} = D_{j+1} \cap [N_j \cap (B_{j+1} \cup M_j)] = N_{j+1} \cap M_{j+1}$ . Доказательство по индукции закончено. При  $r=n$   $M_r = T$ , откуда

$$C = Q_1 \cup \dots \cup Q_n = D_1 \cap D_2 \cap \dots \cap D_n \supseteq A_1, \quad (8.5.3)$$

где последнее включение справедливо, так как  $D_h \supseteq A_1$ ,  $h=1, \dots, n$ . Учитывая, что  $C \supseteq A_1$ , применяем модулярный закон  $(C \cap \bar{A}_1) \cup A_1 = C \cap (\bar{A}_1 \cup A_1) = C \cap T = C$ . Используя тривиальное равенство  $C \cap \bar{A}_1 \cap A_1 = 0$ , получаем

$$C = A_1 \times (C \cap \bar{A}_1) = Q_1 \times \dots \times Q_n. \quad (8.5.4)$$

По предположению индукции, теорема верна для элемента  $C$ , и поэтому  $A_1$  можно заменить некоторой неразложимой компонентой одного из элементов  $Q_h$  (скажем, компонентой  $E \subseteq Q_h$ ). В силу этой заменяемости  $d(E) = d(A_1)$ . Кроме того, так как  $C = E \times (C \cap \bar{A}_1)$ , мы получаем  $0 = E \cap C \cap \bar{A}_1 = E \cap \bar{A}_1$ . Следовательно,  $d(E \cup \bar{A}_1) = d(E) + d(\bar{A}_1) = d(A_1) + d(\bar{A}_1) = d(T)$ , а потому  $T = \bar{A}_1 \cup E = E \times \bar{A}_1$ . Кроме того,  $E \subseteq Q_h = (A_1 \cup \bar{B}_h) \cap B_h \subseteq B_h$  и  $E \cap (\bar{A}_1 \cap B_h) = E \cap \bar{A}_1 = 0$ . Далее,  $E \cup (\bar{A}_1 \cap B_h) = B_h \cap (E \cup \bar{A}_1) = B_h \cap T = B_h$ , откуда

$$B_h = E \times (\bar{A}_1 \cap B_h). \quad (8.5.5)$$

Но по предположению элемент  $B_h$  неразложим, а  $d(E) = d(A_1) > 0$ . Значит,  $B_h = E$  и  $\bar{A}_1 \cap B_h = 0$ . Отсюда получаем

$$T = A_1 \times \bar{A}_1 = B_h \times \bar{A}_1. \quad (8.5.6)$$

Кроме этого,  $B_h = E \subseteq Q_h \subseteq B_h$ , следовательно,  $B_h = Q_h = (A_1 \cup \bar{B}_h) \cap B_h$ . Таким образом,  $B_h \subseteq \bar{A}_1 \cup \bar{B}_h$ , и поэтому  $A_1 \cup \bar{B}_h \supseteq$

$\exists B_h \cup \bar{B}_h = T$ . Так как  $d(A_1) = d(B_h)$ , получаем равенства  
 $d(A_1 \cup \bar{B}_h) = d(A_1) + d(\bar{B}_h) - d(A_1 \cup \bar{B}_h) =$   
 $= d(B_h) + d(\bar{B}_h) - d(T) = 0$ .

Следовательно,

$$T = A_1 \times \bar{B}_h, \quad (8.5.7)$$

и в итоге компоненты  $A_1$  и  $B_h$  взаимозаменяемы, причем  $h \neq 1$ , так как  $A_1 \cup \bar{B}_h = T$ , в то время как  $A_1 \cup \bar{B}_1 \neq T$ .

Случай 3.  $A_1 \cup \bar{B}_j = T$  для всех  $j$ , но  $\bar{A}_1 \cup B_j \subset T$  для всех  $j$ . Это единственная возможность, не охватываемая случаями 1 и 2. Поменяв ролями  $A_i$  и  $B_j$ , мы применим случай 2, и тогда произвольную компоненту  $B_j$  (скажем,  $B_n$ ) можно заменить на некоторую компоненту  $A_i$  (но не  $A_1$ ), которую при соответствующей нумерации можно взять как элемент  $A_m$ . Тогда

$$T = A_1 \times \dots \times A_{m-1} \times A_m = B_1 \times \dots \times B_{n-1} \times A_m = \bar{B}_n \times A_m. \quad (8.5.8)$$

При этом соответствие  $z \rightarrow (z \cup A_m) \cap \bar{A}_m$  является проекцией частного  $\bar{B}_n/0$  на  $\bar{A}_m/0$ , которое, согласно следствию из теоремы 8.3.1, оказывается структурным изоморфизмом. Следовательно, полагая  $B_j^* = (B_j \cup A_m) \cap \bar{A}_m$ ,  $j = 1, \dots, n-1$ , мы в силу изоморфизма получаем

$$\bar{A}_m = A_1 \times \dots \times A_{m-1} = B_1^* \times \dots \times B_{n-1}^*. \quad (8.5.9)$$

По предположению индукции, теорема верна для  $\bar{A}_m$ . Поэтому элемент  $A_1$  заменим некоторым  $B_j^*$  (например,  $B_1^*$ ) в разложении  $\bar{A}_m$ . Тогда  $B_1 \cup A_m = (B_1 \cup A_m) \cap (\bar{A}_m \cup A_m) = [(B_1 \cup A_m) \cap \bar{A}_m] \cup A_m = = B_1^* \cup A_m$ . Следовательно,  $B_1 \cup \bar{A}_1 = (B_1^* \cup A_2 \cup \dots \cup A_{m-1}) \cup A_m = = (A_1 \cup A_2 \cup \dots \cup A_{m-1}) \cup A_m = T$ , так как элемент  $B_1^*$  заменяет  $A_1$  в разложении  $\bar{A}_m$ . Но здесь  $A_1 \cup \bar{B}_1 = T = B_1 \cup \bar{A}_1$ , а потому можно применить результат случая 1. Итак, компоненты  $A_1$  и  $B_1$  взаимозаменяемы. Отметим, что случай 3 в действительности не встречается, а во всех случаях для данной компоненты  $A_1$  существует такая компонента  $B_j$ , что  $A_1$  и  $B_j$  взаимозаменяемы.

В применении к группам получается следующая

Теорема 8.5.2. (Теорема Веддербарна — Ремака — Шмидта<sup>1)</sup>.)

Пусть  $G$  — группа, инвариантные подгруппы которой образуют

<sup>1)</sup> Первое доказательство этой теоремы принадлежит Веддербарну [1]. Ремак [1, 2] восполнил пробел в нем, О. Ю. Шмидт обобщил эту теорему на группы с операторами. Теорема 8.5.1 для структур была доказана Орэ [1], ее доказательство, изложенное здесь, взято у Биркгофа [1], но несколько изменено.

структурой конечной размерности. Если группа  $G$  двумя способами представима как прямое произведение неразложимых подгрупп

$$G = A_1 \times \dots \times A_m,$$

$$G = B_1 \times \dots \times B_n,$$

то  $m = n$  и любая подгруппа  $A_i$  может быть заменена некоторой подгруппой  $B_j$ , причем подгруппы  $A_i$  и  $B_j$  центрально изоморфны. Эта теорема справедлива также для групп с операторами и для отношений конгруэнтности луп со свойством обращения.

**Доказательство.** Так как уже установлено, что инвариантные подгруппы образуют модулярную структуру, нам нужно только убедиться, что в случае групп прямое объединение элементов структуры является прямым произведением подгрупп. При разложениях  $G = A_i \times \bar{A}_i = B_j \times \bar{A}_i$  подгруппы  $A_i$  и  $B_j$  перспективны фактор-группе  $G/\bar{A}_i$  и, следовательно, проективны. Таким образом, существует центральный изоморфизм между  $A_i$  и  $B_j$ , который превращается в центральный автоморфизм группы  $G$ , если отображать подгруппу  $\bar{A}_i$  на себя. Следовательно, соответствующие элементы из подгрупп  $A_i$  и  $B_j$  отличаются друг от друга сомножителем, принадлежащим центру группы  $G$ .

## 8.6. Композиционные ряды в группах

Пусть  $G = A_0 \supset A_1 \supset \dots \supset A_n = H$  — композиционный ряд между  $G$  и подгруппой  $H$ . По определению,  $A_{i+1}$  является максимальным нормальным делителем группы  $A_i$ . Следовательно, фактор-группа  $A_i/A_{i+1}$  проста, так как ее нормальному делителю соответствовал бы нормальный делитель группы  $A_i$ , содержащий  $A_{i+1}$  (теорема 2.3.4). Таким образом, если группа  $A_i/A_{i+1}$  абелева, то она не содержит даже собственных подгрупп и, следовательно, является конечной группой простого порядка. Между главными и композиционными рядами существует отношение, устанавливаемое следующей теоремой.

**Теорема 8.6.1.** Пусть  $H$  — такая инвариантная подгруппа группы  $G$ , что между  $G$  и  $H$  существует композиционный ряд. Тогда между  $G$  и  $H$  существует главный ряд

$$G = B_0 \supset B_1 \supset \dots \supset B_m = H,$$

причем любая фактор-группа  $B_i/B_{i+1}$  является прямым произведением конечного числа изоморфных простых групп. Обратно, если такой ряд существует и фактор-группы  $B_i/B_{i+1}$  являются прямым произведением конечного числа изоморфных

простых групп, то существует композиционный ряд между  $G$  и  $H$ .

**Доказательство.** Любой нормальный ряд от  $G$  до  $H$  может быть уплотнен до композиционного. Поэтому любой нормальный ряд от  $G$  до  $H$  обязательно короче композиционного ряда и, следовательно, имеет конечную длину. Таким образом, между  $G$  и  $H$  существует главный ряд

$$G = B_0 \supset B_1 \supset \dots \supset B_m = H.$$

Далее применяем индукцию по  $m$ . Если  $m = 1$ , то группа  $G/H$  проста, и теорема доказана. Предположим теперь, что каждая из групп  $B_0/B_1, \dots, B_{m-2}/B_{m-1}$  является прямым произведением конечного числа изоморфных простых групп. Достаточно доказать, что группа  $B_{m-1}/B_m$  есть прямое произведение конечного числа изоморфных простых групп.

Любая инвариантная подгруппа группы  $B_{m-1}/B_m$  соответствует инвариантной подгруппе группы  $B_{m-1}$ , содержащей  $B_m$ . Следовательно, существует минимальная инвариантная подгруппа  $K/B_m$ , где  $K \supset B_m$ , и подгруппа  $K$  инвариантна в группе  $B_{m-1}$ . Если  $K = B_{m-1}$ , то группа  $B_{m-1}/B_m$  проста и доказывать больше нечего. Рассмотрим теперь подгруппы  $K_j$ , сопряженные с  $K$  во всей группе  $G$ .  $K_j \subseteq B_{m-1}$ , так как подгруппа  $B_{m-1}$  инвариантна в  $G$ . Более того, так как трансформирование элементом из  $G$  индуцирует автоморфизм группы  $B_{m-1}$ , любая подгруппа  $K_j$  инвариантна в  $B_{m-1}$ . Далее, группа  $\bigcup_j K_j$  инвариантна в группе  $G$ , так как трансформирование элементом из  $G$  просто переставляет группы  $K_j$  между собой. Следовательно,  $\bigcup_j K_j = B_{m-1}$ , так как не существует

инвариантных подгрупп группы  $G$  между  $B_{m-1}$  и  $B_m$ . Пусть  $K = K_1, K_2 \not\subseteq K_1, K_3 \not\subseteq K_1 \cup K_2, \dots, K_j \not\subseteq K_1 \cup \dots \cup K_{j-1}$ . Каждая из подгрупп  $U_j = K_1 \cup \dots \cup K_j$  инвариантна в группе  $B_{m-1}$  и, кроме того, содержит предшествующую подгруппу  $U_{j-1}$ . Так как между  $G$  и  $B_m$  существует композиционный ряд, включающий  $B_{m-1}$ , то подгруппа  $U_j$  только конечное число, и, следовательно, для некоторого конечного  $j$  получаем, что  $B_{m-1} = K_1 \cup \dots \cup K_j$ . Подгруппа  $K_i$ , не содержащаяся в объединении остальных таких подгрупп, имеет пересечение с этим объединением, совпадающее с  $B_m$ , так как каждая подгруппа  $K_j$  является минимальной инвариантной подгруппой группы  $B_{m-1}$ , содержащей  $B_m$ . Следовательно, пренебрегая подгруппами  $K_j$ , содержащимися в объединении остальных, мы получаем  $B_{m-1}/B_m = K_1/B_m \cup \dots \cup K_s/B_m$ , где каждая подгруппа  $K_i/B_m$  инвариантна в группе  $B_{m-1}/B_m$  и пересекает объединение остальных по единице. Тогда в силу

теоремы 3.2.2 группа  $B_{m-1}/B_m$  является прямым произведением подгрупп  $K_1/B_m, \dots, K_s/B_m$ . Если бы подгруппа  $K_1/B_m$  имела собственный нормальный делитель, то последний был бы нормальным делителем в группе  $B_{m-1}/B_m$ , так как она была бы инвариантной в группе  $K_1/B_m$  и остальные прямые сомножители лежали бы в нормализаторе этой подгруппы. Но по построению  $K_1/B_m$  — минимальная инвариантная подгруппа, поэтому  $K_1/B_m$  — простая группа, и фактор-группа  $B_{m-1}/B_m$  является прямым произведением  $s$  изоморфных простых групп.

Чтобы убедиться в истинности утверждения, обратного доказанному, достаточно заметить, что ряд  $B_m \subset K \subset U_2 \subset U_3 \subset \dots \subset B_{m-1}$  является частью композиционного ряда, так как каждая его фактор-группа проста.

**Теорема 8.6.2<sup>1)</sup>.** *Пересечение двух субинвариантных подгрупп группы  $G$  есть субинвариантная подгруппа. Объединение и пересечение двух подгрупп, встречающихся в композиционном ряду, являются членами некоторого композиционного ряда.*

**Доказательство.** Пусть  $A$  и  $B$  — две субинвариантные подгруппы группы  $G$ . По определению, существуют два ряда вида

$$\begin{aligned} A &= A_r \triangleleft A_{r-1} \triangleleft \dots \triangleleft A_1 \triangleleft G, \\ B &= B_s \triangleleft B_{s-1} \triangleleft \dots \triangleleft B_1 \triangleleft G. \end{aligned}$$

Тогда в ряду  $A = A_r \supseteq A_r \cap B_1 \supseteq \dots \supseteq A_r \cap B_s = A \cap B$  каждая подгруппа или равна предшествующей, или инвариантна в ней (теорема 2.4.1). Отсюда получаем

$$A \cap B \triangleleft C_u \triangleleft C_{u-1} \triangleleft \dots \triangleleft C_1 \triangleleft A_r \triangleleft \dots \triangleleft A_1 \triangleleft G,$$

где  $C_i$  — различные члены предыдущего ряда. Поэтому подгруппа  $A \cap B$  субинвариантна.

Предположим теперь, что оба исходных ряда являются композиционными. Если  $B_1 \neq A_1$ , то  $G = A_1 \cup B_1$ , так как и  $B_1$ , и  $A_1$  — максимальные нормальные делители в  $G$ . Подгруппа  $A_1 \cap B_1$  инвариантна в  $G$ , причем группа  $A_1/A_1 \cap B_1$  изоморфна группе  $G/B_1$ , а значит, проста. Поэтому  $A_1 \cap B_1$  — максимальная инвариантная подгруппа в  $A_1$ . Здесь или  $A_1 \cap B_1 = A_2$ , или подгруппы  $A_1 \cap B_1$  и  $A_2$  являются максимальными инвариантными подгруппами в группе  $A_1$ , откуда  $A_1 = A_2 \cup (A_1 \cap B_1)$  и  $A_2 \cap B_1 = A_2 \cap (A_1 \cap B_1)$ , а, значит, группа  $A_2/A_2 \cap B_1 \cong A_1/A_1 \cap B_1 \cong G/B_1$  проста. При этом  $A_1 \cap B_1/A_2 \cap B_1 \cong A_1 \cap A_2$ . Продолжая этот процесс, мы придем к тому, что или  $A = A_r = A_r \cap B_1$ , или  $A_r \cap B_1 \triangleleft A_r$ , и группа  $A_r/A_r \cap B_1 \cong G/B_1$  проста. Мы получаем композиционные ряды

$$\begin{aligned} A_r \cap B_1 &\triangleleft A_{r-1} \cap B_1 \triangleleft \dots \triangleleft A_1 \cap B_1 \triangleleft B_1 \triangleleft G, \\ B_s &\triangleleft B_{s-1} \triangleleft \dots \triangleleft B_2 \triangleleft B_1 \triangleleft G, \end{aligned}$$

<sup>1)</sup> Эти результаты принадлежат Виландту [2].

аналогичные исходным, но с меньшим числом членов, следующих за  $B_1$ . Повторив эти построения для  $B_2$  в роли  $B_1$  и т. д., мы в итоге получим композиционный ряд между  $G$  и  $A \cap B$ .

Намного труднее доказывается, что объединение двух композиционных групп (так мы будем называть подгруппы, встречающиеся в композиционных рядах) будет снова композиционной группой. Применим индукцию по длинам  $r$  и  $s$  двух композиционных рядов от  $A = A_r$  и  $B = B_s$  до  $G$ . Точнее говоря, мы применим индукцию по  $r + s$ , исходя из того, что теорема верна при  $r + s = 2$ , так как  $A_1 \cup B_1$  — инвариантная подгруппа группы  $G$ . Нам понадобится

**Лемма 8.6.1.** *Если  $C$  — композиционная подгруппа группы  $G$ , которая строго содержит композиционную группу  $A$ , то между  $G$  и  $A$  существует композиционный ряд, включающий подгруппу  $C$ , и, следовательно, длина композиционного ряда от  $G$  до  $C$  меньше длины композиционного ряда от  $G$  до  $A$ .*

Действительно, если

$$\begin{aligned} C &= C_t \triangleleft C_{t-1} \triangleleft \dots \triangleleft C_1 \triangleleft G, \\ A &= A_r \triangleleft A_{r-1} \triangleleft \dots \triangleleft A_1 \triangleleft G \end{aligned}$$

— какие-либо композиционные ряды между  $G$  и  $C$ ,  $G$  и  $A$ , то, повторяя вышеприведенное построение, мы получаем ряд

$$A_r = A_r \cap C_t \triangleleft A_{r-1} \cap C_t \triangleleft \dots \triangleleft A_1 \cap C_t \triangleleft C_t \triangleleft \dots \triangleleft C_1 \triangleleft G,$$

в котором все различные члены составляют композиционный ряд от  $G$  до  $A_r$  и длина которого, значит, равна  $r$ . Отсюда  $r > t$ .

По предположению индукции,  $A_{r-1} \cup B_s$  и  $A_r \cup B_{s-1}$  — композиционные подгруппы группы  $G$ . Если  $A_{r-1} \cup B_s$  — собственная подгруппа в  $G$ , то  $A_r$  и  $B_s$  — композиционные подгруппы в  $A_{r-1} \cup B_s$  с длинами  $r' < r$  и  $s' < s$  (в силу леммы). Тогда по индукции  $A_r \cup B_s$  — композиционная подгруппа в  $A_{r-1} \cup B_s$  и, следовательно, в  $G$ . Таким образом, предположим, что  $A_{r-1} \cup B_s = G$ . Если опять  $A_r \cup B_{s-1}$  — собственная подгруппа в  $G$ , то доказательство проводится, как и выше. Таким образом, мы можем предположить также, что  $A_r \cup B_{s-1} = G$ . Не ограничивая общности, будем считать, что  $r \leq s$ . Если  $b \in B_s$ , то

$$b^{-1} A_r b \triangleleft b^{-1} A_{r-1} b \triangleleft \dots \triangleleft b^{-1} A_1 b \triangleleft A_1 \triangleleft G,$$

где  $b^{-1} A_1 b = A_1$ , так как подгруппа  $A_1$  инвариантна. Если теперь  $b^{-1} A_r b \neq A_r$ , то  $A_r$  и  $b^{-1} A_r b$  — композиционные группы в  $A_1$ , и в обоих случаях длина их рядов равна  $r - 1$ . Следовательно, по индукции  $A^* = A_r \cup b^{-1} A_r b$  — композиционная группа в  $A_1$ , причем длина цепи от  $A_1$  до  $A^*$  меньше  $r - 1$ . Поэтому опять, по предположению индукции,  $B_s \cup A^*$  — композиционная группа. Но

$B_s \cup A^* = B_s \cup A_r = B \cup A$ . Таким образом, мы можем считать, что группа  $A_r$  трансформируется в себя любым элементом из  $B_s$ . Но  $A_r$  трансформируется в себя также любым элементом подгруппы  $A_{r-1}$ . Поэтому группа  $A_r$  инвариантна в группе  $A_{r-1} \cup B_s = G$ . Так как  $A_r$  инвариантна в  $G$ , мы можем ее взять в качестве  $A_1$ . Но тогда  $B \cup A = B_s \cup A_1 \triangleleft B_{s-1} \cup A_1 \triangleleft \dots \triangleleft B_1 \cup A_1 \triangleleft G$ , так как подгруппы  $B_i$  и  $A_1$  трансформируются в себя группой  $B_{i-1}$ , а кроме того, ясно, что  $A_1$ , будучи подгруппой группы  $B_i \cup A_1$ , трансформирует ее в себя. Следовательно,  $B_i \cup A_1 \triangleleft B_{i-1} \cup A_1$ . Таким образом, подгруппа  $B \cup A$ , будучи субинвариантной подгруппой группы  $G$ , содержащей подгруппу  $A$  в композиционном ряду, также является композиционной группой.

## Упражнения

- Пусть порядок группы  $G$  равен  $p^r q^s$ . Пусть группа  $G$  имеет два композиционных ряда:

$$1 \subset A_1 \subset A_2 \subset \dots \subset A_r \subset A_{r+1} \subset \dots \subset A_{r+s} = G$$

и

$$1 \subset B_1 \subset B_2 \subset \dots \subset B_s \subset B_{s+1} \subset \dots \subset B_{r+s} = G,$$

где порядок подгруппы  $A_r$  равен  $p^r$ , а порядок подгруппы  $B_s$  равен  $q^s$ . Показать, что  $G$  есть прямое произведение подгрупп  $A_r$  и  $B_s$ .

- Обобщая результат упражнения 1, показать, что если  $G$  — конечная группа и если для любого простого числа  $p$ , делящего порядок группы  $G$ , существует композиционный ряд группы  $G$ , одним из членов которого является силовская подгруппа  $S(p)$ , то группа  $G$  есть прямое произведение своих силовских подгрупп.

- Показать, что автоморфизм прямого произведения конечного числа неабелевых простых групп переставляет сомножители.

- Пусть группа  $G$  с конечным числом образующих имеет точно одну максимальную подгруппу  $A$ . Показать, что  $G$  порождается любым элементом, не принадлежащим  $A$ . Показать, что  $G$  — циклическая группа порядка  $p^n$  ( $p$  — простое число).

- Пусть группа  $G$  с конечным числом образующих имеет точно две максимальные подгруппы  $A$  и  $B$ , причем  $[G : A] = p$ ,  $[G : B] = q$ , где  $p$  и  $q$  — различные простые числа. Показать, что группа  $G$  циклическая группа порядка  $p^i q^j$ . (Указание: показать, что подгруппа  $A \cap B$  инвариантна и что группа  $G/A \cap B$  циклическа.)

- Пусть  $G$  — такая конечная группа, что размерность структуры  $L(G)$  равна 2. Показать, что если порядок группы  $G$  свободен от квадратов, то по меньшей мере одна силовская подгруппа инвариантна. Вывести отсюда, что порядок  $G$  равен  $p^2$  или  $pq$ , где  $p$  и  $q$  — простые числа.

## Г л а в а 9

### ТЕОРЕМА ФРОБЕНИУСА. РАЗРЕШИМЫЕ ГРУППЫ

#### 9. 1. Теорема Фробениуса

Теорема 9.1.1, в первоначальной форме принадлежащая Фробениусу [2], по своей природе существенно отлична от других результатов теории групп. В этой теореме говорится не о подгруппах, гомоморфизмах или представлениях подстановками, а о числе решений некоторого уравнения в конечной группе. Теорема была значительно обобщена Ф. Холлом [3], который обобщил как изучаемое уравнение, так и формулировку о свойствах его решения. Но здесь мы изложим только небольшое обобщение первоначальной теоремы.

**Теорема 9.1.1.** *Если  $G$  — группа порядка  $g$  и  $C$  — класс, состоящий из  $h$  сопряженных элементов, то число решений уравнения  $x^n = c$ , где элемент  $c$  пробегает класс  $C$ , кратно  $(hn, g)$ .*

*Доказательство.* Обозначим через  $A(K, n)$  множество тех элементов группы  $G$ ,  $n$ -е степени которых принадлежат множеству  $K$ . Через  $a(K, n)$  обозначим число элементов множества  $A(K, n)$ . При  $g = 1$ ,  $(hn, 1) = 1$ , и утверждение теоремы тривиально; при  $n = 1$  число решений равно  $h = (h, g)$ . Доказательство проведем по индукции, предполагая, что теорема верна для  $n' \leq n$  или  $g' \leq g$ .

Если  $c' = u^{-1}cu$  и  $x^n = c$ , то  $(u^{-1}xu)^n = c'$ . Этим установлено взаимно однозначное соответствие между решениями уравнения для элемента  $c$  и для произвольного элемента, сопряженного с ним. Таким образом,  $a(C, n) = h \cdot a(c, n)$ . Если  $x^n = c$ , то  $x^{-1}cx = x^{-1}(x^n)x = x^n = c$ , т. е. решения уравнения  $x^n = c$  лежат в нормализаторе  $N_c$  элемента  $c$ , состоящем, в силу теоремы 1.6.1, из  $g/h$  элементов. Следовательно, если  $h > 1$ , то теорема верна для подгруппы  $N_c$  и число  $a(c, n)$  кратно числу  $(n, g/h)$ , откуда  $a(C, n) = h \cdot a(c, n)$  кратно  $h(n, g/h) = (hn, g)$ , и теорема для этого случая доказана.

Пусть теперь  $h = 1$ . Если  $n = n_1n_2$ ,  $(n_1, n_2) = 1$ ,  $n_1 > 1$ ,  $n_2 > 1$ , и если  $D = A(C, n_2)$ , то  $A(C, n) = A(D, n_1)$ , причем  $D$  состоит из полных классов сопряженных элементов группы  $G$ . По предположению индукции, число  $(n_1, g)$  делит  $a(C, n)$  и аналогично  $(n_2, g)$  делит  $a(C, n)$ . Но тогда, так как числа  $(n_1, g)$  и  $(n_2, g)$

взаимно простые, их произведение  $(n_1, g)(n_2, g) = (n_1 n_2, g) = (n, g)$  делит  $a(C, n)$ , и теорема для этого случая также доказана.

Мы можем предположить теперь, что  $n = p^e$ , где  $p$  — простое число. Если  $p$  делит порядок  $u$  элемента  $c$ , то порядок элемента  $x$  из  $A(c, n)$  равен  $pu$ . Тогда точно  $n$  элементов циклической подгруппы, порожденной элементом  $x$ , принадлежат множеству  $A(c, n)$ , и все они порождают одну и ту же подгруппу. Поэтому  $a(c, n)$  делится на  $n$ .

Предположим, наконец, что число  $n = p^e$  взаимно просто с порядком  $u$  элемента  $c$ . Так как  $h = 1$ , то  $c$  принадлежит центру группы  $G$ . Элементы центра, порядки которых не делятся на  $p$ , образуют абелеву группу  $B$ , порядок  $b$  которой также не делится на  $p$ .

Пусть теперь  $c_1$  и  $c_2$  — два элемента из  $B$ . Так как  $p \nmid b$ , уравнение  $c_1 = c_2 y^n$  имеет в  $B$  единственное решение  $y$ . Но тогда, если  $x^n = c_1$ ,  $(xy)^n = c_2$ , и поэтому числа  $a(c, n)$  равны для любых элементов  $c \in B$ . Наконец, по формуле

$$g = \sum_{c \in B} a(C, n) + ba(c, n)$$

пересчитываются  $g$  элементов группы  $G$  в зависимости от того, в какой класс сопряженных элементов попадает  $n$ -я степень каждого элемента; при этом учитываются сперва классы, не содержащиеся в  $B$ , а затем (одноэлементные) классы из  $B$ . Для этого последнего случая число элементов для каждого отдельного класса повторяется  $b$  раз. Число  $(n, g)$  делит каждое из слагаемых  $a(C, n)$  или по предположению индукции, или в силу проведенной части доказательства. Далее, так как число  $(n, g)$  делит  $g$  и взаимно просто с  $b$ ,  $(n, g)$  делит  $a(c, n)$ , и теорема полностью доказана.

Если  $c$  — единица группы  $G$ , то  $h = 1$ , и мы получаем первоначальную форму теоремы Фробениуса. В этом случае  $x^g = 1$  для всех элементов группы, и поэтому если  $(n, g) = m$ , то из равенства  $x^n = 1$  следует, что  $x^m = 1$ .

**Теорема 9.1.2.** *Если  $n$  делит порядок группы  $G$ , то число решений уравнения  $x^n = 1$  в группе  $G$  кратно  $n$ .*

Заметим, что единица всегда удовлетворяет уравнению такого типа, следовательно, количество его решений не равно нулю и потому не меньше  $n$ .

В связи с этой теоремой существует следующее интересное предположение.

*Если  $n$  делит порядок группы  $G$  и число решений уравнения  $x^n = 1$  равно точно  $n$ , то эти решения образуют нормальный делитель группы  $G$ .*

Отметим, что если группа  $G$  содержит подгруппу  $H$  порядка  $n$ , то элементы этой подгруппы являются решениями такого уравнения. Более того, если  $x^n = 1$ , то для произвольного  $z$  имеет место  $(z^{-1}xz)^n = 1$ , следовательно,  $H$  — инвариантная подгруппа. Поэтому задача состоит в доказательстве того, что  $n$  решений такого уравнения образуют подгруппу  $H$ . То, что  $n$  делит порядок группы  $G$  существенно, так как по теореме Лагранжа порядок подгруппы делит порядок группы. Например, уравнение  $x^4 = 1$  имеет точно 4 решения в симметрической группе третьей степени, имеющей порядок 6, но эти решения подгруппу не образуют.

## 9.2. Разрешимые группы

Элемент  $x^{-1}y^{-1}xy$  группы  $G$  называется *коммутатором* элементов  $x$  и  $y$  и обозначается  $(x, y)$ . Коммутаторы более высокой степени определяются рекуррентно по правилу  $(x_1, \dots, x_{n-1}, x_n) = ((x_1, \dots, x_{n-1}), x_n)$ . Это так называемые *простые коммутаторы*. Вообще элементы, которые могут быть получены в результате последовательного коммутирования, называются *сложными коммутаторами*, например  $((a, b), (c, d, e))$ . Определим рекуррентно вес  $\omega$  коммутатора, полагая, что веса элементов  $g$  группы  $G$  равны 1,  $\omega(g) = 1$ , а  $\omega(x, y) = \omega(x) + \omega(y)$ . Таким образом, вес элемента, являющегося коммутатором, зависит от формы коммутатора, в которой он записан, но не от самого этого элемента.

Согласно определению,  $(x, y) = 1$  тогда и только тогда, когда  $yx = xy$ . Таким образом, все коммутаторы группы  $G$  равны 1 тогда и только тогда, когда  $G$  — абелева группа. Таким образом, можно считать, что коммутаторы указывают, в какой степени рассматриваемая группа отличается от абелевой. Подгруппа  $G'$  группы  $G$ , порожденная всеми коммутаторами  $x^{-1}y^{-1}xy$ , называется *коммутантом* группы, или *производной подгруппой*. Ясно, что  $G'$  — вполне характеристическая подгруппа.

**Теорема 9.2.1.** *Фактор-группа  $G/G'$  — абелева. Если  $K$  — такая инвариантная подгруппа группы  $G$ , что фактор-группа  $G/K$  абелева, то  $K \supseteq G'$ .*

*Доказательство.* Пусть при отображении  $G \rightarrow G/G' = H$   $x \mapsto u$ ,  $y \mapsto v$ , где  $u$  и  $v$  — произвольные элементы группы  $H$ . Тогда  $x^{-1}y^{-1}xy \mapsto u^{-1}v^{-1}uv$ . Но  $x^{-1}y^{-1}xy \in G'$ , откуда  $x^{-1}y^{-1}xy \mapsto 1 = u^{-1}v^{-1}uv$ , следовательно,  $uv = vu$ , и группа  $G/G'$  — абелева.

Предположим теперь, что фактор-группа  $G/K$  абелева. Если при отображении  $G \rightarrow G/K$   $x \mapsto u$ ,  $y \mapsto v$ , где  $x, y \in G$ , то  $x^{-1}y^{-1}xy \mapsto u^{-1}v^{-1}uv = 1$ . Таким образом, произвольный коммутатор  $x^{-1}y^{-1}xy$  принадлежит подгруппе  $K$ , а потому  $K \supseteq G'$ .

**Определение.** Группа  $G$  называется *разрешимой*, если цепочка  $G \supseteq G' \supseteq G'' \supseteq \dots \supseteq G^{(i)} \supseteq \dots$ , где каждая подгруппа  $G^{(i)}$

является коммутантом предыдущей, обрывается после конечного числа шагов на единичной подгруппе (например,  $G^{(e)} = 1$ ).

По теореме 9.2.1, каждая фактор-группа  $G^{(i)}/G^{(i+1)}$  абелева. Заметим, что из равенства  $G^{(i)} = G^{(i+1)}$  следуют равенства  $G^{(j)} = G^{(j)}$  для всех  $j \geq i$ . Поэтому в цепочке коммутантов разрешимой группы все включения до  $G^{(e)} = 1$  строгие.

**Теорема 9.2.2.** *Любая подгруппа и фактор-группа разрешимой группы разрешима.*

**Доказательство.** Пусть  $H$  — подгруппа разрешимой группы  $G$ . Тогда, по определению,  $H' \leq G'$ , так как подгруппа  $H'$  порождена всеми коммутаторами элементов из  $H$ , а  $G'$  — всеми коммутаторами элементов из  $G$ . Отсюда  $H'' \leq G''$  и т. д. Но  $G^{(e)} = 1$ , значит, и  $H^{(e)} = 1$ , т. е. подгруппа  $H$  разрешима, причем  $H^{(i)}$  может быть единичной подгруппой для некоторого  $i < e$ .

Если  $Q = G/K$ , рассмотрим гомоморфизм  $G \rightarrow Q$ . Тогда любой коммутатор в группе  $Q$  является образом коммутатора элементов из  $G$ , откуда  $G' \rightarrow Q'$  и т. д. Наконец,  $G^{(e)} \rightarrow Q^{(e)}$ , откуда  $Q^{(e)} = 1$ , так как  $G^{(e)} = 1$ , причем опять  $Q^{(i)}$  может быть единичной подгруппой для некоторого  $i < e$ .

**Теорема 9.2.3** <sup>1)</sup>. *Группа  $G$  конечного порядка разрешима тогда и только тогда, когда фактор-группы композиционного ряда группы  $G$  — циклические простого порядка.*

**Доказательство.** Пусть  $G = A_0 \supset A_1 \supset \dots \supset A_r = 1$  — композиционный ряд, где каждая фактор-группа  $A_{i-1}/A_i$  ( $i = 1, \dots, r$ ) — циклическая группа простого порядка. В силу теоремы 9.2.1,  $A_1 \cong G'$ , так как фактор-группа  $G/A_1$  абелева. Далее аналогично:  $A_2 \cong A_1 \cong \cong G''$  и т. д. Наконец,  $A_r \cong G^{(r)}$ , откуда  $G^{(r)} = 1$ , т. е. группа  $G$  разрешима.

Обратно, пусть конечная группа  $G$  разрешима. Так как группа  $G/G'$  абелева, в ряду  $G \supset G' \supset G'' \supset \dots \supset G^{(e)} = 1$  существует максимальная инвариантная подгруппа  $A_1 \trianglelefteq G'$ . Так как группа  $G/A_1$  простая и абелева, она — циклическая группа простого порядка. Аналогично, так как группа  $A_1$  разрешима, она содержит максимальную инвариантную подгруппу  $A_2$ , причем фактор-группа  $A_1/A_2$  — циклическая группа также простого порядка. Продолжая это построение, мы получаем ряд  $G = A_0 \supset A_1 \supset \dots \supset A_r = 1$  с циклическими фактор-группами  $A_{i-1}/A_i$ , порядки которых просты. Следовательно, этот ряд композиционный.

1) Исторически это свойство композиционного ряда было первым определением разрешимости, но это определение неприменимо к бесконечным группам. В теории Галуа доказывается, что полиномиальное уравнение  $f(x) = 0$  разрешимо в радикалах тогда и только тогда, когда его группа Галуа разрешима.

**Теорема 9.2.4.** В главном ряду  $G = C_0 \supseteq C_1 \supseteq \dots \supseteq C_s = 1$  разрешимой конечной группы  $G$  фактор-группы  $C_{i-1}/C_i$ ,  $i = 1, \dots, s$ , являются элементарными абелевыми группами.

**Доказательство.** По теореме 8.6.1  $C_{i-1}/C_i$  есть прямое произведение изоморфных между собой простых групп. По теореме 9.2.2 эти простые группы разрешимы, а следовательно, цикличны и имеют простой порядок. Таким образом,  $C_{i-1}/C_i$  является прямым произведением циклических групп одного и того же простого порядка  $p$ , т. е. элементарной абелевой группой. Обратно, если группа  $G$  обладает таким главным рядом, то в силу абелевости его фактор-групп,  $G$  — разрешимая группа. Порядки  $c_1, \dots, c_s$  групп  $C_0/C_1, \dots, C_{s-1}/C_s$  соответственно называются **главными факторами** группы  $G$  и, как показано, являются степенями простых чисел. Ясно, что для фактор-группы  $G/K$  главные факторы образуют подмножество главных факторов всей группы  $G$ , так как существуют главные ряды группы  $G$ , содержащие инвариантную подгруппу  $K$ . Для подгруппы  $H$  группы  $G$  различные члены ряда

$$H \supseteq H \cap C_1 \supseteq H \cap C_2 \supseteq \dots \supseteq H \cap C_s = 1$$

составляют нормальный ряд для  $H$ , который или сам является главным, или допускает уплотнение до главного ряда для  $H$ . Отсюда следует, что главные факторы для  $H$  являются делителями главных факторов для  $G$ , так как группа  $H \cap C_{i-1}/H \cap C_i$  изоморфна некоторой подгруппе группы  $C_{i-1}/C_i$ .

**Теорема 9.2.5.** Следующие два свойства группы  $G$  эквивалентны свойству разрешимости:

1) группа  $G$  обладает конечным инвариантным рядом

$$G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_s = 1,$$

в котором все фактор-группы  $A_{i-1}/A_i$  ( $i = 1, \dots, s$ ) абелевы;

2) группа  $G$  обладает конечным нормальным рядом

$$G = B_0 \supseteq B_1 \supseteq B_2 \supseteq \dots \supseteq B_t = 1,$$

в котором все фактор-группы  $B_{i-1}/B_i$  ( $i = 1, \dots, t$ ) абелевы.

**Доказательство.** Если группа  $G$  разрешима, то ряд из её коммутантов

$$G \supset G' \supset G'' \supset \dots \supset G^{(r)} = 1$$

является конечным инвариантным рядом, в котором фактор-группы  $G^{(i-1)}/G^{(i)}$  абелевы при  $i = 1, \dots, r$ , откуда следует свойство (1) и тем более свойство (2). Остается показать, что из свойства (2) следует разрешимость. Если  $G = B_0 \supseteq B_1 \supseteq \dots \supseteq B_t = 1$

— нормальный ряд с абелевыми фактор-группами  $B_{i-1}/B_i$  при  $i = 1, \dots, t$ , то в силу абелевости группы  $G/B_1 = B_0/B_1$  имеем  $B_1 \supseteq G'$ . Аналогично, если  $B_{i-1} \supseteq G^{(i-1)}$ , то  $B_i \supseteq B'_{i-1} \supseteq G^{(i)}$ . Поэтому  $1 = B_t \supseteq G^{(t)}$  и  $G^{(t)} = 1$ , т. е. группа  $G$  разрешима.

**Следствие 9.2.1.** *Группа  $G$  разрешима, если она обладает такой инвариантной подгруппой  $H$ , что  $H$  и  $G/H$  — разрешимые группы.*

Если  $G/H \supseteq A_1/H \supseteq \dots \supseteq A_{r-1}/H \supseteq H/H$  и  $H \supseteq B_1 \supseteq \dots \supseteq B_{s-1} \supseteq 1$  — ряды, удовлетворяющие свойству (2) групп  $G/H$  и  $H$  соответственно, то ряд  $G \supseteq A_1 \supseteq \dots \supseteq A_{r-1} \supseteq H \supseteq B_1 \supseteq \dots \supseteq B_{s-1} \supseteq 1$  удовлетворяет свойству (2) группы  $G$ .

### 9.3. Обобщенные силовские теоремы для разрешимых групп

Силовская подгруппа конечной группы обладает тем свойством, что ее порядок  $m = p^a$  взаимно прост с ее индексом  $n$ . Ф. Холл [1] показал, что теоремы Силова обобщаются в случае разрешимых групп для таких подгрупп, порядок которых  $m$  взаимно прост с их индексом  $n$ ; при этом не требуется, чтобы порядок  $m$  подгруппы обязательно был степенью простого числа.

**Теорема 9.3.1.** *Пусть  $G$  — разрешимая группа порядка  $tnp$  при  $(m,n)=1$ . Тогда*

1)  *$G$  обладает по меньшей мере одной подгруппой порядка  $m$ ;*

2) *любые две подгруппы порядка  $m$  сопряжены;*

3) *любая подгруппа, порядок  $m'$  которой делит  $m$ , содержится в подгруппе порядка  $m$ ;*

4) *число  $h_m$  подгрупп порядка  $m$  может быть представлено как произведение сомножителей, каждый из которых, во-первых, сравним с 1 по модулю некоторого простого делителя числа  $m$  и, во-вторых, является степенью простого числа, делящего один из главных факторов группы  $G$ .*

**Доказательство.** Отметим, что для  $m = p^a$  свойства (1) и (3) составляют содержание первой теоремы Силова (теорема 4.2.1), свойство (2) — это вторая теорема Силова, а свойство (4) — утверждение более сильное, чем третья теорема Силова.

Доказательство будем вести индукцией по порядку группы  $G$ . Теорема очевидна, если порядок  $G$  равен степени простого числа. В доказательстве будет существенно использована теорема 8.3.3 о строении главных рядов группы  $G$ , а также теорема 2.3.4 о строении фактор-групп.

**Случай 1.** *Группа  $G$  обладает собственной инвариантной подгруппой  $H$  порядка  $t_1n_1$  и индекса  $t_2n_2$ , где  $m = t_1t_2$ ,  $n = n_1n_2$  и  $n_1 < n$ .*

**Свойство (1).** Группа  $G/H$  в силу предположения индукции содержит подгруппу порядка  $m_2$ , которой соответствует подгруппа  $D$  группы  $G$  порядка  $mn_1$ .  $D$  по индукции содержит подгруппу порядка  $m$ .

**Свойство (2).** Если  $M$  и  $M'$  — две подгруппы порядка  $m$ , то порядки подгрупп  $M \cup H = MH$  и  $M' \cup H = M'H$  делят число  $m_1m_2 \cdot m_1n_1$ , так как  $M \cup H / H \cong M/M \cap H$  (теорема 2.4.1). Так как порядок этих подгрупп также делит  $mn$ , то он делит и  $mn_1$ . Но он, кроме того, кратен  $m$  и  $n_1$ . Следовательно, порядки подгрупп  $M \cup H$  и  $M' \cup H$  равны  $mn_1 = m_1n_1m_2$ , а потому  $M \cup H / H$  и  $M' \cup H / H$  — подгруппы группы  $G/H$  порядка  $m_2$ , которые, по предположению индукции, сопряжены. Если элемент  $a^*$  группы  $G/H$  трансформирует  $M' \cup H / H$  в  $M \cup H / H$  и  $a^*$  — образ  $a \in G$  при гомоморфизме  $G \rightarrow G/H$ , то образом  $a^{-1}(M' \cup H) a = M \cup H$ . Здесь подгруппы  $a^{-1}M'a$  и  $M$  имеют порядок  $m$  и содержатся в подгруппе  $M \cup H$ . В силу предположения индукции они сопряжены. Следовательно, подгруппы  $M$  и  $M'$  сопряжены в группе  $G$ .

**Свойство (3).** Если  $M_1$  — подгруппа порядка  $m'$ , где  $m'$  делит  $m$ , то порядок группы  $M_1 \cup H / H$  делит  $m_2$ , и, следовательно, последняя подгруппа содержится в подгруппе порядка  $m_2$  группы  $G/H$ . Таким образом,  $M_1$  содержится в соответствующей подгруппе порядка  $mn_1$  группы  $G$ , и опять в силу предположения индукции подгруппа  $M_1$  содержится в подгруппе порядка  $m$ .

**Свойство (4).** Будем исходить из доказательства свойства (2). Число  $h_m$  подгрупп, сопряженных с подгруппой  $M$  порядка  $m$ , равно произведению  $h_{m_2}$  (числа подгрупп порядка  $m_2$  группы  $G/H$ ) и числа подгрупп, сопряженных с  $M$  в группе  $M \cup H = D$ . При этом главные факторы подгруппы  $D$  делят главные факторы группы  $G$ , а главные факторы для  $G/H$  составляют подмножество совокупности главных факторов для  $G$ . Таким образом,  $h_m$  есть произведение двух сомножителей, каждый из которых в силу предположения индукции обладает свойством (4), что доказывает это свойство и для  $h_m$ .

Порядок наименьшей инвариантной подгруппы  $K$  главного ряда равен  $p^a$ , где  $p$  — простое число. Группа  $K$  удовлетворяет требованиям, сформулированным для подгруппы  $H$ , кроме того случая, когда  $n = p^a$ . Таким образом, мы можем считать, что порядок любого минимального нормального делителя равен  $p^a$ . Но этот нормальный делитель является силовской подгруппой порядка  $p^a$ , поэтому существует только один такой нормальный делитель.

**Случай 2.** Группа  $G$  содержит единственный минимальный нормальный делитель  $K$  порядка  $n = p^a$ .

**Свойство (1).** Пусть  $L$  — минимальный нормальный делитель, строго содержащий  $K$ . Тогда порядок группы  $L/K$  равен  $q^b$ , где  $q \neq p$ . Пусть  $Q$  — силовская подгруппа группы  $L$  порядка  $q^b$ , и пусть  $M$  — нормализатор подгруппы  $Q$  в  $G$ . Рассмотрим  $M \cap K = T$ .  $T$  — инвариантная подгруппа группы  $M$ , которая, будучи подгруппой группы  $K$ , является элементарной абелевой  $p$ -группой. Любой элемент из  $T$  перестановочен с любым элементом из  $Q$ , так как коммутатор любого элемента из  $Q$  и любого элемента из  $T$  принадлежит подгруппе  $T \cap Q = 1$ . Следовательно,  $T$  содержится в центре  $C$  подгруппы  $L$ , который, являясь характеристической подгруппой в  $L$ , инвариантен во всей группе  $G$ . Так как  $K$  — единственная минимальная инвариантная подгруппа, то или  $C = K$ , или  $C = 1$ . Если  $C = K$ , то  $L = K \times Q$  и  $Q$  — инвариантна в  $G$ , что противоречит единственности подгруппы  $K$ . Следовательно,  $T = C = 1$ . Таким образом,  $Q$  совпадает со своим нормализатором в  $L$ , и число подгрупп в  $L$ , сопряженных с  $Q$ , равно индексу  $Q$  в  $L$ , т. е.  $n = p^a$ . Любая подгруппа, сопряженная с  $Q$  во всей группе  $G$ , содержится в  $L$ , так как  $L$  — нормальный делитель. Итак,  $Q$  имеет  $n = p^a$  сопряженных подгрупп в  $G$ , и, следовательно, индекс подгруппы  $M$  в  $G$  равен  $n = p^a$ , а ее порядок равен  $m$ .

**Свойства (2) и (4).** Нормализаторы всех  $p^a$  сопряженных с  $Q$  подгрупп сопряжены и различны. Таким образом, мы имеем  $p^a$  сопряженных подгрупп порядка  $m$ . Кроме того,  $p^a \equiv 1 \pmod{q}$ , так как  $p^a$  — это число силовских подгрупп порядка  $q^b$  в группе  $L$ . Если теперь  $M'$  — любая подгруппа порядка  $m$ , то порядок подгруппы  $M' \cup L$  делится на  $m$  и  $n$ , откуда  $M' \cup L = G$ . Так как  $G/L = M'/M' \cap L$ , порядок подгруппы  $M' \cap L$  равен  $q^b$ , и, следовательно, она сопряжена с  $Q$ . Кроме того,  $M' \cap L$  — инвариантная подгруппа в  $M'$ , откуда  $M'$  — нормализатор некоторой подгруппы, сопряженной с  $Q$ . Таким образом, уже найденные  $p^a$  сопряженных подгрупп порядка  $m$  исчерпывают всю совокупность подгрупп порядка  $m$ . Этим доказаны свойства (2) и (4).

**Свойство (3).** Пусть  $M'$  — подгруппа порядка  $m'/m$ . Если порядок  $M$  равен  $m$ , то порядок подгруппы  $M \cap (M' \cup K) = M^*$  равен  $m'$  и в силу свойства (2) группы  $M' \cup K$  подгруппа  $M^*$  сопряжена с  $M'$ . Следовательно,  $M'$  содержится в подгруппе, сопряженной с  $M$ . Этим свойство (3) доказано.

Приведенные выше свойства разрешимых групп обычно нарушаются в простых группах. Простая группа порядка 60 (знакопеременная группа пятой степени) не содержит подгрупп порядка 15, а потому свойство (1) нарушается; она содержит подгруппу порядка 6, порожденную подстановками (123) и (12)(45), которая не содержится в подгруппе порядка 12; таким образом, здесь нарушается свойство (3). Наконец, число силовских подгрупп

порядка 5 равно 6, но так как  $6 = 2 \cdot 3$ , свойство (4) также не выполняется. Группа автоморфизмов элементарной абелевой группы  $A$  порядка 8 — простая группа  $G$  порядка 168.  $G$  представляет транзитивно семь подгрупп группы  $A$  порядка 2, а также семь подгрупп порядка 4. Следовательно, группа  $G$  обладает двумя различными множествами сопряженных подгрупп индекса 7 и порядка 24, поэтому нарушается свойство (2).

В действительности первое свойство теоремы 9.3.1 характеризует разрешимые группы. Для доказательства этого факта нам понадобится следующая теорема, которая будет доказана в главе 16 как теорема 16.8.7.

**Теорема 9.3.2.** (Теорема Бернсайда.) *Группа порядка  $p^aq^b$ , где  $p$  и  $q$  — простые числа, разрешима.*

Предполагая, что эта теорема доказана, мы можем характеризовать разрешимые группы свойством (1). В группе  $G$  порядка  $g$  под  $p$ -дополнением мы понимаем подгруппу  $S_p'$ , индекс которой  $p^e$  является наивысшей степенью числа  $p$ , делящей порядок  $g$  группы  $G$ .

Первое свойство доказанной теоремы утверждает, в частности, существование  $p$ -дополнений в разрешимых группах. С помощью теоремы Бернсайда мы докажем обратное утверждение.

**Теорема 9.3.3.** *Если группа  $G$  содержит  $p$ -дополнение для любого простого  $p$ , делящего ее порядок, то  $G$  — разрешимая группа.*

**Доказательство.** Пусть порядок группы  $G$  равен  $g = p_1^{e_1} \dots p_r^{e_r}$ , где  $p_i$  — простые числа. Если  $H_1$  и  $H_2$  — подгруппы индексов  $p_i^{e_i}$  и  $p_j^{e_j}$  соответственно, то индекс подгруппы  $H_{12} = H_1 \cap H_2$  равен  $p_i^{e_i} p_j^{e_j}$ , так как индексы  $p_i^{e_i}$  и  $p_j^{e_j}$  взаимно прости (теорема 1.5.6). Пересечение  $H_{12}$  с  $p_k$ -дополнением опять в силу теоремы 1.5.6 имеет индекс  $p_i^{e_i} p_j^{e_j} p_k^{e_k}$ . Продолжая этот процесс, мы можем найти подгруппу порядка  $m$  и индекса  $n$ , где  $(m, n) = 1$ , которая является пересечением  $p$ -дополнений для простых  $p$ , делящих  $n$ . Таким образом, существования  $p$ -дополнений достаточно для доказательства существования подгруппы порядка  $m$ , взаимно простого с индексом  $n$ , и тем самым для доказательства свойства (1).

Предположим, что теорема верна для групп, порядки которых меньше  $g$ , и докажем теорему индукцией по  $g$ . В группе порядка  $p^a$  индекс любой максимальной подгруппы равен  $p$ , причем эта подгруппа инвариантна (следствие 4.1.2), а, следовательно, группа порядка  $p^a$  разрешима. В силу принятой без доказательства теоремы Бернсайда группа порядка  $p^aq^b$  разрешима. Поэтому мы можем ограничиться рассмотрением случаев, когда порядок

группы  $G$  делится по меньшей мере на три различных простых числа. Группа  $G$  содержит подгруппу  $H$  порядка  $p^aq^b = m$ , взаимно простого с индексом  $n$ , причем  $p$  и  $q$  — различные простые числа, делящие  $n$ . Подгруппа  $H$ , будучи разрешимой группой, содержит наименьшую инвариантную подгруппу  $K$ , являющуюся, согласно теореме 9.2.4, элементарной абелевой группой, порядок которой равен степени простого числа, например  $p^i$ . Тогда  $K$  содержится в силовской подгруппе  $P \subseteq H \subseteq G$  порядка  $p^a$ . При этом  $q$ -дополнение  $L^*$  в группе  $G$  содержит силовскую подгруппу  $P^*$ , сопряженную с подгруппой  $P$  в  $G$ . Следовательно, трансформирование некоторым элементом из  $G$  отображает  $L^*$  на некоторое  $q$ -дополнение  $L$ , содержащее  $P$ . Значит,  $L \supseteq P$  и  $H \supseteq P$ , а рассмотрение порядков показывает, что  $L \cap H = P$ ,  $L \cup H = G$  и даже  $LH = G$ , так как множество  $LH$  содержит  $g$  различных элементов. Таким образом, каждый смежный класс по подгруппе  $L$  содержит один элемент из  $H$ , и, следовательно, все подгруппы, сопряженные с  $L$ , получаются трансформированием элементами  $h \in H$ . Но  $h^{-1}Lh \supseteq K$ , так как в силу инвариантности  $K$  в  $H$   $h^{-1}Kh = K$ . Поэтому пересечение  $M$  всех подгрупп, сопряженных с  $L$ , — собственная подгруппа группы  $G$ , так как  $K \subseteq M \subset L$ ; оно к тому же является нормальным делителем, так как  $M$  — пересечение полного класса взаимно сопряженных подгрупп.

Итак,  $G$  содержит собственную инвариантную подгруппу  $M$ . Если  $S'_p$  —  $p$ -дополнение в группе  $G$ , то  $S'_p \cap M$  —  $p$ -дополнение в  $M$ , а  $S'_p \cup M/M$  —  $p$ -дополнение в фактор-группе  $G/M$ . Следовательно, группы  $M$  и  $G/M$  обладают  $p$ -дополнениями и, в силу предположения индукции, разрешимы. Отсюда следует разрешимость группы  $G$ .

#### 9.4. Дальнейшие результаты о разрешимых группах

**Теорема 9.4.1.** *Если  $G$  — разрешимая группа порядка  $g$  и  $n$  — такой делитель  $g$ , что уравнение  $x^n = 1$  имеет точно  $n$  решений, то эти решения образуют инвариантную подгруппу группы  $G$ .*

**Доказательство.** Теорема верна, если  $g$  — простое число. Предположим, что она также верна для разрешимых групп порядков, меньших  $g$ . Будучи разрешимой группой,  $G$  содержит минимальную инвариантную подгруппу  $K$ , которая является элементарной абелевой группой порядка  $p^l$ . Рассмотрим два случая:  $p$  делит  $n$  и  $p$  не делит  $n$ .

**Случай 1.  $p$  делит  $n$ .**

Тогда порядок каждого элемента подгруппы  $K$  равен  $p$  и, следовательно, все элементы являются решениями уравнения  $x^n = 1$ .

Пусть  $n = p^j n_1$ ,  $g = p^s g_1$ . Порядок фактор-группы  $G/K$  равен  $p^{s-i} g_1$ ; он делится на  $u = p^{j-i} n_1$ , если  $j \geq i$ , и на  $u = n_1$ , если  $j < i$ . Поэтому в группе  $G/K$  найдутся  $ku$  элементов  $z$ , таких, что  $z^u = 1$ . Если теперь  $x$  — такой элемент из группы  $G$ , что  $x$  отображается в  $z$  при гомоморфизме  $G \rightarrow G/K$ , то  $x^u \in K$ , так как  $z^u = 1$ . Отсюда  $x^{up} = 1$ , но  $up$  делит  $n$ . Поэтому  $x^n = 1$  для любого такого элемента  $x$ . Эти элементы  $x$  составляют  $ku$  смежных классов по  $K$  в группе  $G/K$ . Следовательно, существует по меньшей мере  $kup^i$  элементов  $x$  группы  $G$ , удовлетворяющих уравнению  $x^n = 1$ . Но если  $j < i$ , то  $up^i$  — собственное кратное  $n$ , т. е. при этом предположении получается больше, чем  $n$ , решений уравнения  $x^n = 1$ , что по условию невозможно. Следовательно,  $j \geq i$ ,  $up^i = n$  и существует не менее  $kn$  решений. Отсюда  $k = 1$  и уравнение  $z^u = 1$  имеет точно  $u$  решений в группе  $G/K$ . Согласно предположению индукции, эти  $u$  решений образуют инвариантную подгруппу  $H/K$  группы  $G/K$ , ее полный прообраз  $H$  в группе  $G$  является инвариантной подгруппой порядка  $up^i = n$ , элементы которой составляют как раз  $n$  решений уравнения  $x^n = 1$ .

### Случай 2. $p$ не делит $n$ .

В этом случае  $n$  делит порядок группы  $G/K$  и существует  $kn$  решений уравнения  $z^n = 1$  в фактор-группе  $G/K$ . Если  $y \in G$  и  $y \rightarrow z$  при естественном гомоморфизме, то  $y^n \in K$  и  $y^{pn} = 1$ . Следовательно, в группе  $G$  имеются  $kn$  смежных классов по  $K$ , состоящих из элементов  $y$ , для которых  $y^{pn} = 1$ . Мы утверждаем, что каждый смежный класс  $Ky$  дает точно одно решение уравнения  $x^n = 1$ . Пусть  $Ky_1$  и  $Ky_2$  — различные смежные классы по  $K$ , причем  $y_1 \rightarrow z_1$ ,  $y_2 \rightarrow z_2$ ,  $z_1 \neq z_2$ . При этом  $y_1^{pn} = 1$ ,  $y_2^{pn} = 1$ , следовательно, элементы  $y_1^p = x_1$  и  $y_2^p = x_2$  являются решениями уравнения  $x^n = 1$  в группе  $G$ . Если  $y_1^p = y_2^p$ , то  $z_1^p = z_2^p$ . Но  $z_1^n = 1$ ,  $z_2^n = 1$  и  $(p, n) = 1$ , откуда  $z_1 = z_2$ , что противоречит нашему допущению. Следовательно, если уравнение  $z^n = 1$  имеет  $kn$  решений в группе  $G/K$ , то уравнение  $x^n = 1$  имеет не менее  $kn$  решений в группе  $G$ . Отсюда  $k = 1$ , и в силу предположения индукции  $G/K$  содержит инвариантную подгруппу  $U/K$  порядка  $n$ . Соответствующая подгруппа  $U$  группы  $G$  имеет порядок  $p^i n$ . Но, будучи разрешимой группой,  $U$  содержит  $p$ -дополнение  $H$  порядка  $n$ . Таким образом,  $n$  элементов подгруппы  $H$  — это  $n$  решений уравнения  $x^n = 1$ , и так как трансформирование произвольным элементом из  $G$  переставляет эти решения между собой, то  $H$  — нормальный делитель в  $G$ .

**Теорема 9.4.2.** *Если две соседние фактор-группы производного ряда  $G' \supset G'' \supset G''' \supset \dots$  группы  $G$  цикличны, то вторая из них — единичная группа.*

*Доказательство.* Будем считать, что  $G''' = 1$  и фактор-группы  $G'/G''$  и  $G''/G'''$  циклически. Покажем, что  $G'' = 1$ . Пусть  $b$  — образующий элемент группы  $G''$ .  $G$  является нормализатором подгруппы  $G''$ , а фактор-группа  $G/Z_b$ , где  $Z_b$  — централизатор  $G''$ , изоморфна группе автоморфизмов циклической группы и потому абелева. Следовательно,  $Z_b \supseteq G'$ . Но тогда  $G''$  содержится в центре подгруппы  $G'$ .  $G'$  получается присоединением к  $G''$  одного элемента. Следовательно, подгруппа  $G'$  абелева, откуда  $G'' = 1$ , что и требовалось доказать.

Группа  $G$  называется *метациклической*, если группы  $G/G'$  и  $G'$  циклические. Тогда  $G'' = 1$ , и метациклическая группа  $G$  имеет *производный ряд длины 2* (т. е. является двуступенчатой метациклической группой). В силу теоремы 9.4.2 не существует трехступенчатых метациклических групп.

**Теорема 9.4.3.** *Если силовские подгруппы конечной группы  $G$  порядка  $g$  все циклически, то  $G$  — метациклическая группа, порожденная двумя элементами  $a$  и  $b$  с определяющими отношениями:*

$$\begin{aligned} a^m &= 1, \quad b^n = 1, \quad b^{-1}ab = a^r, \\ mn &= g, \quad [(r-1), nm] = 1, \\ r^n &\equiv 1 \pmod{m}. \end{aligned}$$

*Обратно, группа, заданная этими определяющими отношениями, обладает только циклическими силовскими подгруппами.*

*Доказательство.* Сначала нужно показать, что группа  $G$  разрешима. Пусть  $g = p_1^{e_1} \dots p_s^{e_s}$ ,  $p_1 < p_2 < \dots < p_s$ , где  $p_i$  — простые числа. Покажем, что для  $m = p_j^{f_j} p_{j+1}^{e_{j+1}} \dots p_s^{e_s}$ ,  $f_j \leq e_j$  уравнение  $x^m = 1$  имеет точно  $m$  решений. При  $m = g$  это, безусловно, верно. Следовательно, достаточно проверить, что если уравнение  $x^{mp} = 1$  имеет точно  $mp$  решений и  $p$  — наименьшее простое число, делящее  $mp$ , то уравнение  $x^m = 1$  имеет точно  $m$  решений. Так как силовская  $p$ -подгруппа циклическа, то, обозначая через  $p^{f+1}$  наивысшую степень  $p$ , делящую  $mp$ , получаем, что в группе  $G$  существуют элементы порядка  $p^{f+1}$ . Поэтому не все решения уравнения  $x^{mp} = 1$  являются решениями уравнения  $x^m = 1$ . Следовательно,  $km$  решений последнего уравнения в силу теоремы 9.1.2 составляют некоторое собственное подмножество множества решений уравнения  $x^{mp} = 1$ , и потому  $1 \leq k < p$ . Элемент, удовлетворяющий уравнению  $x^{mp} = 1$ , но не удовлетворяющий уравнению  $x^m = 1$ , имеет порядок  $t$ , который делится точно на степень  $p^{f+1}$  простого числа  $p$ . Существует  $\varphi(t)$ <sup>1)</sup> элементов, порождающих

<sup>1)</sup>  $\varphi(t)$  — функция Эйлера. ( $\varphi(t)$  — число классов вычетов по модулю  $t$ , взаимно простых с  $t$ .) — Прим. перев.

ту же циклическую группу, порядок которой делится точно на  $p^{f+1}$ . Далее, так как  $t$  делится на  $p^{f+1}$ ,  $\varphi(t)$  делится на  $p - 1$ . Следовательно,  $pm - km = (p - k)m$  — число элементов, удовлетворяющих уравнению  $x^{pm} = 1$ , но не удовлетворяющих уравнению  $x^m = 1$ , — делится на  $p - 1$ . Поскольку  $p$  — наименьшее простое число, делящее  $m$ ,  $p - 1$  взаимно просто с  $m$ . Таким образом,  $p - 1$  делит  $p - k$ , а так как  $1 \leq k < p$ , это возможно только в случае  $k = 1$ , т. е. когда уравнение  $x^m = 1$  имеет точно  $m$  решений. В частности, последнее утверждение справедливо, когда  $m = p_s^e$ . Но существует силовская подгруппа этого порядка, которая, следовательно, инвариантна в  $G$ . Она циклическа и потому, конечно, разрешима.

Мы доказали, что группа  $G$  с циклическими силовскими подгруппами обладает инвариантной подгруппой  $H$ . Но в таком случае группы  $H$  и  $G/H$  также содержат только циклические силовские подгруппы. Можно предположить по индукции, что  $H$  и  $G/H$  — разрешимые группы и, следовательно, что  $G$  — также разрешимая группа, так как группа простого порядка разрешима.

Абелева группа, силовские подгруппы которой циклически, сама циклическа. Следовательно, в ряду  $G \supset G' \supset G'' \supset \dots$  факторгруппы циклически и, следовательно, в силу теоремы 9.4.2,  $G'' = 1$ . Если  $G' = 1$ , то  $G$  — циклическая группа, и этот случай отпадает, если считать, что  $b = 1$ ,  $r = 1$ ,  $n = 1$ ,  $m = g$ . Поэтому допустим, что  $G' \neq 1$ ,  $a$  — образующий элемент подгруппы  $G'$ ,  $a^m = 1$ . Пусть  $b$  — элемент из смежного класса  $G'b$ , порождающего циклическую фактор-группу  $G/G'$ . Тогда элементы  $a$  и  $b$  порождают группу  $G$  и  $b^{-1}ab = a^r$ , где  $r \neq 1$ , так как  $G'$  — инвариантная подгруппа. Если бы  $r$  было равно 1, группа  $G$  была бы абелевой и тем самым — циклической, что противоречит предположению. Если порядок группы  $G/G'$  равен  $n$ , то  $b^{-n}ab^n = a^{rn} = a$ , откуда  $r^n \equiv 1 \pmod{m}$ . Любой элемент из  $G$  может быть представлен в виде  $b^j a^l$ , поэтому коммутатор  $(b^u a^v, b^j a^l)$  может быть представлен как произведение коммутаторов вида  $(a^k, b^l)$ , которые в свою очередь являются степенями коммутатора  $a^{-1}b^{-1}ab = a^{r-1}$ . Следовательно, элемент  $a^{r-1}$  порождает подгруппу  $G'$ , и потому  $(r - 1, m) = 1$ . Далее, элемент  $b^n \in G'$  является степенью  $a^j$  элемента  $a$ , которая перестановочна с  $b$ , откуда  $a^{rj} = a^j$ , но так как  $(r - 1, m) = 1$ , то  $j = 0$ , т. е.  $b^n = 1$ . Если бы числа  $m$  и  $n$  имели общим делителем простое число  $p$ , то элементы  $a^{m/p}$  и  $b^{n/p}$  порождали бы нециклическую подгруппу порядка  $p^2$ , но это противоречит условию, что все силовские подгруппы циклические. Поэтому  $(m, n) = 1$ . Этим доказано прямое утверждение теоремы.

Докажем обратное утверждение. Пусть числа  $m$ ,  $n$ ,  $r$  и  $g$  удовлетворяют отношениям, указанным в теореме. Тогда отображение  $a \rightarrow a^r$  в силу сравнения  $r^n \equiv 1 \pmod{m}$  является автоморфизмом циклической группы, порожденной элементом  $a$ , порядок которого делит  $n$ . Теперь  $mn$  элементов вида  $b^j a^l$ , где индексы  $j$  и  $i$  рассматриваются соответственно по модулям  $n$  и  $m$ , образуют группу относительно закона умножения  $b^j a^l \cdot b^k a^t = b^{j+k} a^{l+t}$ , где  $h = ir_k + t$ . Выполнение ассоциативного закона и существование обратных элементов можно проверить. Итак, мы имеем группу порядка  $g = mn$  с определяющими отношениями  $a^m = 1$ ,  $b^n = 1$ ,  $b^{-1}ab = a^r$ , причем отметим, что закон умножения является следствием этих определяющих отношений. В этой группе любой коммутатор является степенью коммутатора  $a^{-1}b^{-1}ab = a^{r-1}$ , откуда в силу равенства  $(r-1, m) = 1$  подгруппа  $G'$  порождается элементом  $a$ . Так как  $(m, n) = 1$ , любая силовская подгруппа сопряжена с подгруппой  $\{a\}$  или подгруппой  $\{b\}$  и поэтому также циклична.

**Следствие 9.4.1.** Любая группа  $G$  порядка, свободного от квадратов, — метациклическая группа типа, указанного в теореме 9.4.3.

Это следует из того, что все силовские подгруппы имеют простые порядки, т. е. они цикличны.

## Упражнения

1. Пусть порядок конечной группы  $G$  делится на 12 и уравнение  $x^{12} = 1$  имеет точно 12 решений в  $G$ . Показать, что эти решения образуют инвариантную подгруппу.

2. Пусть порядок группы  $G$  равен  $p^2q$ , где  $p$  и  $q$  — различные простые числа. Показать, что в таком случае одна из силовских подгрупп инвариантна, а группа  $G$  разрешима.

3. Пусть порядок группы  $G$  равен  $p^2qr$ , где  $p$ ,  $q$  и  $r$  — различные простые числа. Показать, что в таком случае или  $G$  — разрешимая группа, или  $G$  — знакопеременная группа  $A_5$  порядка 60. (Использовать теорему 14.3.1 и ее следствие.)

4. Пусть уравнение  $x^n = 1$  имеет точно  $m$  решений  $x_1 = 1, x_2, \dots, x_m$  в группе  $G$ . Показать, что  $K = \{x_1, \dots, x_m\}$  — инвариантная подгруппа, ее элементы представимы в виде произведения  $x_2^{a_2} x_3^{a_3} \dots x_m^{a_m}$  и порядок подгруппы  $K$  не превосходит  $(m-1)^n$ .

## Глава 10

# СВЕРХРАЗРЕШИМЫЕ И НИЛЬПОТЕНТНЫЕ ГРУППЫ

### 10.1. Определения

Существуют еще два групповых свойства, качественно более сильных, чем разрешимость. Это *сверхразрешимость* и *нильпотентность*.

**ОПРЕДЕЛЕНИЕ.** Группа  $G$  сверхразрешима, если она обладает конечным инвариантным рядом  $G = A_0 \supseteq A_1 \supseteq \dots \supseteq A_r = 1$ , в котором каждая фактор-группа  $A_{i-1}/A_i$  циклична.

**ОПРЕДЕЛЕНИЕ.** Группа  $G$  нильпотента, если она обладает конечным инвариантным рядом  $G = A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_r = 1$ , в котором каждая фактор-группа  $A_{i-1}/A_i$  содержится в центре группы  $G/A_i$ .

Так как в обоих случаях группы  $A_{i-1}/A_i$  абелевы, из сверхразрешимости и нильпотентности следует разрешимость группы  $G$ . Заметим, что в сверхразрешимой группе  $G$   $A_{i-1} = \{b_{i-1}, A_i\}$ , где  $b_{i-1}$  — любой элемент из  $A_{i-1}$ , отображаемый<sup>1)</sup> в образующий элемент циклической группы  $A_{i-1}/A_i$ , и, следовательно,  $G$  — группа с конечным числом образующих. Так как класс нильпотентных групп включает все абелевы группы, то ясно, что нильпотентная группа не обязательно допускает конечное число образующих.

Бэр [12] определяет сверхразрешимость в более общем смысле: группа  $G$  сверхразрешима, если любой гомоморфный образ группы  $G$  содержит циклическую инвариантную подгруппу. Он показал, что это определение эквивалентно нашему для групп с конечным числом образующих. Но группы, сверхразрешимые в его более общем смысле, не обладают, вообще говоря, свойствами, которые будут доказаны в этой главе.

### 10.2. Нижний и верхний центральные ряды

Будем, как и прежде, обозначать коммутатор  $x^{-1}y^{-1}xy$  через  $(x, y)$ . Если  $A$  и  $B$  — подгруппы, то  $(A, B)$  — это группа, порожденная всеми коммутаторами  $(a, b)$ , где  $a \in A$ ,  $b \in B$ . Мы определили *простой коммутатор* следующим образом:

$$(x_1, \dots, x_{n-1}, x_n) = ((x_1, \dots, x_{n-1}), x_n).$$

<sup>1)</sup> При естественном гомоморфизме. — Прим. ред.

Аналогичное определение введем для подгрупп  $A_1, \dots, A_{n-1}, A_n$ :

$$(A_1, \dots, A_{n-1}, A_n) = ((A_1, \dots, A_{n-1}), A_n).$$

Для удобства обозначим  $x^{-1}ax$  через  $a^x$ . Выпишем ряд важных тождеств для сложных коммутаторов:

$$(y, x) = (x, y)^{-1}, \quad (10.2.1.1)$$

$$(xy, z) = (x, z)^y (y, z) = (x, z)(x, z, y)(y, z), \quad (10.2.1.2)$$

$$(x, yz) = (x, z)(x, y)^z = (x, z)(x, y)(x, y, z), \quad (10.2.1.3)$$

$$(x, y^{-1}, z)^y (y, z^{-1}, x)^z (z, x^{-1}, y)^x = 1, \quad (10.2.1.4)$$

$$(x, y, z)(y, z, x)(z, x, y) =$$

$$= (y, x)(z, x)(z, y)^x (x, y)(x, z)^y (y, z)^x (x, z)(z, x)^y. \quad (10.2.1.5)$$

Они непосредственно вытекают из определения коммутатора. Определим ряд подгрупп группы  $G$  следующими формулами:

$$\Gamma_1(G) = G,$$

$$\Gamma_k(G) = \{(x_1, \dots, x_k)\}$$

для произвольных  $x_i \in G$ .

Так как  $(y_1, y_2, \dots, y_{k+1}) = [(y_1, y_2), y_3, \dots, y_{k+1}]$ , то для всех  $k$  справедливы включения  $\Gamma_{k+1}(G) \subseteq \Gamma_k(G)$ . Очевидно, что  $\Gamma_k(G)$  — вполне характеристическая подгруппа группы  $G$ . Ряд

$$G = \Gamma_1(G) \supseteq \Gamma_2(G) \supseteq \Gamma_3(G) \supseteq \dots$$

называется *нижним центральным рядом* группы  $G$ .

**Теорема 10.2.1.**  $\Gamma_{k+1}(G) = (\Gamma_k(G), G)$ .

*Доказательство.* Так как  $(y_1, \dots, y_k, y_{k+1}) = ((y_1, \dots, y_k), y_{k+1})$ , то включение  $\Gamma_{k+1}(G) \subseteq (\Gamma_k(G), G)$  очевидно. Чтобы доказать обратное включение, воспользуемся равенствами (10.2.1). Положим в (10.2.1.2)  $x = (a_1, \dots, a_k)$ ,  $y = (a_1, \dots, a_k)^{-1}$ ,  $z = a_{k+1}$ . Тогда  $1 = (1, a_{k+1}) = (a_1, \dots, a_k, a_{k+1})^y ((a_1, \dots, a_k)^{-1}, a_{k+1})$ . Отсюда получаем  $((a_1, \dots, a_k)^{-1}, a_{k+1}) \in \Gamma_{k+1}(G)$ , так как остальные члены принадлежат  $\Gamma_{k+1}(G)$ . Подгруппа  $(\Gamma_k(G), G)$  порождается элементами вида  $(u_1 u_2 \dots u_n, g)$ , где  $u_i = (a_1, \dots, a_k)$  или  $u_i = (a_1, \dots, a_k)^{-1}$ . Как мы показали,  $(u_i, g) \in \Gamma_{k+1}(G)$ . Полной индукцией по  $n$  покажем, что  $(u_1 u_2 \dots u_n, g) \in \Gamma_{k+1}(G)$ . Для этого положим в (10.2.1.2)  $x = u_1 u_2 \dots u_{n-1}$ ,  $y = u_n$ ,  $z = g$ . Тогда получим  $(u_1 \dots u_{n-1} u_n, g) = (u_1 \dots u_{n-1}, g)^{u_n} (u_n, g)$ . По предположению индукции элемент в правой части принадлежит подгруппе  $\Gamma_{k+1}(G)$ , откуда  $(\Gamma_k(G), G) \subseteq \Gamma_{k+1}(G)$ , и теорема доказана. Из нее вытекает важное следствие.

**Следствие 10.2.1.** Группа  $\Gamma_k(G)/\Gamma_{k+1}(G)$  содержится в центре фактор-группы  $G/\Gamma_{k+1}(G)$ .

Мы можем также определить *верхний центральный ряд* группы  $G$ :

$$Z_0 = 1 \subseteq Z_1(G) \subseteq Z_2(G) \subseteq \dots \subseteq Z_i(G) \subseteq Z_{i+1}(G) \subseteq \dots,$$

где подгруппа  $Z_{i+1}(G)$  определяется условием  $Z_{i+1}(G)/Z_i(G)$  — *центр группы*  $G/Z_i(G)$ . Так как центр группы — характеристическая (но не обязательно вполне характеристическая) подгруппа, подгруппа  $Z_i$  характеристична в группе  $G$ . Следующая теорема оправдывает термины *верхний* и *нижний* центральные ряды.

Ряд  $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots \supseteq A_{r+1} = 1$ , каждая фактор-группа  $A_i/A_{i+1}$  которого лежит в центре группы  $G/A_{i+1}$ , называется *центральным рядом*.

**Теорема 10.2.2.** *Пусть  $G = A_1 \supseteq A_2 \supseteq A_3 \supseteq \dots \supseteq A_{r+1} = 1$  — центральный ряд группы  $G$ . Тогда  $A_i \supseteq \Gamma_i(G)$ ,  $i = 1, 2, \dots, r+1$  и  $A_{r+1-i} \subseteq Z_j(G)$ ,  $j = 0, 1, \dots, r$ .*

*Доказательство.* Имеем  $A_1 = G = \Gamma_1(G)$ . Предположим,  $A_i \supseteq \Gamma_i(G)$ . Так как фактор-группа  $A_i/A_{i+1}$  принадлежит центру группы  $G/A_{i+1}$ , справедливо включение  $(A_i, G) \subseteq A_{i+1}$ . Но тогда  $\Gamma_{i+1}(G) = (\Gamma_i(G), G) \subseteq (A_i, G) \subseteq A_{i+1}$ . Этим доказано, что  $A_i \supseteq \Gamma_i(G)$  для всех  $i$ . Предположим теперь, что  $A_{r+1-i} \subseteq Z_i(G)$  для некоторого  $i$ . Тогда группа  $T = G/Z_i(G)$  есть гомоморфный образ группы  $U = G/A_{r+1-i}$  с ядром  $Z_i(G)/A_{r+1-i}$ . Группа  $A_{r-i}/A_{r+1-i}$  содержится в центре группы  $U$ , откуда следует, что гомоморфный образ подгруппы  $A_{r-i}/A_{r+1-i}$  должен лежать в центре группы  $T$ . Но этим образом является подгруппа  $A_{r-i} \cup Z_i/Z_i$ , в то время как центр группы  $T$  есть  $Z_{i+1}/Z_i$ . Следовательно,  $A_{r-i} \subseteq A_{r-i} \cup Z_i \subseteq Z_{i+1}$ . Теорема доказана индукцией по  $i$ .

**Следствие 10.2.2.** *В нильпотентной группе  $G$  нижний и верхний центральные ряды имеют одну и ту же конечную длину  $c$ .*

Действительно, если существует конечный центральный ряд длины  $r$ , то из теоремы следует, что длины нижнего и верхнего центральных рядов не превосходят  $r$ . А так как между членами этих рядов имеет место почленное включение, длины их равны. Их общая длина  $c$  называется *классом* нильпотентной группы. Нильпотентная группа класса 1 — это абелева группа.

**Теорема 10.2.3.** *Если группа  $G$  порождается элементами  $x_1, \dots, x_r$ , то фактор-группа  $\Gamma_k(G)/\Gamma_{k+1}(G)$  порождается простыми коммутаторами  $(y_1, y_2, \dots, y_k) \text{ mod } \Gamma_{k+1}(G)$ , где  $y_i$  — некоторые из элементов  $x_1, \dots, x_r$ , причем не обязательно различные.*

**Следствие 10.2.3.** *Если группа  $G$  порождается  $r$  элементами, то фактор-группа  $\Gamma_k(G)/\Gamma_{k+1}(G)$  порождается не более чем  $r^k$  элементами.*

*Доказательство* проведем индукцией по  $k$ . При  $k = 1$  теорема очевидна. Пусть она верна для  $k - 1$ . Подгруппа  $\Gamma_k(G)$  порождается всеми коммутаторами  $C = (a_1, \dots, a_{k-1}, a_k)$ , где  $a_i \in G$ . Далее имеем  $C = ((a_1, \dots, a_{k-1}), a_k)$  и  $(a_1, \dots, a_{k-1}) \in \Gamma_{k-1}(G)$ , откуда, в силу предположения индукции,  $(a_1, \dots, a_{k-1}) = u_1^{\epsilon_1} u_2^{\epsilon_2} \dots u_n^{\epsilon_n} w$ , где  $\epsilon_i = \pm 1$ ,  $u_1, \dots, u_n$  — коммутаторы вида  $(y_1, \dots, y_{k-1})$ , причем  $y_i$  — это некоторые из элементов  $x_j$  и  $w \in \Gamma_k(G)$ . Поэтому  $C = (u_1^{\epsilon_1} u_2^{\epsilon_2} \dots u_n^{\epsilon_n} w, a_k)$ . Применяем соотношение (10.2.1.2).

$$\begin{aligned} C &= (u_1^{\epsilon_1} u_2^{\epsilon_2} \dots u_n^{\epsilon_n}, a_k) (u_1^{\epsilon_1} u_2^{\epsilon_2} \dots u_n^{\epsilon_n}, a_k, w) (w, a_k) \equiv \\ &\equiv (u_1^{\epsilon_1} u_2^{\epsilon_2} \dots u_n^{\epsilon_n}, a_k) (\text{mod } \Gamma_{k+1}). \end{aligned}$$

Но  $a_k = x_{i_1}^{\eta_1} \dots x_{i_m}^{\eta_m}$ ,  $\eta_j = \pm 1$  и  $x_i \in \Gamma_{k-1}$ , откуда повторным применением соотношений (10.2.1.2) и (10.2.1.3) мы получаем, что элемент  $C$  по модулю  $\Gamma_{k+1}$  является произведением коммутаторов вида  $(u_j^{\epsilon_j}, x_{i_s}^{\eta_s})$ . Кроме того, из тех же соотношений следует, что  $(u^{\epsilon}, x^{\eta}) \equiv (u, x)^{\epsilon\eta} \pmod{\Gamma_{k+1}(G)}$ , следовательно, фактор-группа  $\Gamma_k(G)/\Gamma_{k+1}(G)$  порождается коммутаторами вида  $(u, x) \pmod{\Gamma_{k+1}(G)}$  или  $(y_1, \dots, y_{k-1}, x_{i_k}) \pmod{\Gamma_{k+1}(G)}$ , что и требовалось доказать. Заметим, что мы не пользовались конечностью числа  $r$ .

Непосредственным следствием доказанной теоремы является следующая теорема, устанавливающая связь между нильпотентными и сверхразрешимыми группами.

**Теорема 10.2.4. Нильпотентная группа с конечным числом образующих сверхразрешима.**

*Доказательство.* Пусть  $G$  — нильпотентная группа с конечным числом образующих. Пусть

$$G = \Gamma_1(G) \supset \Gamma_2(G) \supset \dots \supset \Gamma_c(G) \supset \Gamma_{c+1}(G) = 1$$

— ее нижний центральный ряд. Поскольку  $\Gamma_c(G)$  — абелева подгруппа с конечным числом образующих, она представима как прямое произведение  $m$  циклических групп, где  $m$  — некоторое натуральное число. Так как  $\Gamma_c(G)$  принадлежит центру группы  $G$ , каждая ее подгруппа инвариантна в  $G$ . Следовательно, существует ряд  $\Gamma_{c+1} = 1 \subset \{a_1\} \subset \{a_1, a_2\} \subset \dots \subset \{a_1, a_2, \dots, a_m\} = \Gamma_c(G)$  инвариантных подгрупп группы  $G$  с циклическими факторами. Аналогично мы можем построить ряд инвариантных подгрупп между  $\Gamma_{i+1}(G)$  и  $\Gamma_i(G)$  с циклическими факторами. В итоге получается ряд для группы  $G$ , который характеризует сверхразрешимость группы.

**Следствие 10.2.4.** *Нильпотентная группа с конечным числом образующих удовлетворяет условию максимальности.*

Группа  $G$  удовлетворяет условию максимальности, если любая возрастающая цепочка ее подгрупп имеет конечную длину. Это условие эквивалентно требованию, чтобы группа  $G$  и любая ее подгруппа обладали конечной системой образующих. Как будет показано в теореме 10.5.1, любая подгруппа сверхразрешимой группы сверхразрешима, а потому имеет конечную систему образующих. Соответствующее утверждение для разрешимых групп не выполняется. Так, если  $F$  — свободная группа с двумя образующими  $a$  и  $b$ , то фактор-группа  $F/F''$  разрешима, но подгруппа  $F'/F''$  имеет бесконечно много образующих вида  $a^{-i}b^{-j}a^i b^j$ .

### 10.3. Теория нильпотентных групп

Если группа  $G$  нильпотентна класса  $c$ , то любой коммутатор  $(a_1, \dots, a_{c+1})$  равен единице, и, обратно, если любой коммутатор вида  $(a_1, \dots, a_{c+1})$  равен единице, то класс нильпотентности группы  $G$  не превосходит  $c$ . Будем говорить, что группа  $G$  обладает свойством *ниль-с*<sup>1)</sup>, если  $(a_1, \dots, a_{c+1}) = 1$  для всех  $a_i \in G$ .

**Теорема 10.3.1.** *Если группа  $G$  обладает свойством ниль-с, то любая подгруппа и фактор-группа группы  $G$  обладают свойством ниль-с.*

**Доказательство.** Если  $G$  ниль-с, то тем более для подгруппы  $H$  все коммутаторы  $(a_1, \dots, a_{c+1})$ , где  $a_i \in H$ , равны 1, следовательно, подгруппа  $H$  ниль-с. Если  $T$  — гомоморфный образ группы  $G$ , то каждый коммутатор  $(b_1, \dots, b_{c+1})$ , где  $b_i \in T$ , является гомоморфным образом некоторого коммутатора  $(a_1, \dots, a_{c+1})$  из группы  $G$ , а следовательно, равен единице, откуда группа  $T$  — ниль-с группа.

Следующая теорема относится к нильпотентным инвариантным подгруппам группы  $G$ , которая сама не обязательно нильпотента.

**Теорема 10.3.2.** *Если  $H$  и  $K$  — инвариантные подгруппы группы  $G$ , причем  $H$  — ниль-с группа, а  $K$  — ниль- $d$  группа, то подгруппа  $H \cup K = HK$  — ниль-( $c+d$ ).*

**Доказательство.** Подгруппа  $\Gamma_m(HK)$  порождается всеми коммутаторами вида  $(u_1, u_2, \dots, u_m)$ , где  $u_i \in HK$ , т. е.  $u_i = h_i k_i$ ,  $h_i \in H$ ,  $k_i \in K$ . Мы утверждаем, что элемент  $(u_1, u_2, \dots, u_m)$  является произведением коммутаторов вида  $w = (v_1, v_2, \dots, v_m)$ , где каждый элемент  $v_i$  принадлежит либо  $H$ , либо  $K$ . Для  $m=1$  это очевидно. Пусть это верно для  $m-1$ . Тогда, применяя равенство

<sup>1)</sup> Или является ниль-с группой. — Прим. ред.

(10.2.1.3) и пользуясь инвариантностью подгрупп  $H$  и  $K$ , получаем  
 $(u_1, \dots, u_{m-1}, u_m) = (w_1 w_2 \dots w_t, h_m k_m) =$

$$\begin{aligned} &= (w_1 \dots w_t, k_m) (w_1 \dots w_t, h_m)^{k_m} = \\ &= (w_1 \dots w_t, k_m) (w_1^{k_m} \dots w_t^{k_m}, h_m^{k_m}) = \\ &= (w_1 \dots w_t, k_m) (w'_1 \dots w'_t, h'_m). \end{aligned}$$

Аналогично, применяя соотношение (10.2.1.2), получаем

$$\begin{aligned} (w_1 \dots w_t, k_m) &= (w_1, k_m)^{w_2 \dots w_t} (w_2 \dots w_t, k_m) = \\ &= (w''_1, k''_m) (w_2 \dots w_t, k_m). \end{aligned}$$

Продолжая это разложение, мы получим представление коммутатора  $(u_1, \dots, u_{m-1}, u_m)$  в виде произведения элементов типов  $(w, h_m^{(i)})$  и  $(w, k_m^{(i)})$ , которые имеют вид  $(v_1, \dots, v_m)$ , где  $v_i$  — элемент или из  $H$ , или из  $K$ . Наше утверждение доказано полной индукцией. Мы показали, что подгруппа  $\Gamma_{c+d+1}(HK)$  порождается коммутаторами  $(v_1, \dots, v_{c+d+1})$ , где  $v_i$  — элемент из  $H$  или  $K$ . Но  $(v_1, \dots, v_{t-1}, v_t) = (v_1, \dots, v_{t-1})^{-1} v_t^{-1} (v_1, \dots, v_{t-1}) v_t$ . Если  $(v_1, \dots, v_{t-1}) \in \Gamma_i(H)$  и  $v_t \in K$ , то, в силу инвариантности подгруппы  $\Gamma_i(H)$  в группе  $HK$ ,  $(v_1, \dots, v_t) \in \Gamma_i(H)$ , а если  $v_t \in H$ , то  $(v_1, \dots, v_t) \in \Gamma_{t+1}(H)$ . Следовательно, если среди элементов  $v_1, \dots, v_{c+d+1}$  есть  $c+1$  элементов из  $H$ , то  $(v_1, \dots, v_{c+d+1}) \in \Gamma_{c+1}(H) = 1$ , т. е.  $(v_1, \dots, v_{c+d+1}) = 1$ ; если нет, то среди них есть не менее  $d+1$  элементов из  $K$ , а тогда  $(v_1, \dots, v_{c+d+1}) \in \Gamma_{d+1}(K) = 1$ . В обоих случаях  $(v_1, \dots, v_{c+d+1}) = 1$ , откуда группа  $H \cup K = HK$  обладает свойством ниль-( $c+d$ ).

**Теорема 10.3.3.** *Если группа  $G$  — ниль- $c$  группа,  $H = H_0$  — произвольная подгруппа и  $H_{i+1}$  — нормализатор подгруппы  $H_i$  в  $G$ , то  $H_c = G$ .*

**Доказательство.** Ясно, что  $H_0 \supseteq Z_0 = 1$ . Докажем по индукции, что  $H_m \supseteq Z_m$  для всех  $m$ . Предположим, что  $H_i \supseteq Z_i$ . Тогда, согласно определению  $Z_{i+1}$ , для любого элемента  $z_{i+1} \in Z_{i+1}$  и любого  $g \in G$  мы имеем  $z_{i+1}^{-1} g^{-1} z_{i+1} g = z_i \in Z_i$ , откуда при  $g^{-1} = h_i \in H_i$  получаем  $z_{i+1}^{-1} h_i z_{i+1} = z_i h_i \in H_i$ , и, следовательно,  $Z_{i+1}$  содержится в нормализаторе подгруппы  $H_i$ , откуда  $H_{i+1} \supseteq Z_{i+1}$ , что доказывает индуктивное утверждение.

Теперь из того, что  $Z_c = G$ , следует требуемое равенство  $H_c = G$ .

**Следствие 10.3.1.** *Любая собственная подгруппа нильпотентной группы является собственной подгруппой своего нормализатора.*

**Следствие 10.3.2.** Любая максимальная подгруппа нильпотентной группы инвариантна, имеет простой индекс и содержит производную группу.

Пусть  $M$  — максимальная подгруппа нильпотентной группы  $G$ . Так как нормализатор  $N_G(M)$  строго содержит  $M$ , имеем  $N_G(M) = G$  или  $M \triangleleft G$ . Далее, в силу максимальности  $M$  фактор-группа  $G/M$  не содержит собственных подгрупп, т. е. она циклическая группа простого порядка. Поэтому индекс подгруппы  $M$  прост, а производная группа  $G'$  содержится в  $M$ , так как фактор-группа  $G/M$  абелева.

**Следствие 10.3.3.** Если  $G$  — нильпотентная группа и  $H$  — такая подгруппа, что  $G = G'H$ , то  $H = G$ .

Допустим, что не выполняется утверждение следствия:  $H \neq G$ . Тогда в силу теоремы при  $H = H_0$  и  $H_{i+1} = H_i Z_{i+1}$  мы бы имели, что каждая подгруппа  $H_i$  инвариантна в  $H_{i+1}$ . Если  $H_j \neq G$ , но  $H_{j+1} = G$ , то  $H_j$  — собственная инвариантная подгруппа, причем фактор-группа  $G/H_j$  абелева, откуда  $H_j \trianglelefteq G'$ . Но тогда  $HG' \subseteq H_j G' = H_j \neq G$ , что противоречит условию. Итак,  $H = G$ , что и требовалось доказать. Заметим, что при доказательстве не понадобилось предположения о том, что  $G$  содержит максимальные подгруппы.

**Теорема 10.3.4.** Конечные  $p$ -группы нильпотентны. Конечная группа нильпотентна тогда и только тогда, когда она представима как прямое произведение своих силовских подгрупп.

**Доказательство.** По теореме 4.3.1 любая конечная  $p$ -группа  $P$  имеет нетривиальный центр. Следовательно, верхний центральный ряд группы  $P$  обрывается на всей группе  $P$ , т. е. эта группа нильпотентна. Отсюда следует нильпотентность прямого произведения конечных  $p$ -групп. Пусть теперь  $G$  — конечная нильпотентная группа,  $P$  — силовская  $p$ -подгруппа группы  $G$ . Тогда нормализатор  $N_G(P)$  совпадает со своим собственным нормализатором (теорема 4.2.4), а в силу следствия 10.3.1,  $N_G(P) = G$ , т. е.  $P \triangleleft G$ . Так как каждая силовская подгруппа группы  $G$  инвариантна в ней, то  $G$  представима как прямое произведение своих силовских подгрупп.

**Следствие 10.3.4.** (Виландт.) Конечная группа нильпотентна тогда и только тогда, когда все ее максимальные подгруппы инвариантны.

В самом деле, согласно следствию 10.3.2 из теоремы 10.3.3, максимальные подгруппы нильпотентной группы инвариантны. С другой стороны, в силу теоремы 4.2.4 нормализатор  $N_G(P)$  силовской подгруппы  $P$  не может содержаться в собственной инвариантной подгруппе группы  $G$ . Следовательно, если максимальные подгруппы инвариантны, то  $P \triangleleft G$  и  $G$  представима как прямое произведение своих силовских подгрупп.

**Теорема 10.3.5.** Если  $X, Y$  и  $Z$  — подгруппы группы  $G$  и  $K$  — инвариантная подгруппа, содержащая  $(X, Y, Z)$  и  $(Z, X, Y)$ , то  $K$  содержит также  $(Y, Z, X)$ .

**Доказательство.** Из соотношения (10.2.1.4) имеем

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

откуда и следует требуемое включение.

**Теорема 10.3.6.** Если  $H = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots$  — ряд таких инвариантных подгрупп группы  $G$ , что  $(H_{i-1}, L) \subseteq H_i$  для всех  $i$  и некоторой подгруппы  $L$ , то  $(H_i, \Gamma_j(L)) \subseteq H_{i+j}$ .

**Следствие 10.3.6.**  $(\Gamma_i(G), \Gamma_j(G)) \subseteq \Gamma_{i+j}(G)$ .

**Доказательство.** Проведем индукцию по  $j$ , начиная с  $j = 1$ . Пусть  $(H_i, \Gamma_{j-1}(L)) \subseteq H_{i+j-1}$  для любого  $i$ . Тогда по индукции  $(L, H_i, \Gamma_{j-1}(L)) \subseteq (H_{i+1}, \Gamma_{j-1}(L)) \subseteq H_{i+j}$  и  $(H_i, \Gamma_{j-1}(L), L) \subseteq \subseteq (H_{i+j-1}, L) \subseteq H_{i+j}$ . Так как  $(\Gamma_{j-1}(L), L) = \Gamma_j(L)$ , то, применяя теорему 10.3.5, мы получаем

$$(H_i, \Gamma_j(L)) = (H_i, (\Gamma_{j-1}(L), L)) = (\Gamma_{j-1}(L), L, H_i) \subseteq H_{i+j},$$

что и требовалось доказать.

## 10.4. Подгруппа Фраттини

Пусть  $G$  — произвольная группа. Подгруппа  $\Phi$  группы  $G$ , называемая подгруппой Фраттини, определяется следующим образом:  $\Phi = G \bigcap_M M$ , где  $M$  пробегает множество всех максимальных под-

групп группы  $G$ , если группа  $G$  обладает таковыми. Следовательно,  $\Phi = G$  тогда и только тогда, когда  $G$  не содержит максимальных подгрупп. Так как любой автоморфизм группы  $G$  переставляет максимальные подгруппы между собой, то ясно, что подгруппа Фраттини является характеристической подгруппой.

Интересна связь подгруппы Фраттини группы  $G$  с множеством образующих элементов группы  $G$ . Подгруппа  $\Phi$  состоит из элементов группы  $G$ , которые являются „необразующими элементами“ для  $G$  в следующем смысле.

**Определение.** Говорят, что элемент  $x$  группы  $G$  является необразующим для  $G$ , если из равенства  $G = \{T, x\}$ , где  $T$  — произвольное множество в  $G$ , следует равенство  $G = \{T\}$ .

Отметим, что здесь требуется выполнение равенства  $\{T, x\} = \{T\}$  для любого подмножества  $T$ , для которого  $\{T, x\} = G$ . Например, если  $G \neq 1$ , то ясно, что  $1$  — необразующий элемент.

**Теорема 10.4.1.** Если группа  $G$  отлична от единичной, то ее подгруппа Фраттини состоит из всех необразующих элементов группы  $G$ .

*Доказательство.* Пусть  $x \in G$ . Если существует максимальная подгруппа  $M$ , которая не содержит  $x$ , то группа  $\{M, x\}$  строго содержит  $M$ , откуда в силу максимальности подгруппы  $M$  имеем  $\{M, x\} = G$ , но  $\{M\} = M \neq G$ . Таким образом, необразующие элементы группы  $G$  содержатся во всех максимальных подгруппах, а потому и в группе  $\Phi = G \bigcap_M M$ . Нам остается показать обратное: если  $u \in \Phi$ , то элемент  $u$  является необразующим для  $G$ . По условию,  $G \neq 1$ , значит, 1 — необразующий элемент.

Предположим, что  $G = \{T, u\}$ , где  $T$  — некоторое подмножество в  $G$ . Покажем, что предположение  $\{T\} = H \neq G$  приводит к противоречию. Элемент  $u$  не содержится в  $H$ , так как в противном случае  $H = \{H, u\} \supseteq \{T, u\} = G$ . Итак,  $u \notin H$ . Тогда, по лемме Цорна, существует подгруппа  $K \supseteq H$ , максимальная по отношению к свойству  $u \notin K$ . Следовательно,  $\{K, u\} \supseteq \{T, u\} = G$ , откуда  $\{K, u\} = G$ . Но в силу нашего выбора подгруппы  $K$  любая подгруппа, строго содержащая  $K$ , должна содержать элемент  $u$ . Следовательно,  $K = M$  — максимальная подгруппа, не содержащая  $u$ , что противоречит условию  $u \in \Phi = G \bigcap_M M$ . Итак,  $\{T\} = G$ .

Любой элемент  $u \in \Phi$  является необразующим для  $G$ .

**Теорема 10.4.2.** *Подгруппа Фраттини конечной группы нильпотентна.*

*Доказательство.* Пусть  $G$  — конечная группа и  $\Phi$  — ее подгруппа Фраттини. Пусть  $P$  — сильовская  $p$ -подгруппа группы  $\Phi$ ; последняя как характеристическая подгруппа группы  $G$  инвариантна в ней. Поэтому все подгруппы, сопряженные с  $P$  в  $G$ , содержатся в  $\Phi$ ; так как они являются сильовскими  $p$ -подгруппами группы  $\Phi$ , то они сопряжены в  $\Phi$ . Таким образом, подгруппа  $P$  имеет столько же сопряженных подгрупп в  $\Phi$ , сколько и во всей группе  $G$ , и поэтому  $[G : N_G(P)] = [\Phi : N_\Phi(P)]$ . Но  $[G : N_\Phi(P)] = [G : \Phi][\Phi : N_\Phi(P)] = [G : N_G(P)][N_G(P) : N_\Phi(P)]$ , откуда  $[G : \Phi] = [N_G(P) : N_\Phi(P)]$ . Заметив, что  $N_\Phi(P) = N_G(P) \cap \Phi$ , и применяя теорему 1.5.5 о неравенствах для индексов, получаем  $[N_G(P) \cup \Phi : \Phi] \geq [N_G(P) : N_G(P) \cap \Phi] = [G : \Phi]$ . Отсюда  $N_G(P) \cup \Phi = G$ . Подгруппа  $\Phi$  состоит из конечного числа необразующих элементов; следовательно,  $G = \{N_G(P), \Phi\} = \{N_G(P)\} = N_G(P)$ . Поэтому  $P \triangleleft G$  и тем более  $P \triangleleft \Phi$ . Таким образом, любая сильовская  $p$ -подгруппа инвариантна в  $\Phi$ . Поэтому  $\Phi$  — прямое произведение своих сильовских подгрупп и тем самым  $\Phi$  — нильпотентная группа.

**Теорема 10.4.3.** *Подгруппа Фраттини нильпотентной группы содержит производную группу.*

*Доказательство.* Согласно следствию 10.3.3, если группа  $G$  нильпотентна и  $G = HG'$ , то  $G = H$ . Это означает, что элементы

подгруппы  $G'$  могут быть вычеркнуты из любого множества образующих группы  $G$ , следовательно,  $\Phi \trianglelefteq G'$ .

Для конечных групп имеет место обратное утверждение.

**Теорема 10.4.4.** (Виландт.) *Если подгруппа Фраттини конечной группы  $G$  содержит производную подгруппу  $G'$ , то группа  $G$  нильпотентна.*

*Доказательство.* Пусть  $P$  — силовская подгруппа группы  $G$ . Если  $N_G(P) = H \neq G$ , то подгруппа  $H$  содержится в некоторой максимальной подгруппе  $M$  группы  $G$ . Тогда  $M \trianglelefteq \Phi$  и по условию  $\Phi \trianglelefteq G'$ . Так как фактор-группа  $G/G'$  абелева,  $M$  — нормальный делитель в  $G$ . С другой стороны, в силу теоремы 4.2.4, так как  $M \trianglelefteq N_G(P)$ , подгруппа  $M$  совпадает со своим нормализатором. Мы пришли к противоречию. Следовательно,  $N_G(P) = G$ . Так как все силовские  $p$ -подгруппы группы  $G$  инвариантны,  $G$  является их прямым произведением и, следовательно, нильпотентной группой.

## 10.5. Сверхразрешимые группы

**Теорема 10.5.1.** *Подгруппа и фактор-группа сверхразрешимой группы сверхразрешимы.*

*Доказательство.* Пусть  $G$  — сверхразрешимая группа и  $G = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_r = 1$  — инвариантный ряд с циклическими факторами  $A_{i-1}/A_i$ . Тогда гомоморфные образы  $B_i$  подгрупп  $A_i$  в фактор-группе  $G/K = T$  образуют инвариантный ряд  $T = B_0 \supseteq B_1 \supseteq B_2 \supseteq \dots \supseteq B_r = 1$ . Отсюда, исключив все повторения, получаем инвариантный ряд с циклическими факторами, так как гомоморфный образ циклической группы является или циклической или единичной группой. Для подгруппы  $H$  составим ряд

$$H = C_0 \supseteq C_1 \supseteq C_2 \supseteq \dots \supseteq C_r = 1,$$

где  $C_i = H \cap A_i$ . Для любого  $i$  подгруппа  $H \cap A_i$  инвариантна в  $H$ , а в силу теоремы 2.4.1,  $C_i/C_{i+1} = H \cap A_i/H \cap A_{i+1} \cong \cong A_{i+1} \cup (H \cap A_i)/A_{i+1}$ . Но последняя фактор-группа содержится в циклической группе  $A_i/A_{i+1}$ , откуда следует, что она или циклическая, или единичная. Таким образом, фактор-группа  $C_i/C_{i+1}$  или циклическая, или единичная, следовательно, подгруппа  $H$  сверхразрешима.

**Следствие 10.5.1.** *Сверхразрешимые группы удовлетворяют условию максимальности.*

Сверхразрешимая группа имеет конечную систему образующих. То же самое справедливо для любой ее подгруппы (теорема 10.5.1). Отсюда вытекает выполнение условия максимальности.

**Теорема 10.5.2.** *Сверхразрешимая группа  $G$  обладает инвариантным рядом  $G = B_0 \supset B_1 \supset B_2 \supset \dots \supset B_k = 1$ , все фактор-группы  $B_{i-1}/B_i$  которого являются или бесконечными циклическими группами, или циклическими группами простых порядков.*

**Доказательство.** Пусть  $G = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_r = 1$  — инвариантный ряд группы  $G$  с циклическими фактор-группами. Если порядок фактор-группы  $A_{j-1}/A_j$  конечен и равен  $p_1 p_2 \dots p_s$ , где  $p_1, p_2, \dots, p_s$  — простые (но не обязательно различные) числа, то группа  $A_{j-1}/A_j$  содержит по одной циклической подгруппе порядков  $p_1, p_1 p_2, \dots, p_1 \dots p_{s-1}$ , и все эти подгруппы являются характеристическими. Следовательно,  $s - 1$  соответствующих подгрупп между  $A_{j-1}$  и  $A_j$  инвариантны в группе  $G$ , а соответствующие фактор-группы циклически и имеют простые порядки. Проделав подобные уплотнения исходного ряда во всех тех случаях, когда порядки фактор-групп  $A_{j-1}/A_j$  конечны, мы получим инвариантный ряд, в котором каждая фактор-группа — циклическая группа бесконечного или простого порядка.

Эту теорему можно усилить, так как можно упорядочить простые факторы по величинам соответствующих простых чисел.

**Теорема 10.5.3.** *Сверхразрешимая группа  $G$  обладает инвариантным рядом  $G = C_0 \supset C_1 \supset C_2 \supset \dots \supset C_k = 1$ , у которого циклические факторы имеют или бесконечный, или простой конечный порядок, а если факторы  $C_{i-1}/C_i$  и  $C_i/C_{i+1}$  имеют соответственно простые порядки  $p_i$  и  $p_{i+1}$ , то  $p_i \leqslant p_{i+1}$ .*

**Доказательство.** Рассмотрим ряд  $G = B_0 \supset B_1 \supset B_2 \supset \dots \supset B_k = 1$  (см. теорему 10.5.2). Если порядки факторов  $B_{i-1}/B_i$  и  $B_i/B_{i+1}$  — простые числа  $q$  и  $p$  соответственно, причем  $q > p$ , то порядок фактор-группы  $B_{i-1}/B_{i+1}$  равен  $pq$ , где  $p < q$ . Эта фактор-группа содержит характеристическую подгруппу порядка  $q$ , полный прообраз которой  $B_i^*$  инвариантен в группе  $G$ . Если в последнем ряду заменить  $B_i$  на  $B_i^*$ , то порядки факторов  $B_{i-1}/B_i^*$  и  $B_i^*/B_{i+1}$  будут равны соответственно  $p$  и  $q$ . Продолжая этот процесс, не изменяющий длину инвариантного ряда, мы в итоге получим ряд, простые порядки факторов которого упорядочены по величине, что и требовалось доказать.

**Следствие 10.5.2.** *Если  $G$  — конечная сверхразрешимая группа порядка  $p_1 p_2 \dots p_r$ , где  $p_1 \leqslant p_2 \leqslant \dots \leqslant p_r$  — простые числа, то она обладает главным рядом  $G = A_0 \supset A_1 \supset \dots \supset A_r = 1$ , в котором порядок фактора  $A_{i-1}/A_i$  равен  $p_i$ .*

**Теорема 10.5.4.** *Производная группа сверхразрешимой группы нильпотента.*

**Доказательство.** Пусть  $G = A_0 \supset A_1 \supset \dots \supset A_r = 1$  — инвариантный ряд с циклическими фактор-группами  $A_{i-1}/A_i$ .

Положим  $H_i = G' \cap A_i$ . Тогда  $G' = H_0 \supseteq H_1 \supseteq \dots \supseteq H_r = 1$  — инвариантный ряд, различные члены  $K_i$  которого составляют ряд  $G' = K_0 \supset K_1 \dots \supset K_s = 1$  с циклическими факторами. Докажем, что этот ряд — центральный для группы  $G'$ . Любая подгруппа  $K_i$  будет пересечением инвариантных подгрупп группы  $G$ , следовательно,  $K_i \triangleleft G$ . Поэтому циклическая подгруппа  $K_{i-1}/K_i$  содержится в группе  $G/K_i$  в качестве инвариантной подгруппы, а трансформирование элементом из  $G$  индуцирует автоморфизм циклической группы  $K_{i-1}/K_i$ . Автоморфизмы циклической группы образуют абелеву группу, а поэтому два элемента из группы  $G/K_i$  индуцируют перестановочные автоморфизмы группы  $K_{i-1}/K_i$ . Но тогда коммутатор любых двух элементов  $x^{-1}y^{-1}xy$  индуцирует тождественный автоморфизм группы  $K_{i-1}/K_i$ . Но это означает, что подгруппа  $K_{i-1}/K_i$  лежит в центре группы  $G'/K_i$ . Этим доказано, что ряд из подгрупп  $K_i$  является центральным для  $G'$  и что  $G'$  — нильпотентная группа.

Существует очень интересное свойство рядов произвольных подгрупп сверхразрешимой группы. Будем говорить, что подгруппа  $H_2$  имеет индекс  $\infty^1$  в подгруппе  $H_1$ , если  $H_1 = \sum_x H_2 a^x$ , где  $a$  — некоторый элемент, а  $x$  пробегает все целые числа от  $-\infty$  до  $+\infty$ . Так, если  $A_j \triangleleft A_{j-1}$  и  $A_{j-1}/A_j$  — бесконечная циклическая группа, то индекс подгруппы  $A_j$  в группе  $A_{j-1}$  равен  $\infty^1$ , так как в качестве элемента  $a$  мы можем взять любой элемент из смежного класса по подгруппе  $A_j$ , являющегося образующим элементом циклической группы  $A_{j-1}/A_j$ . Но подгруппа  $H_2$  может иметь индекс  $\infty^1$  в  $H_1$  и в том случае, когда  $H_2$  — неинвариантная подгруппа в  $H_1$ .

**Теорема 10.5.5.** В сверхразрешимой группе  $G$  любая цепь подгрупп  $G = M_0 \supset M_1 \supset M_2 \supset \dots \supset M_s = 1$  может быть уплотнена подгруппами  $M_{i-1} = M_{i,0} \supset M_{i,1} \supset \dots \supset M_{i,t} = M_i$ ,  $t = t(i)$ ,  $i = 1, \dots, s$ , так что индекс подгруппы  $M_{i,j}$  в подгруппе  $M_{i,j-1}$  равен или простому числу, или  $\infty^1$ .

**Доказательство.** Так как подгруппа  $M_1$  сверхразрешима, достаточно показать, что можно произвести такое уплотнение промежутка между  $G = M_0$  и  $M_1$ . Проделав такие же построения последовательно для  $M_1, \dots, M_{s-1}$ , мы получим требуемое уплотнение всего ряда.

Пусть  $G = A_0 \supset A_1 \supset A_2 \supset \dots \supset A_r = 1$  — инвариантный ряд группы  $G$  с циклическими фактор-группами простых или бесконечных порядков. Ясно, что  $M_1 \supseteq A_r = 1$ , но  $M_1 \not\supseteq A_0 = G$ . Следовательно, для некоторого числа  $i$  из последовательности  $1, \dots, r$  имеем  $M_1 \supseteq A_i$ , но  $M_1 \not\supseteq A_{i-1}$ . Рассмотрим два случая: 1) порядок фактор-группы  $A_{i-1}/A_i$  прост, 2)  $A_{i-1}/A_i$  — бесконечная циклическая группа.

**Случай 1.** Порядок фактор-группы  $A_{i-1}/A_i$  прост. В этом случае  $A_{i-1} \supset M_1 \cap A_{i-1} \supseteq A_i$ . Так как индекс подгруппы  $A_i$  в  $A_{i-1}$  прост, между  $A_i$  и  $A_{i-1}$  не существует подгрупп. Следовательно,  $M_1 \cap A_{i-1} = A_i$ . Если  $A_{i-1} = \sum_x A_i a^x$ ,  $x = 0, \dots, p-1$ , то  $M_1 \cup A_{i-1} = M_1 A_{i-1} = M_1^*$  и  $M_1^* = \sum_x M_1 a^x$ ,  $x = 0, 1, \dots, p-1$ , так как  $M_1$  содержит подгруппу  $A_i$  и  $a^p \in A_i$ , но  $a \notin A_i$ . Здесь индекс подгруппы  $M_1$  в группе  $M_1^*$  равен простому числу и  $M_1^* \supseteq A_{i-1}$ .

**Случай 2.**  $A_{i-1}/A_i$  — бесконечная циклическая группа. И здесь  $A_{i-1} \supset M_1 \cap A_{i-1} \supseteq A_i$ . Так как любая подгруппа группы  $A_{i-1}/A_i$  характеристична, подгруппа  $M_1 \cap A_{i-1}$  инвариантна в  $G$ . Если  $M_1 \cap A_{i-1} = A_i$  и  $A_{i-1} = \sum_x A_i a^x$ , то положим  $M_1^* = M_1 \cup A_{i-1} = = M_1 A_{i-1} = \sum_x M_1 a^x$ , откуда индекс  $M_1$  в  $M_1^*$  равен  $\infty^1$ , так как  $M_1$  содержит подгруппу  $A_i$ , но не содержит степеней элемента  $a$ . Если же  $M_1 \cap A_{i-1} \supset A_i$ , то, так как любая подгруппа бесконечной циклической группы имеет конечный индекс, индекс подгруппы  $M_1 \cap A_{i-1}$  в группе  $A_{i-1}$  также конечен. Таким образом, в наш инвариантный ряд мы можем вставить подгруппы между  $A_{i-1}$  и  $M_1 \cap A_{i-1}$  так, что индекс каждой подгруппы в ближайшей содержащей ее подгруппе простой, и, как в случае 1, находим подгруппу  $M_1^*$ , в которой индекс подгруппы  $M_1$  прост. Повторяя эту конструкцию, мы находим ряд  $M_1 \subset M_1^* \subset \subset M_1^{**} \subset \dots \subset M_1^{(u)}$ , в котором индекс каждой подгруппы в последующей прост и  $M_1^{(u)} \supseteq A_{i-1}$ .

Продолжив это построение, мы через конечное число шагов достигнем группы  $M_1^{(v)} \supseteq A_0 = G$ , т. е. осуществим требуемое уплотнение интервала между  $G$  и  $M_1$ . Как уже отмечалось, такими же построениями достигается уплотнение всего ряда.

Интересную форму принимает эта теорема для конечных групп.

**Теорема 10.5.6.** В конечной сверхразрешимой группе  $G$  все максимальные цепочки подгрупп имеют одну и ту же длину, равную  $r$ , где  $r$  — число простых делителей (не обязательно различных) порядка группы  $G$ .

**Доказательство.** Согласно предыдущей теореме, в максимальной цепочке индекс любой подгруппы в содержащей ее подгруппе — простое число, а потому длина максимальной цепочки равна  $r$ .

**Следствие 10.5.1.** Любая максимальная подгруппа конечной сверхразрешимой группы имеет простой индекс.

Замечательный факт, впервые доказанный Хуппертом [1], состоит в том, что обратное утверждение также верно. Для его доказательства нам понадобятся некоторые из теорем теории представлений групп, которые будут доказаны в главе 16. Сейчас мы докажем одну неопубликованную теорему Филипа Холла.

**Теорема 10.5.7.** (Ф. Холл.) *Пусть  $G$  — конечная группа со свойством (M): все максимальные подгруппы группы  $G$  имеют индекс  $p$  или  $p^2$ , где  $p$  — простое число. Тогда группа  $G$  разрешима.*

*Доказательство* будем проводить индукцией по порядку группы  $G$ . Пусть  $p$  — наибольшее простое число, которое делит этот порядок,  $S$  — силовская  $p$ -подгруппа группы  $G$ ,  $N$  — ее нормализатор в  $G$ . Если  $N = G$ , то  $S \triangleleft G$  и фактор-группа обладает свойством (M), откуда по предположению индукции группа  $G/S$  разрешима. При этом  $S$  —  $p$ -группа, следовательно, группа  $G$  разрешима. Если же  $N \subset G$ , то выбираем максимальную подгруппу  $H$  группы  $G$ , содержащую  $N$ .  $N$  — нормализатор группы  $S$  как в группе  $G$ , так и в подгруппе  $H$ . Поэтому, применяя третью теорему Силова, получаем  $[G:N] = 1 + k_1 p$ ,  $[H:N] = 1 + k_2 p$ . Это числа силовских  $p$ -подгрупп в группах  $G$  и  $H$  соответственно. Отсюда  $[G:H] = 1 + kp$ . Но по условию  $[G:H] = q$  или  $q^2$ , где  $q$  — некоторое простое число, причем ясно, что  $q < p$ ,  $k > 0$ . Итак,  $kp = q^2 - 1 = (q+1)(q-1)$ , но  $p \geq q+1$ , откуда  $p = q+1$ . Последнее возможно только при  $p=3$ ,  $q=2$ . Тогда порядок группы  $G$  равен  $2^a 3^b$ . Отсюда и из теоремы 16.8.7 следует, что группа  $G$  разрешима.

**Теорема 10.5.8.** (Хупперт) *Пусть  $G$  — конечная группа со свойством ( $M^1$ ): все ее максимальные подгруппы имеют простые индексы. Тогда группа  $G$  сверхразрешима.*

*Доказательство.* Предположим, что теорема не верна. Рассмотрим группу  $G$  наименьшего порядка, обладающую свойством ( $M^1$ ) и не сверхразрешимую. Тогда в силу теоремы 10.5.7 группа  $G$  разрешима. Пусть  $N$  — минимальная инвариантная подгруппа группы  $G$  порядка  $p^a$ , где  $p$  — простое число. Согласно свойству минимальности группы  $G$ , фактор-группа  $G/N$  сверхразрешима, так что среди главных факторов группы  $G$  только группа  $N$  не является циклической. Отсюда заключаем, что  $N$  — единственная минимальная инвариантная подгруппа. Пусть  $H/N$  — минимальная инвариантная подгруппа группы  $G/N$ . Рассмотрим два случая: 1)  $[H:N] = p$ , 2)  $[H:N] = q$ , где  $p$  и  $q$  — простые числа,  $p \neq q$ . В первом случае группа  $H$  абелева, так как в противном случае мы бы имели  $1 \subset H' \subset N$ , где  $H'$  — нормальный делитель в  $G$ . Так как  $\alpha > 1$ , подгруппа  $H$  не может содержать элементов порядка  $p^2$ ; в противном случае подгруппа  $N$  содержала бы характеристическую подгруппу группы  $H$  порядка  $p$ . Как и выше, заклю-

чаем, что тогда  $N$  — не минимальный нормальный делитель. Итак,  $H$  — элементарная абелева группа.

Теперь группа  $G$  естественным образом может быть представлена как группа автоморфизмов группы  $H$ , т. е. как группа линейных преобразований по модулю  $p$  степени  $\alpha+1$  (так как порядок  $H$  равен  $p^{\alpha+1}$ ). Пусть  $K$  — множество всех таких элементов  $a \in G$ , что для всех  $x \in H$  имеет место  $a^{-1}xa = x^m$ , где  $m = m(a)$  не зависит от  $x$ ; пусть  $L$  — централизатор подгруппы  $H$  в группе  $G$ . Тогда  $K/L$  содержится в центре группы  $G/L$ . Кроме того,  $K$  строго содержится в  $G$ , так как  $N$  — единственная минимальная инвариантная подгруппа группы  $G$ , между тем как все подгруппы группы  $H$  инвариантны в  $K$ . Пусть  $M/K$  — минимальная инвариантная подгруппа в  $G/K$ . Если  $[M : K] = p$ , то группа  $M/L$  — прямое произведение подгруппы  $K/L$ , порядок которой взаимно прост с  $p$  и которая содержится в центре группы  $G/L$ , и подгруппа  $\{L, a\}/L$  порядка  $p$ , причем подгруппа  $M_1 = \{L, a\}$  инвариантна в  $G$ . Так как взаимный коммутант  $(N, L) = 1$  и  $[M_1 : L] = p$ , то  $N$  содержит отличный от единицы элемент из центра группы  $M_1$ . Но центр группы  $M_1$  — нормальный делитель в  $G$ . Поэтому в силу минимальности подгруппы  $N$  она содержится в центре группы  $M_1$  и  $(M_1, N) = 1$ . Если  $H = \{N, b\}$ , то группа  $(H, M_1)$  имеет порядок, равный  $p$ , и порождается элементом  $(a, b) = c \in N, c \neq 1$ . Эта группа инвариантна в  $G$ , но это противоречит предположению, что подгруппа  $N$  — минимальная инвариантная подгруппа.

Поэтому  $[M : K] = q$  ( $q$  — простое число, отличное от  $p$ ), и тем самым порядок фактор-группы  $M/L$  взаимно прост с  $p$ . По теореме о полной приводимости (теорема 16.3.1) отсюда следует, что  $H = N \times P$ , где  $P$  — инвариантная подгруппа порядка  $p$  в  $M$ . Подгруппы, сопряженные с  $P$  в  $G$ , — нормальные делители порядка  $p$  в  $M$ , а их объединение  $Q$  — инвариантная подгруппа в  $G$ . Так как  $N$  — единственная минимальная инвариантная подгруппа группы  $G$  и  $Q \neq N$ , отсюда следует, что  $Q = H$ . Так как подгруппа  $P$  не содержится в  $N$ , ни одна сопряженная с  $P$  подгруппа не содержится в  $N$ . Пусть  $P = \{b\}$ , где  $b^p = 1$ . Если  $P_i$  — произвольная подгруппа, сопряженная с  $P$  и отличная от нее, то  $PP_i \cap N = R$ , где подгруппа  $R$  имеет порядок  $p$ , так как  $[H : N] = p$ . Порождающий элемент  $c$  подгруппы  $P_i$  можно выбрать так, чтобы  $P_i = \{c\}, R = \{bc\}$ . Так как  $P, P_i$  и  $R$  — инвариантные подгруппы в  $M$ , отсюда следует, что для любого элемента  $a \in M$  имеем  $a^{-1}ba = b^m, a^{-1}ca = c^n, a^{-1}(bc)a = (bc)^t$ . Но тогда  $(bc)^t = b^mc^n$  и  $t = m = n$ . Но  $P_i$  — произвольная сопряженная с  $P$  подгруппа, следовательно, для любого  $x \in H$  имеем  $a^{-1}xa = x^m$ , где  $m = m(a)$  не зависит от  $x$ . Поэтому  $M \subseteq K$ , т. е. мы пришли к противоречию. Таким образом, случай (1) невозможен.

Случай (2) можно отбросить сразу. Если число  $[H : N] = q$  отлично от  $p$ , то пусть  $Q$  — силовская  $q$ -подгруппа группы  $H$ , а  $T$  — нормализатор группы  $Q$  в  $G$ . Любая подгруппа, сопряженная с  $Q$  в группе  $G$ , содержится в  $H$  и, следовательно, сопряжена с  $Q$  в  $N$ . Поэтому  $G = NT$ . Тогда  $N \cap T$  инвариантна в  $G$ . Но  $T \not\subseteq N$ , так как в противном случае мы бы имели  $T = G$ , т. е.  $Q \trianglelefteq G$ . Следовательно,  $N \cap T = 1$ ,  $[G : T] = p^a$ . Но  $T$  — максимальная подгруппа группы  $G$ , так как в случае  $T \subset T_1 \subset G$  мы бы имели  $1 \subset T_1 \cap N \subset N$ , где подгруппа  $T_1 \cap N$  инвариантна в  $G$ . Таким образом, группа  $G$  содержит максимальную подгруппу не-простого индекса, что противоречит условию.

## Упражнения

- Пусть  $I^{(1)} = I^{(1)}(G)$  — группа внутренних автоморфизмов группы  $G$ , а  $I^{(n)}$  — группа внутренних автоморфизмов группы  $I^{(n-1)}$ . Показать, что если для некоторого  $n$  группа  $I^{(n)}$  равна единичной группе, то группа  $G$  nilпотентна.
- Пусть  $G$  — группа, удовлетворяющая условию максимальности. Показать, что группа  $G$  сверхразрешима, если группа  $A(G)$  автоморфизмов группы  $G$  сверхразрешима.
- Пусть  $a$  и  $b$  — элементы nilпотентной группы  $G$ , причем  $a^m = b^n = 1$  и  $(m, n) = 1$ . Пусть  $w = a^{-1}b^{-1}ab$ . Показать, что если  $w \in \Gamma_i(G)$ , то  $w^m \in \Gamma_{i+1}(G)$ ,  $w^n \in \Gamma_{i+1}(G)$ , откуда  $w \in \Gamma_{i+1}(G)$ . Следовательно,  $w = 1$  и  $ab = ba$ .
- Доказать утверждение, обратное утверждению упр. 2 гл. 8, т. е. если  $G$  — конечная nilпотентная группа и если  $p_1, p_2, \dots, p_s$  — произвольно упорядоченная последовательность простых чисел, произведение которых равно порядку группы  $G$ , то группа  $G$  обладает композиционным рядом  $G = A_0 \supset A_1 \supset \dots \supset A_s = 1$  с факторами  $A_{i-1}/A_i$  порядков  $p_i$ .
- Пусть  $G$  —  $p$ -группа, для которой  $\Gamma_3(G) = 1$ . Показать, что если  $p^m$  есть наивысший порядок элемента группы  $G/\Gamma_2(G)$ , то ни один элемент из группы  $\Gamma_2(G)$  не имеет порядка большего, чем  $p^m$ .

## Г л а в а 11

### БАЗИСНЫЕ КОММУТАТОРЫ

#### 11.1. Собирательный<sup>1)</sup> процесс

Рассмотрим формальные слова, или цепочки,  $b_1 b_2 \dots b_n$ , где каждый символ  $b$  представляет одну из букв  $x_1, x_2, \dots, x_r$ . Определим также формальные коммутаторы  $c_j$  и их веса  $\omega(c_j)$  следующим образом:

- 1)  $c_i = x_i$ ,  $i = 1, \dots, r$  — коммутаторы веса 1, т. е.  $\omega(x_i) = 1$ ,
- 2) если  $c_i$  и  $c_j$  — коммутаторы, то и  $c_k = (c_i, c_j)$  — коммутатор и  $\omega(c_k) = \omega(c_i) + \omega(c_j)$ .

Отметим, что, согласно этому определению, существует только конечное число формальных коммутаторов заданного веса. Упорядочим коммутаторы, располагая сначала  $c_i = x_i$ ,  $i = 1, \dots, r$ , а затем все остальные коммутаторы в порядке возрастания их весов, причем порядок среди коммутаторов одного и того же веса произволен.

Будем говорить, что слово  $c_{i_1} \dots c_{i_m}$ , составленное из коммутаторов, собрано, если  $i_1 \leq i_2 \leq \dots \leq i_m$ , т. е. если коммутаторы расположены в порядке возрастания индексов слева направо<sup>2)</sup>. Произвольное слово из коммутаторов

$$c_{i_1} \dots c_{i_m} c_{i_{m+1}} \dots c_{i_n} \quad (11.1.1)$$

содержит, вообще говоря, собранную часть  $c_{i_1} \dots c_{i_m}$ , где  $i_1 \leq \dots \leq i_m$  и  $i_m \leq i_j$ ,  $j = m+1, \dots, n$ , и несобранную часть  $c_{i_{m+1}} \dots c_{i_n}$ , где  $i_{m+1}$  уже не наименьший из индексов  $i_j$ ,  $j = m+1, \dots, n$ . Собранная часть слова  $c_{i_1} \dots c_{i_m}$  пуста, если только  $i_1$  — не наименьший из индексов.

Определим *собирательный процесс* для слов из коммутаторов. Пусть  $c_u$  — коммутатор с наименьшим индексом в несобранной части слова, и пусть  $c_{i_j} = c_u$  — первое вхождение  $c_u$

<sup>1)</sup> В оригинале „collecting“. Термин должен указывать на тот факт, что слова данного вида возникают в результате действия некоторого алгоритма, названного „собирательным процессом“. — Прим. ред.

<sup>2)</sup> Предполагается, конечно, что индексы коммутаторов являются порядковыми номерами коммутаторов в вышеопределенном упорядочении. — Прим. ред.

в несобранную часть. Заменим тогда слово

$$c_{i_1} \dots c_{i_m} \dots c_{i_{j-1}} c_{i_j} \dots c_{i_n}$$

словом

$$c_{i_1} \dots c_{i_m} \dots c_{i_j} c_{i_{j-1}} (c_{i_{j-1}}, c_{i_j}) \dots c_{i_n}.$$

При этом коммутатор  $c_{i_j}$  сдвинется на одно место влево и появится новый коммутатор  $(c_{i_{j-1}}, c_{i_j})$ , который по весу больше, чем  $c_{i_j}$ .

Таким образом, и после указанного преобразования  $c_{i_j}$  останется коммутатором с наименьшим индексом в несобранной части. После конечного числа таких шагов коммутатор  $c_{i_j}$  займет  $(m+1)$ -е место и станет элементом собранной части. Так определенный собирательный процесс, вообще говоря, не будет обрываться, так как на каждом шаге вводится новый коммутатор.

Пусть  $x_1, \dots, x_r$  — образующие элементы группы  $F$  (мы будем в основном рассматривать случай, когда группа  $F$  — свободная группа с образующими  $x_1, x_2, \dots, x_r$ ), и пусть  $(u, v) = u^{-1}v^{-1}uv$ , тогда

$$c_{i_{j-1}} c_{i_j} = c_{i_j} c_{i_{j-1}} (c_{i_{j-1}}, c_{i_j}), \quad (11.1.2)$$

и мы видим, что собирательный процесс не изменяет элемент группы, представленный словом. При нашем определении собирательный процесс применим не ко всем словам, а только к так называемым *положительным* словам, т. е. к словам, составленным из букв  $x_i$  и не содержащим букв вида  $x_i^{-1}$ . Ниже мы освободимся от этого ограничения.

В ходе собирательного процесса, примененного к положительным словам, возникают не любые коммутаторы. Так, например, коммутатор  $(x_2, x_1)$  может возникнуть, а коммутатор  $(x_1, x_2)$  возникнуть не может, так как буква  $x_1$  собирается до  $x_2$ . Коммутаторы, которые действительно могут возникнуть в собирательном процессе, называются *базисными*. Дадим формальное определение базисных коммутаторов группы  $F$  с образующими  $x_1, x_2, \dots, x_r$ .

#### ОПРЕДЕЛЕНИЕ БАЗИСНЫХ КОММУТАТОРОВ

1)  $c_i = x_i$ ,  $i = 1, \dots, r$  — базисные коммутаторы веса один,  $\omega(c_i) = 1$ .

2) Пусть базисные коммутаторы весов, меньших  $n$ , уже определены. Тогда базисными коммутаторами веса  $n$  являются коммутаторы  $c_k = (c_i, c_j)$ , где

a)  $c_i$  и  $c_j$  — базисные коммутаторы и  $\omega(c_i) + \omega(c_j) = n$ ;

b)  $c_i > c_j$ , а если  $c_i = (c_s, c_t)$ , то  $c_j \geqslant c_t$ .

3) Коммутаторы веса  $n$  следуют за коммутаторами весов, меньших  $n$ , и между собой они упорядочены произвольным образом. Базисные коммутаторы считаем пронумерованными так, что они упорядочены по индексам.

Заметим, что если коммутаторы упорядочены по весам, а в остальном — произвольным образом, то собирательный процесс, примененный к положительным словам, дает только базисные коммутаторы. Например, при замене

$$c_u c_v = c_v c_u (c_u, c_v) \quad (11.1.3)$$

мы собираем  $c_v$  до  $c_u$ , откуда  $c_u > c_v$ , а если  $c_u = (c_s, c_t)$ , то это означает, что буква  $c_t$  собиралась до  $c_v$ , откуда  $c_v \geq c_t$ .

Мы покажем сейчас, что по модулю  $\Gamma_{k+1}(F)$ , где  $\Gamma_{k+1}(F)$  —  $(k+1)$ -й член нижнего центрального ряда группы  $F$ , обозначаемый также  $F_{k+1}$  ( $k$  — любое число), произвольный элемент может быть представлен в виде

$$f = c_1^{e_1} c_2^{e_2} \dots c_t^{e_t} \bmod F_{k+1}, \quad (11.1.4)$$

где  $c_1, \dots, c_t$  — базисные коммутаторы весов  $1, 2, \dots, k$ .

В ходе собирательного процесса имеем

$$vu = uv(v, u), \quad (11.1.5)$$

где  $u, v$  и  $(v, u)$  — базисные коммутаторы. Мы должны также рассмотреть выражения  $vu^{-1}$ ,  $v^{-1}u^{-1}$  и  $v^{-1}u$ . При этом  $vu^{-1} = u^{-1}v(v, u^{-1})$ , а из соотношения (10.2.1.3) имеем

$$1 = (v, uu^{-1}) = (v, u^{-1})(v, u)(v, u, u^{-1}), \quad (11.1.6)$$

откуда

$$(v, u^{-1}) = (v, u, u^{-1})^{-1}(v, u)^{-1}.$$

Аналогично

$$(v, u, u^{-1}) = (v, u, u, u^{-1})^{-1}(v, u, u)^{-1}.$$

Положив  $v_0 = v$  и  $v_{t+1} = (v_t, u)$ , получим

$$\begin{aligned} (v, u^{-1}) &= (v_1, u^{-1})^{-1}v_1^{-1} = v_2(v_2, u^{-1})v_2^{-1} = \\ &\equiv v_2v_4 \dots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}. \end{aligned} \quad (11.1.7)$$

Если здесь коммутатор  $v_1 = (v, u)$  базисный, то и  $v_2, v_3, \dots$  — также базисные коммутаторы. По модулю  $F_{k+1}$  мы можем пренебречь коммутатором  $(v_s, u^{-1})$ , если индекс  $s$  настолько велик, что вес этого коммутатора не меньше  $k+1$ . Следовательно, в качестве элементарного этапа собирательного процесса мы допускаем следующую замену:

$$vu^{-1} \equiv u^{-1}v \cdot v_2v_4 \dots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}. \quad (11.1.8)$$

Аналогично,  $v^{-1}u = uv^{-1}(v^{-1}, u)$ , и из равенства (10.2.1.2) получаем  $1 = (vv^{-1}, u) = (v, u)(v, u, v^{-1})(v^{-1}, u)$ , откуда, полагая  $w_1 = (v, u)$ ,  $w_{t+1} = (w_t, v)$ , имеем

$$v^{-1}u \equiv uv^{-1}w_2w_4 \dots w_3^{-1}w_1^{-1} \pmod{F_{k+1}}. \quad (11.1.9)$$

Имеет место тождество  $v^{-1}u^{-1} = u^{-1}(uvu^{-1})^{-1}$ , а из (11.1.8) получаем

$$uvu^{-1} \equiv v \cdot v_2v_4 \dots v_5^{-1}v_3^{-1}v_1^{-1} \pmod{F_{k+1}}, \quad (11.1.10)$$

откуда

$$v^{-1}u^{-1} \equiv u^{-1}v_1v_3v_5 \dots v_4^{-1}v_2^{-1}v^{-1} \pmod{F_{k+1}}. \quad (11.1.11)$$

Повторное применение замен (11.1.5, 8, 9, 11) приводит к записи (11.1.4) произвольного элемента  $f$  группы  $F$  в виде слова из базисных коммутаторов.

Если  $F$  — свободная группа с образующими  $x_1, x_2, \dots, x_r$ , то, как мы покажем в § 11.2, при заданной нумерации базисных коммутаторов запись (11.1.4) единственна. В частности, базисные коммутаторы веса  $k$  образуют свободный базис факторгруппы  $F_k/F_{k+1}$ , являющейся, следовательно, свободной абелевой группой. Это обстоятельство, конечно, оправдывает термин *базисный* в применении к этим коммутаторам.

## 11.2. Формула Витта. Теорема о базисе

Предположим, нам дана последовательность базисных коммутаторов  $c_1, c_2, \dots$ , состоящих из образующих  $x_1, x_2, \dots, x_r$ . Назовем произведение базисных коммутаторов

$$c_{i_1}c_{i_2} \dots c_{i_s} \quad (11.2.1)$$

*базисным*, если слово (11.2.1) собрано, т. е. если  $i_1 \leq i_2 \leq \dots \leq i_s$ . Для произведения коммутаторов  $p = a_1a_2 \dots a_n$  произвольного вида мы определим понятие веса  $\omega(p)$ :  $\omega(p) = \omega(a_1) + \dots + \omega(a_n)$ . Собирательный процесс изменяет вес произведения. Мы определим сейчас аналогичный процесс — *процесс заключения в скобки*, не меняющий веса произведения. Если  $u, v$  и  $(u, v)$  — базисные коммутаторы, то слово  $\dots uv \dots$  заменяется на  $\dots (u, v) \dots$  в отличие от собирательного процесса, где слово  $\dots uv \dots$  заменяется произведением  $\dots vu(u, v) \dots$ .

**Теорема 11.2.1.** Число базисных произведений веса  $n$ , составленных из образующих  $x_1, \dots, x_r$ , равно  $r^n$ .

*Доказательство.* Для всех  $k = 1, 2, \dots$  определим семейство  $P_k = P_k^{(n)}$  всех произведений  $a_1a_2 \dots a_t$  веса  $n$  (где  $a_i$  — базисные коммутаторы) вида

$$c_1^{e_1}c_2^{e_2} \dots c_k^{e_k}c_{i_1} \dots c_{i_s}, \quad (11.2.2)$$

где  $e_i \geq 0$ ,  $i_1 > k$ ,  $i_2, \dots, i_s \geq k$ , и для каждого коммутатора  $c_{i_j} = (c_u, c_v)$  коммутатор  $c_v$  предшествует  $c_k$ . Таким образом,  $P_k$  можно рассматривать как семейство слов, в которых коммутаторы  $c_1, \dots, c_{k-1}$  собраны, а  $c_k$  еще не собраны. Обозначим число таких произведений семейства  $P_k$  через  $|P_k|$ . Ясно, что  $P_1$  — семейство всех произведений  $n$  образующих  $x_i$ , откуда  $|P_1| = r^n$ . Можно установить взаимно однозначное соответствие между элементами семейств  $P_k$  и  $P_{k+1}$ . Действительно, если  $c_1^{e_1} \dots c_k^{e_k} c_{i_1} \dots c_{i_s}$  — произведение из семейства  $P_k$ , то коммутатор  $c_{i_1}$  следует за  $c_k$  и, хотя в произведении могут встречаться цепочки коммутаторов  $c_k$  в несобранной части, каждой такой цепочке непосредственно предшествует коммутатор  $c_y$ , где  $y > k$ . Ко всем подобным цепочкам

$$c_y c_k \dots c_k c_w, \quad y > k, \quad w > k,$$

применим операции заключения в скобки, заменив их выражениями  $((c_y, c_k), c_k), \dots, c_k) c_w$ , и так как при условии  $c_y = (c_u, c_v)$ ,  $k > v$ , то вновь возникающий коммутатор будет опять базисным и будет следовать за  $c_k$ . Указанное преобразование дает однозначно определенное произведение из семейства  $P_{k+1}$ . Обратно, если в произведении из семейства  $P_{k+1}$  убрать все скобки, заключающие коммутатор  $c_k$ , то мы получим однозначно определенное произведение из семейства  $P_k$ . Следовательно,  $|P_k| = |P_{k+1}|$ , откуда для любого  $k$  имеем  $|P_k| = |P_1| = r^n$ . Но при достаточно большом  $k$  семейство  $P_k$  состоит из всех базисных произведений веса  $n$ . Этим теорема доказана.

С помощью теоремы 11.2.1 можно найти число базисных коммутаторов веса  $n$ , и, даже более того, можно найти число базисных коммутаторов с заданными весами относительно каждого образующего. Определим вес  $\omega_i(c)$ ,  $i = 1, 2, \dots, r$ , следующим образом:  $\omega_i(x_i) = 1$ ,  $\omega_i(x_j) = 0$ ,  $i \neq j$ , а далее по правилу  $\omega_i[(c_u, c_v)] = \omega_i(c_u) + \omega_i(c_v)$ . Пусть  $M_r(n)$  — число базисных коммутаторов веса  $n$  от  $r$  образующих  $x_1, x_2, \dots, x_r$ , и пусть  $M(n_1, n_2, \dots, n_r)$  — число таких коммутаторов  $c$ , что  $\omega_i(c) = n_i$ ,  $i = 1, 2, \dots, r$ , причем  $n = n_1 + n_2 + \dots + n_r$ . Тогда имеет место следующая теорема.

Теорема 11.2.2. (Теорема Витта.)

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu(d) r^{n/d}, \quad (11.2.3)$$

$$M(n_1, n_2, \dots, n_r) = \frac{1}{n} \sum_{d|n} \mu(d) \left(\frac{n}{d}\right)! \left|\left(\frac{n_1}{d}\right)! \dots \left(\frac{n_r}{d}\right)!\right| \quad (11.2.4)$$

Здесь  $\mu(m)$  — функция Мёбиуса, определенная на множестве натуральных чисел следующим образом:  $\mu(1) = +1$ ; для  $n = p_1^{e_1} \dots p_s^{e_s}$ , где  $p_1, \dots, p_s$  — различные простые числа,  $\mu(n) = 0$ , если хоть один показатель степени  $e_i > 1$ , а  $\mu(p_1 p_2 \dots p_s) = (-1)^s$ .

*Доказательство.* Согласно теореме 11.2.1, число базисных произведений равно  $r^n$ . Это приводит к следующему формальному тождеству для степенных рядов от переменной  $z$ :

$$\frac{1}{1 - rz} = \prod_{n=1}^{\infty} (1 - z^n)^{-M_r(n)}.$$

Процесс расстановки скобок оставляет веса  $\omega_i (i = 1, \dots, r)$  неизменными. Число слов  $W$  от образующих  $x_1, \dots, x_r$  с весом  $\omega_i(W) = n_i$  равно, очевидно,

$$\frac{n!}{n_1! \dots n_r!}.$$

Отсюда вытекает формальное тождество для рядов от переменных  $z_1, \dots, z_r$ :

$$\frac{1}{1 - z_1 - \dots - z_r} = \prod_{n_1, \dots, n_r=1}^{\infty} (1 - z_1^{n_1} \dots z_r^{n_r})^{-M(n_1, \dots, n_r)}. \quad (11.2.6)$$

Витт [2] исходил из указанных тождеств, переходил к логарифмам и применял формулу обращения Мёбиуса для доказательства формул теоремы. Здесь же мы воспользуемся несколько видоизмененным результатом Мейера-Вундерли [1], доказав его аналогично теореме 11.2.1, и выведем из него формулу Витта.

Слово  $a_1 \dots a_n$  будем называть *циклическим*, если считать, что  $a_1$  следует за  $a_n$ , а  $a_1 a_2 \dots a_n, a_2 \dots a_n a_1, \dots, a_n a_1 \dots a_{n-1}$  — записи одного и того же слова. Циклическое слово  $C$  длины  $n$  может быть получено в результате повторения подслова из  $d$  букв  $n/d$  раз, где  $d$  — некоторый делитель  $n$ . Тогда мы будем говорить, что  $C$  — циклические слова периода  $d$ . Каждому циклическому слову соответствует единственный наименьший период, который в свою очередь однозначно определяет некоторое циклическое слово длины  $d$ .

**Лемма 11.2.1.** *Между базисными коммутаторами веса  $n$  и циклическими словами длины  $n$  имеется место взаимно однозначное соответствие. Оно осуществляется подходящей расстановкой скобок в циклическом слове.*

*Доказательство.* Пусть  $a_1 a_2 \dots a_n$  — циклическое слово длины  $n$ . Циклические слова веса  $n$  образуют семейство  $C_k^n = C_k$ , если они вида  $c_{i_1} c_{i_2} \dots c_{i_s}$ , где  $c_{i_j}$  — базисные коммутаторы, и

для любого  $c_{ij} = c_w$ , если  $c_w = (c_u, c_v)$ , то  $v < k$ , причем или (1)  $i_1 = i_2 = \dots = i_s$  (включая случай  $s=1$ ), или (2)  $i_1, \dots, i_s \geq k$  и некоторый индекс  $i_j > k$ . Если имеет место случай (1), то слово принадлежит, по определению, также семейству  $C_{k+1}$ , если же налицо случай (2), то мы берем каждую циклическую подпоследовательность (если таковые существуют) вида  $c_w, c_k, \dots, c_k, c_t, w > k, t > k$ , и расставляем скобки следующим образом:

$$((\dots((c_w, c_k), \dots, c_k) c_t.$$

Получается вполне определенное циклическое слово из семейства  $C_{k+1}$ . Обратно, удалив из какого-либо слова семейства  $C_{k+1}$  все скобки, заключающие  $c_k$ , получаем определенное слово из семейства  $C_k$ . Таким образом, установлено существование однозначного соответствия между словами семейства  $C_{k+1}$  и семейства  $C_k$  для произвольного  $k$ . Если же  $k$  достаточно велико, то коммутатор  $c_k$  имеет вес, больший  $n$ , и случай (2) невозможен. Следовательно, в итоге процесс расстановки скобок прерывается и получается циклическое слово, для которого имеет место случай (1). Это слово будет или базисным коммутатором веса  $n$ , или последовательностью  $s = n/d$  тождественных базисных коммутаторов веса  $d$ . Расстановка скобок, при помощи которой осуществляется переход от семейства  $C_k$  к семейству  $C_{k+1}$ , охватывает один коммутатор  $c_w$  и некоторое число коммутаторов  $c_k$ . Следовательно, каждая такая расстановка скобок осуществляется только внутри одного периода и в точности повторяется во всех остальных процессах. При всем этом число периодов в слове остается неизменным. Следовательно, расстановка скобок во всех циклических словах длины (и периода)  $n$  дает все базисные коммутаторы веса  $n$ , а в случае  $d|n$  дает все базисные коммутаторы веса  $d$ , повторенные  $n/d$  раз каждый, так как все они являются членами семейства  $C_k$  при достаточно большом  $k$ . Приведенные рассуждения доказывают утверждение леммы и даже несколько больше.

Сколько существует циклических слов длины и периода  $n$ ? Циклическое слово длины  $n$  и периода  $d$ , где  $d|n$ , дает точно  $d$  обычных<sup>1)</sup> слов длины  $n$ :

$$\begin{aligned} &a_1 \dots a_d a_1 \dots a_d \dots a_1 \dots a_d \\ &a_2 \dots a_d a_1 \dots a_1 \dots a_d a_1 \\ &\dots \dots \dots \dots \dots \dots \\ &a_d a_1 \dots a_d \dots a_1 \dots a_{d-1}. \end{aligned}$$

<sup>1)</sup> То есть нециклических. — Прим. ред.

Таким образом,  $r^n = \sum_{d|n} dM_r(d)$ , так как число циклических слов длины и периода  $d$  равно  $M_r(d)$  и каждому из  $r^n$  обычных слов соответствует вполне определенный период  $d$ . Из тождества

$$r^n = \sum_{d|n} dM_r(d) \quad (11.2.7)$$

можно найти  $M_r(d)$ , пользуясь формулой обращения Мёбиуса<sup>1)</sup>: если

$$f(n) = \sum_{d|n} g(d), \quad (11.2.8)$$

то

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \quad (11.2.9)$$

Отсюда

$$nM_r(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d$$

или

$$M_r(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) r^d. \quad (11.2.10)$$

т. е. получим формулу Витта.

Число обычных слов  $W$ , таких, что  $\omega_i(W) = n_i$ , где  $n_1 + \dots + n_r = n$ , равно

$$\frac{n!}{n_1! \dots n_r!}.$$

Это приводит к формуле

$$\frac{n!}{n_1! \dots n_r!} = \sum_{d|n_1, \dots, n_r} dM\left(\frac{n_1}{d}, \frac{n_2}{d}, \dots, \frac{n_r}{d}\right). \quad (11.2.11)$$

Здесь  $d$  пробегает все делители числа  $n_0 = (n_1, \dots, n_r)$ . Применяя формулу обращения Мёбиуса, мы получаем вторую формулу Витта:

$$M(n_1, n_2, \dots, n_r) = \frac{1}{n} \sum_{d|n_1, \dots, n_r} \mu(d) \frac{\left(\frac{n}{d}\right)!}{\left(\frac{n_1}{d}\right)! \dots \left(\frac{n_r}{d}\right)!}. \quad (11.2.12)$$

Рассмотрим свободное ассоциативное кольцо  $R$  с целочисленными коэффициентами и с  $r$  образующими  $x_1, x_2, \dots, x_r$ .

<sup>1)</sup> Харди и Райт [1], стр. 235 (см. также Хассе Г., Лекции по теории чисел, ИЛ, М., 1953, стр. 58. — Прим. перев.).

Элементы степени  $m$  образуют свободную абелеву группу  $R_m$  с базисом, состоящим из  $r^m$  произведений вида  $x_{i_1} \dots x_{i_m}$ . В этом кольце  $R$  мы следующим образом определяем коммутатор  $[u, v]$ :

$$[u, v] = uv - vu. \quad (11.2.13)$$

Формальные свойства расстановки скобок для коммутаторов кольца те же, что и для коммутаторов групп. Мы покажем, что в действительности существует очень тесная связь между групповыми и кольцевыми коммутаторами, которая впервые была установлена Магнусом [1].

**Теорема 11.2.3.** *Базисные произведения степени  $m$  образуют аддитивный базис группы  $R_m$ .*

**Следствие 11.2.1.** *Базисные коммутаторы степени  $m$  линейно независимы.*

**Доказательство.** Так как, согласно теореме 11.2.1, число базисных произведений степени  $m$  равно  $r^m$ , т. е. числу базисных элементов группы  $R_m$ , то достаточно показать, что любой элемент из  $R_m$  может быть представлен как линейная комбинация базисных произведений с целыми коэффициентами. Так как семейство  $P_1^{(m)} = P_1$  образует базис, состоящий из  $r^m$  произведений  $x_{i_1} \dots x_{i_m}$ , и так как для достаточно большого  $k$  семейство  $P_k$  состоит из базисных произведений, то достаточно выразить элементы из  $P_k$  в виде линейных комбинаций с целыми коэффициентами элементов из  $P_{k+1}$ . Для этого нам понадобится одно тождество. Для упрощения записи введем обозначения:

$$[\dots [u, v], v \dots], v = [u, \overbrace{v, \dots, v}^s, v] = [^s u, v^s],$$

если число букв  $v$  равно  $s$ .

Необходимое нам тождество выглядит так:

$$uv^s = v^s u + \sum_{j=1}^s \binom{s}{j} v^{s-j} [^j u, v^j]. \quad (11.2.14)$$

При  $s = 1$  оно сводится к  $uv = vu + [u, v]$ . Предположив выполнимость (11.2.14) для  $s$ , при помощи тождества

$$[^j u, v^j] v = [^{j+1} u, v^{j+1}] + v[^j u, v^j] \quad (11.2.15)$$

легко показать справедливость равенства (11.2.14) для  $s + 1$ . Для этого нужно умножить (11.2.14) справа на  $v$ , применить соотношение (11.2.15) и собрать подобные члены.

Если элемент из  $P_k$  содержит подпоследовательность вида  $\dots uc_k \dots c_k w \dots u$ ,  $w \neq c_k$ , где коммутатор  $u$  больше ком-

мутатора  $c_k$ , который встречается здесь  $s$  раз, то мы применяем тождество (11.2.14), полагая  $u = u$ ,  $v = c_k$ . При этом получаются произведения или принадлежащие семейству  $P_{k+1}$ , или семейству  $P_k$  с меньшим числом коммутаторов  $c_k$ , или содержащие коммутаторы  $c_k$  ближе к началу слова. В результате многократного применения тождества (11.2.14) произведение из  $P_k$  представится в виде линейной комбинации с целыми коэффициентами элементов из  $P_{k+1}$ . Теорема доказана.

Присоединим теперь к кольцу  $R$  единицу 1 и будем рассматривать целые рациональные числа как элементы степени нуль. Их совокупность обозначим через  $R_0$ . Образуем в  $R$  факторкольцо  $\bar{R}$  по двустороннему идеалу, порожденному всеми членами, степени которых не меньше  $n+1$ . Тогда

$$\bar{R} = R_0 + R_1 + \dots + R_n. \quad (11.2.16)$$

В  $\bar{R}$  элементы вида  $1+z$ , где  $z \in R_1 + \dots + R_n$ , образуют группу  $G$ , так как в силу равенства  $z^{n+1} = 0$  имеем

$$(1+z)^{-1} = 1 - z + z^2 - \dots + (-1)^n z^n. \quad (11.2.17)$$

Если  $1+z = 1+u_m+u_{m+1}+\dots+u_n$ , где  $u_j \in R_j$  для  $j = m, \dots, n$  и  $u_m \neq 0$ , то мы говорим, что  $u_m$  — старший член<sup>1)</sup> элемента  $1+z$ . Старший член 1 равен 0.

**Лемма 11.2.2.** Пусть  $u, v \neq 1$  — элементы группы  $G$  со старшими членами  $u_s$  и  $v_t$  степеней  $s$  и  $t$  соответственно. Старшими членами элементов  $u^{-1}$  и  $v^{-1}$  являются элементы —  $u_s$  и  $-v_t$ . Если  $s < t$ , то старший член элемента  $uv$  есть  $u_s$ . Если  $t < s$ , то старший член  $uv$  равен  $v_t$ . Если  $t = s$  и  $u_s + v_t \neq 0$ , то старший член произведения равен  $u_s + v_t$ . Если кольцевой коммутатор  $[u_s, v_t]$  не равен нулю, то он является старшим членом группового коммутатора  $(u, v)$ .

**Доказательство.** Пусть  $u = 1+a$ ,  $v = 1+b$ ,  $u^{-1} = 1+a'$ ,  $v^{-1} = 1+b'$ . Тогда

$$\begin{aligned} a + a' + aa' &= 0, \quad aa' = a'a, \\ b + b' + bb' &= 0, \quad bb' = b'b, \\ a = u_s + \dots + u_n, \quad b = v_t + \dots + v_n, \\ uv &= 1 + a + b + ab. \end{aligned}$$

Из этих соотношений сразу получаются утверждения леммы о старших членах элементов  $u^{-1}$ ,  $v^{-1}$  и  $uv$ . Используя эти же соотношения, получаем

$$\begin{aligned} (u, v) &= u^{-1}v^{-1}uv = (1+a')(1+b')(1+a)(1+b) = \\ &= 1 + ab - ba + aa'b - bb'a + b'ab + a'b'a + a'b'ab, \end{aligned}$$

<sup>1)</sup> В смысле принятого ранее порядка. — Прим. ред.

откуда

$$(u, v) = 1 + [u_s, v_t] + \text{слагаемые более высокой степени.} \quad (11.2.18)$$

Лемма доказана.

Пусть  $c_1, c_2, \dots$  — последовательность базисных коммутаторов свободной группы  $F$ , порожденной элементами  $y_1, \dots, y_r$ , и пусть  $d_1, d_2, \dots$  — кольцевые коммутаторы в кольце  $R$ , получающиеся заменой  $y_1, \dots, y_r$  на  $x_1, \dots, x_r$ . Кроме того, пусть  $c_t$  — последний коммутатор веса  $n$ . Тогда существует соответствие между коммутаторами  $c_l$  и  $d_l$  в кольце  $\bar{R}$ , устанавливаемое следующей леммой.

**Лемма 11.2.3.** *При соответствии  $y_i \rightarrow 1 + x_i$ ,  $i = 1, 2, \dots, r$ , определяющем отображение группы  $F$  на группу  $G$ , пусть  $c_l \rightarrow g_l \in G$ . Тогда старший член элемента  $g_i$  равен  $d_i$  ( $i = 1, \dots, t$ ).*

**Доказательство.** Так как  $y_i \rightarrow 1 + x_i$ ,  $i = 1, \dots, r$ , то старший член элемента  $g_i = 1 + x_i$  есть  $x_i$  при  $i = 1, \dots, r$ . Доказательство проведем методом полной индукции. Если  $c_w = (c_u, c_v)$ ,  $w \leq t$ , то, по предположению индукции, старший член элемента  $g_u$  равен  $d_u$ , а элемента  $g_v$  равен  $d_v$ . Следовательно, по лемме 11.2.2 старший член коммутатора  $(g_u, g_v)$  равен  $[d_u, d_v]$ , если последний коммутатор не равен нулю. Будучи базисным коммутатором, он на самом деле не равен нулю, как это показывает следствие из теоремы 11.2.3. Итак, старший член коммутатора  $g_w = (g_u, g_v)$  равен  $[d_u, d_v] = d_w$ , что и требовалось доказать.

**Теорема 11.2.4.** (Теорема о базисе.)<sup>1)</sup> *Если  $F$  — свободная группа со свободными образующими  $y_1, \dots, y_r$  и если в некоторой последовательности базисных коммутаторов  $c_1, c_2, \dots, c_t$  — все базисные коммутаторы весов  $1, 2, \dots, n$ , то произвольный элемент  $f$  группы  $F$  однозначно представим в виде*

$$f \equiv c_1^{e_1} c_2^{e_2} \dots c_t^{e_t} \pmod{F_{n+1}}. \quad (11.2.19)$$

*Базисные коммутаторы веса  $n$  образуют базис свободной абелевой группы  $F_n/F_{n+1}$ .*

**Доказательство.** Сначала докажем второе утверждение. Пусть  $c_s, \dots, c_t$  — базисные коммутаторы веса  $n$ . Согласно лемме 11.2.3, при отображении, определенном соответствиями

$$y_i \rightarrow 1 + x_i = g_i, \quad i = 1, \dots, r, \quad (11.2.20)$$

группы  $F$  на кольцо  $R$ , старшие члены коммутаторов  $c_s, \dots, c_t$  будут соответствующими кольцевыми коммутаторами  $d_s, \dots, d_t$ .

1) См. М. Холл [6].

являющимися кольцевыми базисными коммутаторами степени  $n$ . В силу следствия из теоремы 11.2.3 коммутаторы  $d_s \dots d_t$  линейно независимы, а по лемме 11.2.2 старший член произведения  $c_s^{e_s} \dots c_t^{e_t}$  равен  $e_s d_s + \dots + e_t d_t$ . Он не равен нулю, если только не все числа  $e_s, \dots, e_t$  равны нулю. Следовательно, коммутаторы  $c_s, \dots, c_t$  являются независимыми элементами фактор-группы  $F_n/F_{n+1}$  и, следовательно, образуют базис, так как мы уже знаем из равенства (11.1.4), что любой элемент фактор-группы  $F_n/F_{n+1}$  можно представить как произведение  $c_s \dots c_t$ . Существование по меньшей мере одного представления для элемента  $f$  в виде (11.2.19) установлено соотношением (11.1.4). Покажем единственность этого представления. Действительно, если бы имело место равенство

$$c_1^{e_1} \dots c_t^{e_t} \equiv c_1^{h_1} \dots c_t^{h_t} \pmod{F_{n+1}}, \quad (11.2.21)$$

где  $h_i = e_i$ ,  $i = 1, \dots, j - 1$ , но  $h_j \neq e_j$ , и если бы вес  $c_j$  был равен  $k$ , то это привело бы к зависимости между базисными коммутаторами веса  $k$  по модулю  $F_{k+1}$ . Но этого не может быть, следовательно, представление (11.2.19) однозначно. Теорема доказана.

## Г л а в а 12

### ТЕОРИЯ $p$ -ГРУПП. РЕГУЛЯРНЫЕ $p$ -ГРУППЫ

#### 12.1. Элементарные результаты

В гл. 4 и 10 были установлены следующие элементарные свойства конечной  $p$ -группы  $P$ :

- 1) центр  $Z$  группы  $P$  отличен от единицы (теорема 4.3.1);
- 2) собственная подгруппа  $H$  группы  $P$  не совпадает со своим нормализатором (теорема 4.3.3);
- 3) если порядок группы  $P$  равен  $p^n$ , то любая максимальная подгруппа  $M$  имеет порядок  $p^{n-1}$  и инвариантна в  $P$  (теорема 4.3.2);
- 4) инвариантная подгруппа порядка  $p$  группы  $P$  содержится в центре группы  $P$  (теорема 4.3.4);
- 5) группа  $P$  сверхразрешима (теоремы 10.3.4 и 10.2.4);
- 6) группа  $P$  нильпотентна (теорема 10.3.4).

#### 12.2. Теорема Бернсайда о базисе. Автоморфизмы $p$ -групп

Пусть  $P$  — группа порядка  $p^n$ . Пересечение всех ее максимальных подгрупп — характеристическая подгруппа  $D$  группы  $P$  (подгруппа Фраттини группы  $P$ ). Следовательно, при естественном гомоморфизме  $P \rightarrow P/D$  образующие элементы группы  $P$  отображаются в образующие элементы фактор-группы  $P/D$ . Обратное утверждение также выполняется. Оно составляет содержание теоремы Бернсайда о базисе.

**Теорема 12.2.1.** (Теорема Бернсайда о базисе.) *Пусть  $D$  — пересечение максимальных подгрупп  $p$ -группы  $P$ . Тогда фактор-группа  $P/D = A$  — элементарная абелева группа. Если порядок группы  $A$  равен  $p^r$ , то любое множество образующих элементов  $z_1, \dots, z_s$  группы  $P$  содержит подмножество из  $r$  элементов  $x_1, \dots, x_r$ , также порождающих группу  $P$ . При отображении  $P \rightarrow A$  элементы  $x_1, \dots, x_r$  отображаются в базис  $a_1, \dots, a_r$  группы  $A$ . Обратно, любое множество  $r$  элементов группы  $P$ , отображаемое при  $P \rightarrow A$  на базис группы  $A$ , является системой образующих группы  $P$ .*

*Доказательство.* Если  $M$  — максимальная подгруппа группы  $P$ , то индекс ее равен  $p$  и она инвариантна. Поэтому фактор-группа

$P/M$  — циклическая группа порядка  $p$ . Следовательно,  $p$ -е степени любого элемента из  $P$  и все коммутаторы содержатся в подгруппе  $M$ . Таким образом, пересечение  $D$  всех максимальных подгрупп содержит любую  $p$ -ю степень и любой коммутатор. Поэтому фактор-группа  $P/D=A$  является элементарной абелевой группой. Если ее порядок равен  $p^r$ , то любой ее базис состоит из  $r$  элементов  $a_1, \dots, a_r$ . Если  $b_1, \dots, b_s$  — элементы, порождающие группу  $A$ , то мы можем найти базис этой группы, удаляя из множества  $b_1, \dots, b_s$  элементы, равные 1, а также элементы  $b_i$ , принадлежащие подгруппе, порождаемой элементами  $b_1, \dots, b_{i-1}$ . Итак,  $s \geq r$ , и множество  $b_1, \dots, b_s$  содержит подмножество, являющееся базисом группы  $A$ .

Предположим теперь, что элементы  $z_1, \dots, z_s$  порождают группу  $P$ . Пусть при отображении  $P \rightarrow P/D=A$  образами элементов  $z_i$  являются элементы  $b_i$  ( $i=1, \dots, s$ ). Тогда множество элементов  $b_1, \dots, b_s$  порождает группу  $A$  и поэтому содержит подмножество  $a_1, \dots, a_r$ , являющееся базисом группы  $A$ . Пусть тогда  $x_1, \dots, x_r$  — те из элементов  $z_1, \dots, z_s$ , которые отображаются в элементы  $a_1, \dots, a_r$ . Теорема будет доказана, если мы покажем, что множество  $x_1, \dots, x_r$  элементов группы  $P$  порождает ее. Пусть  $H=\{x_1, \dots, x_r\}$ . Если  $H \neq P$ , то подгруппа  $H$  содержится в некоторой максимальной подгруппе  $M$  группы  $P$ . Но тогда при отображении  $P \rightarrow P/D=A$  мы имеем  $H \rightarrow HD/D \subseteq M/D=B$ , где  $B$  — подгруппа порядка  $p^{r-1}$  группы  $A$ . Но это противоречит тому, что  $H=\{x_1, \dots, x_r\} \rightarrow \{a_1, \dots, a_r\}=A$ . Следовательно,  $H=P$ , т. е. элементы  $x_1, \dots, x_r$  порождают группу  $P$ .

С помощью этой теоремы мы можем получить некоторые сведения о группе автоморфизмов  $A(P)$  группы  $P$ . Базис  $a_1, \dots, a_r$  группы  $P/D$  можно выбрать  $\theta(p^r)=(p^r-1)(p^r-p) \dots (p^r-p^{r-1})$  различными способами. Действительно, первый элемент  $a_1$  может быть любым из  $p^r-1$  элементов группы  $A$ , отличных от единицы. После того как уже выбраны элементы  $a_1, \dots, a_i$ , в качестве следующего базисного элемента  $a_{i+1}$  можно выбрать любой из  $p^r-p^i$  элементов, не содержащихся в подгруппе, порожденной элементами  $a_1, \dots, a_i$ . Таким образом, существует  $\theta(p^r)$  базисов группы  $A$ , и каждое отображение фиксированного базиса  $a_1, \dots, a_r$  на любой другой базис  $b_1, \dots, b_r$  дает автоморфизм группы  $A$ . Но так как любой автоморфизм отображает  $a_1, \dots, a_r$  на некоторый другой базис, то существует точно  $\theta(p^r)$  автоморфизмов группы  $A$ .

Существует точно  $p^{r(n-r)}\theta(p^r)$  последовательностей  $X=(x_1, \dots, x_r)$ , порождающих группу  $P$ . Действительно, при отображении  $x_i \rightarrow a_i$ ,  $i=1, \dots, r$ , последовательность  $X$  переходит в базис группы  $A$ ; последний может быть выбран  $\theta(p^r)$

различными способами, а для каждого элемента  $a_i$  любой из  $p^{n-r}$  элементов смежного класса по  $D$ , отображаемого в  $a_i$ , может быть выбран в качестве  $x_i$ . Любой автоморфизм группы  $P$  отображает последовательности  $X$  друг в друга. Следовательно, группу  $A(P)$  автоморфизмов группы  $P$  можно рассматривать как группу подстановок на множестве последовательностей  $X$ . Но  $A(P)$  действует регулярно на множестве последовательностей  $X$ , так как автоморфизм, отображающий некоторое множество  $X$  на себя, определяет тождественное отображение на множестве элементов  $x_i$ , а следовательно, и на всей группе  $P$ , т. е. является тождественным автоморфизмом. Таким образом, множество последовательностей  $X$  распадается на области транзитивности, в каждой из которых  $k$  множеств, где  $k$  — порядок группы  $A(P)$ . Итак,  $p^{r(n-r)} \theta(p^r) = kt$ . Здесь число  $t$  можно рассматривать, как число существенно различных способов порождения группы  $P$   $r$  элементами. Будем говорить, что два семейства  $X = (x_1, \dots, x_r)$  и  $Y = (y_1, \dots, y_r)$  порождают группу  $P$  *одинаковым образом*, если из любого отношения  $\omega(x_1, \dots, x_r) = 1$  следует отношение  $\omega(y_1, \dots, y_r) = 1$ , и обратно.

Пусть  $A_1(P)$  — инвариантная подгруппа группы  $A(P)$ , индуцирующая тождественный автоморфизм в фактор-группе  $P/D$ . Эти автоморфизмы переставляют регулярно  $p^{r(n-r)}$  порождающих семейств  $X = (x_1, \dots, x_r)$ , которые отображаются в один и тот же базис  $a_1, \dots, a_r$  группы  $A$  при гомоморфизме  $P \rightarrow P/D = A$ . Таким образом, порядок подгруппы  $A_1(P)$  делит  $p^{r(n-r)}$ . Сформулируем эти результаты Ф. Холла [2] в виде теоремы.

**Теорема 12.2.2.** *Пусть  $P$  — группа порядка  $p^n$ ,  $D$  — пересечение максимальных подгрупп группы  $P$ , и пусть  $[P : D] = p^r$ . Тогда порядок группы  $A(P)$  автоморфизмов группы  $P$  делит  $p^{r(n-r)} \theta(p^r)$ . Порядок группы  $A_1(P)$  автоморфизмов, индуцирующих тождественный автоморфизм в группе  $P/D$ , делит  $p^{r(n-r)}$ .*

### 12.3. Собирательная формула

Пусть  $G$  — группа, порожденная элементами  $a_1, a_2, \dots, a_r$ . Мы выведем формулу для выражения  $(a_1 a_2 \dots a_r)^n$  через базисные коммутаторы элементов  $a_1, a_2, \dots, a_r$ . Можно считать, что  $G$  — свободная группа, порожденная элементами  $a_1, \dots, a_r$ ; тогда искомая формула тем более будет справедлива в любой группе, порожденной  $r$  элементами.

Напомним определение базисных коммутаторов, данное в § 11.1, причем установим для них более точное отношение порядка:

1)  $a_1, \dots, a_r$  — коммутаторы веса один, просто упорядоченные следующим образом:  $a_1 < a_2 < \dots < a_r$ ;

2) если базисные коммутаторы весов, меньших  $n$ , уже определены и просто упорядочены, то  $(x, y)$  — базисный коммутатор веса  $n$  тогда и только тогда, когда

а)  $x$  и  $y$  — базисные коммутаторы, причем

$$\omega(x) + \omega(y) = n,$$

б)  $x > y$ ,

в) если  $x = (u, v)$ , то  $y \geqslant v$ ;

3) коммутаторы веса  $n$  следуют за всеми коммутаторами весов, меньших  $n$ ; для коммутаторов одинакового веса  $(x_1, y_1) \leqslant (x_2, y_2)$ , если  $y_1 < y_2$  или если  $y_1 = y_2$ , но  $x_1 < x_2$ .

Рассмотрим тождество

$$(a_1 a_2 \dots a_r)^n = a_1(1) a_2(1) \dots a_r(1) a_1(2) a_2(2) \dots a_r(2) \dots a_r(n), \quad (12.3.1)$$

где мы пронумеровали образующие  $a_i$  слева направо числами в скобках от 1 до  $n$ , чтобы различать все различные вхождения буквы  $a_i$ . Так как по определению коммутатора  $SR = RS(S, R)$ , мы можем правую часть равенства (12.3.1) заменить другим равным ему выражением, в котором вместо некоторой пары  $SR$  последовательных элементов стоит произведение  $RS(S, R)$ . Эта замена сдвигает элемент  $R$  ближе к началу слова, причем появляется коммутатор  $(S, R)$ . Последовательным выполнением таких замен мы можем сдвинуть любую букву как угодно близко к началу слова. Мы будем преобразовывать (12.3.1) в следующем порядке. Сдвигаем  $a_1(2)$  влево до тех пор, пока эта буква не займет место сразу после  $a_1(1)$ , затем сдвигаем  $a_1(3)$  влево до тех пор, пока эта буква не окажется непосредственно за  $a_1(2)$ , и т. д. до тех пор, пока в начале слова не будут собраны все буквы  $a_1(i)$ ,  $i = 1, 2, \dots, n$ . Этим заканчивается первый этап собирательного процесса. После этого мы таким же образом собираем буквы  $a_2(i)$ ,  $i = 1, \dots, n$ , справа за буквами  $a_1(i)$ ,  $i = 1, \dots, n$ .

Опишем собирательный процесс более точно. После  $i$ -го этапа имеем выражение

$$(a_1 a_2 \dots a_r)^n = c_1^{e_1} c_2^{e_2} \dots c_i^{e_i} R_1 R_2 \dots R_t, \quad (12.3.2)$$

где  $c_1, c_2, \dots, c_i$  — первые  $i$  базисных коммутаторов, а  $R_1, \dots, R_t$  — базисные коммутаторы, следующие за  $c_i$ . Если  $R_{j_1}, R_{j_2}, \dots, R_{j_s}$  — те из базисных коммутаторов  $R_1, \dots, R_t$  (выписанные по порядку их следования), которые равны  $c_{i+1}$ , то мы сначала сдвигаем  $R_{j_1}$  на место, непосредственно следующее за элементом  $c_i^{e_i}$ , затем  $R_{j_2}, R_{j_3}, \dots$ , и, наконец,  $R_{j_s}$ , так что  $e_{i+1} = s$ , и тождество (12.3.2) принимает вид

$$(a_1 a_2 \dots a_r)^n = c_1^{e_1} c_2^{e_2} \dots c_{i+1}^{e_{i+1}} R_1^* \dots R_k^*. \quad (12.3.3)$$

Это был  $(i+1)$ -й этап собирательного процесса. В слове (12.3.2) назовем  $c_1^{e_1} \dots c_i^{e_i}$  собранной частью, а  $R_1 \dots R_t$  — несобранной. Но для оправдания приведенного выше описания мы должны показать, что при таком процессе в каждой формуле могут возникнуть только базисные коммутаторы. Исходная формула (12.3.1) представляет собой нулевой этап и содержит только образующие  $a_i$ , являющиеся базисными коммутаторами веса один. Предположим по индукции, что на  $i$ -м этапе преобразований несобранная часть  $R_1 \dots R_t$  содержит только базисные коммутаторы, следующие за  $c_i$ . В процессе собирания коммутаторов  $R_{j_1}, \dots, R_{j_s}$ , равных  $c_{i+1}$ , мы вводим только коммутаторы вида  $(c_j, c_{i+1}, \dots, c_{i+1})$ , где  $j \geq i+2$ . Такие коммутаторы являются базисными, так как если  $c_j = (c_r, c_s)$ , то коммутатор  $c_j$  возник на  $s$ -ом этапе, когда собирались коммутаторы  $c_s$ , откуда  $s < i+1$ , и поэтому  $c_s < c_{i+1}$ . Таким образом, коммутатор  $(c_j, c_{i+1})$  базисный, и, следовательно,  $(c_j, c_{i+1}, \dots, c_{i+1})$  — также базисный коммутатор.

Мы уже пометили в формуле (12.3.1) вхождения образующих  $a_i$  метками  $j$ :  $a_i(j)$ ,  $j = 1, \dots, n$ . Пусть коммутатор  $R$  веса  $w_1$  имеет уже метку  $(\lambda_1, \dots, \lambda_{w_1})$ , а коммутатор  $S$  веса  $w_2$  — метку  $(\mu_1, \dots, \mu_{w_2})$ ; сопоставим тогда коммутатору  $(R, S)$  метку  $(\lambda_1, \dots, \lambda_{w_1}, \mu_1, \dots, \mu_{w_2})$ . Вычисление показателей  $e_1, \dots, e_i, e_{i+1}$  в формуле (12.3.3) может быть осуществлено с помощью определенных нами меток. При этом  $e_{i+1} = s$  есть число несобранных коммутаторов, равных  $c_{i+1}$ , на  $i$ -ом этапе, т. е. это число вхождений коммутатора  $c_{i+1}$  на  $i$ -ом этапе. Пусть  $c_{i+1} = (c_r, c_s)$ ; тогда коммутатор  $c_{i+1}$  возникал всякий раз, когда собирались коммутаторы, равные  $c_s$ , причем  $c_{i+1}$  появлялся, когда вхождение коммутатора  $c_r$  предшествовало вхождению  $c_s$  в несобранной части слова. Следовательно, мы должны также учитывать условия предшествования вхождения коммутатора  $c_r$  вхождению  $c_s$ , когда оба они встречаются в несобранной части.

На нулевом этапе присутствуют только коммутаторы веса один, и для любого индекса  $\lambda = 1, \dots, n$  существует элемент  $a_k(\lambda)$ . При этом элемент  $a_k(\lambda)$  предшествует элементу  $a_s(\mu)$  на нулевом этапе при  $k > s$ , если  $\lambda < \mu$ , а при  $k < s$ , если  $\lambda \leq \mu$ . Итак, в терминах меток на нулевом этапе мы имеем следующие условия существования и предшествования:

$$E_k^0[a_k(\lambda)], \text{ если метка } \lambda \text{ существует (условие пустое),}$$

$$P_{rs}^0[a_r(\lambda)] \text{ предшествует } a_s(\mu)]$$

$$\begin{cases} \lambda < \mu, & \text{если } r > s \\ \lambda \leq \mu & \text{для } r < s \end{cases}.$$

Пусть  $\lambda_1, \dots, \lambda_m$  — множество целых чисел; рассмотрим условия типа  $\lambda_t < \lambda_u$ ,  $\lambda_t \leq \lambda_u$ . Всякие условия, получающиеся с помощью логического сложения и умножения из условий подобных неравенств, будем называть условиями (L). Покажем, что условия  $E_k^i$  существования коммутатора  $c_k$  с меткой  $(\lambda_1, \dots, \lambda_m)$  на  $i$ -ом этапе являются условиями (L) для чисел  $\lambda_1, \dots, \lambda_m$ , а условия предшествования  $P_{rs}^i$  коммутатора  $c_r$  коммутатору  $c_s$  в несобранной части на  $i$ -ом этапе являются условиями (L) для чисел  $\lambda_1, \dots, \lambda_m, \mu_1, \dots, \mu_q$ , если  $(\lambda_1, \dots, \lambda_m)$  — метка коммутатора  $c_r$ , а  $(\mu_1, \dots, \mu_q)$  — метка коммутатора  $c_s$ . Как мы заметили, на нулевом этапе условия существования и предшествования были условиями (L). Докажем по индукции, что это верно на любом этапе. Пусть утверждение верно для  $i$ -го этапа. Чтобы показать его истинность для  $(i+1)$ -го этапа, сравним тождества (12.3.2) и (12.3.3). Для  $R_{j_1} = R_{j_2} = \dots = R_{j_s} = c_{i+1}$  мы собирали сначала  $R_{j_1}$ , затем  $R_{j_2}$  и, наконец,  $R_{j_s}$ . На каждом шаге мы производили замену  $SR$  на  $RS(S, R)$ . При этом любые коммутаторы, существовавшие на  $i$ -ом этапе и отличные от  $c_{i+1}$ , сохраняются также на  $(i+1)$ -ом этапе в том же порядке. Таким образом, для таких коммутаторов

$$E_k^{i+1} = E_k^i \quad \text{и} \quad P_{rs}^{i+1} = P_{rs}^i.$$

Следовательно, нам нужно только рассмотреть условия существования коммутаторов  $c_k$ , возникающих на  $(i+1)$ -ом этапе, и предшествования  $P_{rs}^{i+1}$ , где или один из коммутаторов  $c_r, c_s$ , или оба возникли на рассматриваемом этапе. Коммутатор, возникший на  $(i+1)$ -ом этапе, имеет вид  $c_k = (c_j, R_{u_1}, \dots, R_{u_m})$ , где  $R_{u_i} = c_{i+1}$ . Он был получен перестановкой  $R_{u_1}$  с  $c_j$ , затем  $R_{u_2}$  с возникшим при этом коммутатором и т. д., пока, наконец, мы не поменяли местами  $R_{u_m}$  с коммутатором  $(c_j, R_{u_1}, \dots, R_{u_{m-1}})$ . При этом все коммутаторы  $R_{u_1}, \dots, R_{u_m}$  равны  $c_{i+1}$ .  $E_k^{i+1}$  — логическое произведение условий существования коммутаторов  $c_j, R_{u_1}, \dots, R_{u_m}$  на  $i$ -ом этапе и условий предшествования, согласно которым на  $i$ -ом этапе коммутаторы  $c_j, R_{u_1}, \dots, R_{u_m}$  расположены именно в рассматриваемом порядке. Таким образом,  $E_k^{i+1}$  — условие (L) для метки коммутатора  $c_k$ . На  $(i+1)$ -ом этапе коммутатор  $(S, R)$  возникает в произведении  $SR = RS(S, R)$  непосредственно за элементом  $S$ , но перед всеми коммутаторами, следующими за  $S$ . Мы должны найти условие предшествования  $P_{rs}^{i+1}$ , где  $c_r = c_{j_1}$  или  $c_r = (c_{j_1}, R_{u_1}, \dots, R_{u_m})$  и  $c_s = c_{j_2}$  или  $c_s = (c_{j_2}, R_{v_1}, \dots, R_{v_w})$ . Если  $c_{j_1} \neq c_{j_2}$ , то  $P_{rs}^{i+1} = P_{j_1 j_2}^i$ . Если же  $c_{j_1} = c_{j_2}$ , то условие  $P_{rs}^{i+1}$  зависит от коммутаторов  $R_{u_i}, R_{v_j}$ . Пусть  $e$  — наибольшее целое

число, такое, что  $R_{u_1} = R_{v_1}, \dots, R_{u_e} = R_{v_e}$ . Тогда  $c_r$  предшествует  $c_s$ , если или (1)  $m = e$  и не существует коммутатора  $R_{u_{e+1}}$  (в этом случае  $c_s$  есть коммутатор от коммутатора  $c_r$ ), или (2) коммутатор  $R_{v_{e+1}}$  предшествует  $R_{u_{e+1}}$ . Тогда  $P_{rs}^{i+1}$  — логическая сумма условий предшествования<sup>1)</sup>, которые поэтому являются также условиями (L) для меток коммутатора  $c_r$  и  $c_s$ .

**Лемма 12.3.1.** Число последовательностей  $\lambda_1, \dots, \lambda_m$  ( $1 \leq \lambda_i \leq n$ ), удовлетворяющих данным условиям (L), выражается в виде полинома от  $n$ :  $b_1n + b_2n^{(2)} + \dots + b_mn^{(m)}$ , где  $n^{(i)} = n(n-1)\dots(n-i+1)/i!$ , а  $b_i$  — числа, определяемые данным условием (L), но не зависящие от  $n$ .

**Доказательство.** Разобьем индексы  $1, \dots, m$  на непересекающиеся множества  $S_1, S_2, \dots, S_t$ . Выберем  $t$  чисел  $v_1 < v_2 < \dots < v_t \leq n$ . Если в некоторой последовательности  $\lambda_1, \lambda_2, \dots, \lambda_m$  имеет место  $\lambda_j = v_i$  для  $j \in S_i$ , то тем самым определено упорядочение чисел  $\lambda_i$  по величине. Для любого возможного выбора чисел  $\lambda_i$  существует вполне определенный порядок указанного типа<sup>2)</sup>. Число возможных выборов  $v_1 < v_2 < \dots < v_t \leq n$  равно  $n^{(t)}$ , так как оно просто равно числу сочетаний из  $n$  по  $t$ . При подобном упорядочении чисел  $\lambda_i$ <sup>3)</sup> или все последовательности  $\lambda_1, \dots, \lambda_m$  данного типа упорядочения удовлетворяют условиям (L), или ни одна из них не удовлетворяет этим условиям. Следовательно, число последовательностей  $\lambda_1, \dots, \lambda_m$ , удовлетворяющих данным условиям (L), есть полином  $b_1n + b_2n^{(2)} + \dots + b_mn^{(m)}$ , где  $b_t$  — число возможных упорядочений с  $t$  различными значениями, удовлетворяющими условиям (L), и, очевидно, числа  $b_t$  зависят от этих условий, но не от  $n$ .

Например, если числа  $\lambda_1, \lambda_2, \lambda_3$  удовлетворяют условиям (L)  $\lambda_1 < \lambda_2, \lambda_3 \leq \lambda_2$ , то возможны следующие упорядочения, удовлетворяющие условиям (L):

- 1)  $\lambda_1 = v_1, \lambda_2 = \lambda_3 = v_2, v_1 < v_2,$
- 2)  $\lambda_1 = \lambda_3 = v_1, \lambda_2 = v_2, v_1 < v_2,$
- 3)  $\lambda_1 = v_1, \lambda_3 = v_2, \lambda_2 = v_3, v_1 < v_2 < v_3,$
- 4)  $\lambda_3 = v_1, \lambda_1 = v_2, \lambda_2 = v_3, v_1 < v_2 < v_3,$

а число последовательностей  $\lambda_1, \lambda_2, \lambda_3$ , удовлетворяющих условиям (L), равно  $2n^{(2)} + 2n^{(3)}$ .

Мы уже показали, что показатель степени  $e_i$  коммутатора  $c_i$  в тождестве (12.3.2) равен числу коммутаторов, равных  $c_i$  в не-

<sup>1)</sup> Для этапов, предшествующих  $(i+1)$ -му. — Прим. перев.

<sup>2)</sup> Для подходящего разбиения  $S_1, S_2, \dots, S_t$  и чисел  $v_1 < v_2 < \dots < v_t \leq n$ . — Прим. ред.

<sup>3)</sup> При фиксированном разбиении  $S_1, S_2, \dots, S_t$  и всевозможных выборах  $v_1 < v_2 < \dots < v_t \leq n$ . — Прим. ред.

собранной части слова на  $(i - 1)$ -ом этапе, и что это число можно охарактеризовать как число последовательностей  $\lambda_1, \dots, \lambda_m$ , удовлетворяющих определенным условиям (L), где  $m$  — вес коммутатора  $c_i$ . Таким образом, в лемме 12.3.1 говорится об этих показателях степени. Сформулируем полученные результаты в виде теоремы.

**ТЕОРЕМА 12.3.1.** *Произведение  $(a_1 a_2 \dots a_r)^n$  представимо в виде  $(a_1 a_2 \dots a_r)^n = a_1^n a_2^n \dots a_r^n c_{r+1}^{e_{r+1}} \dots c_i^{e_i} R_1 \dots R_t$ , где  $c_{r+1}, \dots, c_i$  — выписанные в принятом порядке базисные коммутаторы элементов  $a_1, \dots, a_r$ , а  $R_1 \dots R_t$  — базисные коммутаторы, также выписанные здесь в некотором порядке, причем  $c_i < R_1$ . При  $1 \leq j \leq i$   $e_j = b_1 n + b_2 n^{(2)} + \dots + b_m n^{(m)}$ , где  $m$  — вес коммутатора  $c_j$ , а  $b_1, b_2, \dots, b_m$  — неотрицательные целые числа, зависящие только от  $c_j$  и не зависящие от  $n$ . Здесь  $n^{(k)} = n(n-1) \dots (n-k+1)/k!$*

Отсюда легко вывести важное следствие для случая, когда  $G$  —  $p$ -группа класса nilпотентности, меньшего  $p$ . Собрав все коммутаторы весов, меньших  $p$ , мы сведем несобранную часть к единице. Более того, при  $n = p^a$  все показатели степени кратны  $n$ , так как  $n^{(i)}$ ,  $i \leq p-1$ , есть биномиальный коэффициент, в числителе которого встречается сомножитель  $n$ , а сомножители знаменателя не превосходят  $p-1$ .

**Следствие 12.3.1.** *Если  $p$ -группа  $P$  имеет класс nilпотентности, меньший, чем  $p$ , то при  $n = p^a$*

$$(a_1 a_2 \dots a_r)^n = a_1^n a_2^n \dots a_r^n S_1^n S_2^n \dots S_t^n,$$

где  $S_1, S_2, \dots, S_t$  — элементы, принадлежащие коммутанту подгруппы, порожденной элементами  $a_1, a_2, \dots, a_r$ .

## 12.4. Регулярные $p$ -группы

Будем называть  $p$ -группу  $P$  регулярной, если для любых двух элементов  $a$  и  $b$  и любого  $n = p^a$  имеет место равенство

$$(ab)^n = a^n b^n S_1^n \dots S_t^n, \quad (12.4.1)$$

где  $S_1, \dots, S_t$  — подходящие элементы коммутанта группы, порожденной элементами  $a$  и  $b$ . Следующие утверждения легко получаются из этого определения и следствия из теоремы 12.3.1:

1) любая  $p$ -группа, класс nilпотентности которой меньше  $p$ , регулярна;

2) любая  $p$ -группа, порядок которой не больше  $p^p$ , регулярна;

3) группа  $P$  регулярна, если любая подгруппа, порожденная двумя ее элементами, регулярна;

4) любая подгруппа и фактор-группа регулярной группы регулярна.

Для любого  $p$  существует нерегулярная группа порядка  $p^{p+1}$ , а именно силовская подгруппа  $S^{(p)}$  симметрической группы  $S_{p^2}$  степени  $p^2$ . Эта группа порождается двумя элементами порядка  $p$  и содержит элементы порядка  $p^2$ . Как будет показано, такое явление невозможно в регулярной группе.

**Теорема 12.4.1.** В регулярной  $p$ -группе при  $n = p^\alpha$  имеет место тождество  $a^n b^n = (ab)^n S_1^n = (abS_2)^n$ , где  $S_1$  и  $S_2$  — элементы из коммутанта  $H_2(a, b)$  группы  $H(a, b)$ , порожденной элементами  $a$  и  $b$ .

Повторным применением этой теоремы получаем

**Следствие 12.4.1.** В регулярной  $p$ -группе при  $n = p^\alpha$  справедливы равенства  $a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r S_2)^n = (a_1 \dots a_r)^n S_1^n$ , где  $S_1, S_2 \in H_2(a_1, \dots, a_r)$ .

**Доказательство.** В абелевой группе теорема и следствие справедливы, причем  $S_1 = S_2 = 1$ . Для доказательства теоремы для произвольной подгруппы  $H$  применим индукцию. Предположим, что для любой собственной подгруппы группы  $H$  теорема и ее следствие верны. Заметим, что если группа  $H$  порождается элементами  $a_1, \dots, a_r$ , то ее коммутант  $H_2(a_1, \dots, a_r)$  является ее собственной подгруппой. Из тождества (12.4.1) сразу следует, что

$$a^n b^n = (ab)^n S_t^{-n} \dots S_1^{-n}. \quad (12.4.2)$$

По предположению индукции  $S_t^{-n} \dots S_1^{-n} = S^n$ , где  $S \in H_2$ . Но если  $H = H(a, b)$  — неабелева группа, то  $\{H_2, ab\}$  — собственная подгруппа группы  $H$ , откуда по индукции  $(ab)^n S^n = (abS_2)^n$ . Действительно, из теоремы Бернсайда о базисе следует, что если фактор-группа  $H/H_2$  циклическая, то группа  $H$  также циклическая. Таким образом, теорема справедлива для группы  $H$ , если эта теорема и ее следствие верны для любой собственной подгруппы группы  $H$ . Применяя теорему  $r - 1$  раз к произведению  $a_1^n a_2^n \dots a_r^n$ , получаем

$$a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r)^n S_1^n \dots S_{r-1}^n,$$

где  $S_1, \dots, S_{r-1} \in H_2$ . Применяя к подгруппе  $H_2$  следствие, получаем  $a_1^n a_2^n \dots a_r^n = (a_1 a_2 \dots a_r)^n S^n$ , а применяя теорему, получаем  $(a_1 a_2 \dots a_r)^n S^n = (a_1 a_2 \dots a_r S)^n$ .

**Теорема 12.4.2.** Конечная  $p$ -группа  $P$  регулярна тогда и только тогда, когда для любых элементов  $a, b \in P$  имеет место равенство

$$a^p b^p = (ab)^p S^p, \quad (12.4.3)$$

где  $S$  — элемент коммутанта группы, порожденной элементами  $a$  и  $b$ .

*Доказательство.* Условие (12.4.3), конечно, выполняется в регулярной  $p$ -группе; это частный случай теоремы 12.4.1. Докажем обратное утверждение: из условия (12.4.3) вытекает условие

$$a^n b^n = (ab)^n S_1^n, \quad n = p^a, \quad S_1 \in H_2(a, b). \quad (12.4.4)$$

Для этого сначала покажем по индукции справедливость равенств

$$a_1^p a_2^p \dots a_r^p = (a_1 a_2 \dots a_r)^p S_1^p = (a_1 a_2 \dots a_r S_2)^p, \quad (12.4.5)$$

где  $S_1, S_2 \in H_2(a_1, \dots, a_r)$ . Если  $H$  — абелева группа, то эти равенства, конечно, выполняются при  $S_1 = S_2 = 1$ . Если равенство (12.4.5) выполняется для любой собственной подгруппы группы  $H$ , то, применяя соотношение (12.4.3)  $r - 1$  раз, получаем  $a_1^p a_2^p \dots a_r^p = (a_1 a_2 \dots a_r)^p u_1^p \dots u_{r-1}^p$ , где  $u_1, \dots, u_{r-1} \in H_2$ . По предположению индукции  $u_1^p \dots u_{r-1}^p = S_1^p$ . Но элементы  $b = a_1 a_2 \dots a_r$  и  $S_1$  порождают собственную подгруппу группы  $H$ , откуда  $(a_1 a_2 \dots a_r)^p S_1^p = (a_1 \dots a_r S_2)^p$ , и тождество (12.4.5) установлено.

**Лемма 12.4.1.** *Если справедливо соотношение (12.4.3), то  $x^{-p} y^{-p} x^p y^p = S^p$ , где  $S$  — элемент коммутанта группы  $\{x, y\}$ .*

*Доказательство:*

$$\begin{aligned} x^p y^p &= (xy)^p S_1^p, \\ y^p x^p &= (yx)^p S_2^p, \end{aligned}$$

откуда

$$x^{-p} y^{-p} x^p y^p = S_2^{-p} (yx)^{-p} (xy)^p S_1^p,$$

но, кроме того,

$$(y, x)^{-p} (x, y)^p = (x^{-1} y^{-1} xy)^p S_3^p = (x, y)^p S_3^p,$$

следовательно,

$$x^{-p} y^{-p} x^p y^p = S_2^{-p} (x, y)^p S_3^p S_1^p = S^p.$$

Отсюда следует, что любой коммутатор элементов  $a_1^p, a_2^p, \dots, a_r^p$  является  $p$ -й степенью некоторого элемента коммутанта группы  $\{a_1, \dots, a_r\}$ .

Из (12.4.3) имеем

$$a^{p^2} b^{p^2} = (a^p b^p)^p S_1^p = [(ab)^p S_2^p]^p S_1^p = (ab)^{p^2} S_2^{p^2} S_3^p S_1^p, \quad (12.4.6)$$

где  $S_1$  — элемент коммутанта группы  $\{a^p, b^p\}$ , а  $S_3$  — элемент коммутанта группы  $\{(ab)^p, S_2^p\}$ . В силу леммы оба эти элемента

являются  $p$ -ми степенями элементов коммутанта группы  $\{a, b\}$ , откуда

$$a^{p^2}b^{p^2} = (ab)^{p^2}S_2^{p^2}S_4^{p^2}S_5^{p^2}, \quad (12.4.7)$$

т. е. соотношение (12.4.4) справедливо при  $n = p^2$ . Аналогичные рассуждения с применением леммы дают возможность доказать справедливость соотношения (12.4.4) для  $n = p^{\alpha+1}$ , в предположении, что оно верно для  $n = p^\alpha$ , т. е. закончить доказательство соотношения (12.4.4) по индукции.

**Теорема 12.4.3.** *Если  $P$  — регулярная  $p$ -группа и  $n = p^\alpha$ , то*

1) из  $(a^n, b) = 1$  следует  $(a, b)^n = 1$ , и обратно;

2) если  $(a^n, b) = 1$ , то  $(a, b^n) = 1$ ;

3) коммутатор  $S$ , содержащий элемент  $a$ , имеет порядок, не превосходящий порядка элемента  $a$  по модулю  $Z$ , где  $Z$  — центр группы  $P$ ;

4) порядок произведения  $a_1 a_2 \dots a_r$  не больше порядка каждого из элементов  $a_1, a_2, \dots, a_r$ .

*Доказательство.* В абелевой группе первые три свойства тривиальны, а выполнимость четвертого легко проверяется. Для доказательства по индукции предположим, что теорема верна для всех собственных подгрупп неабелевой группы  $P$ . Применяя тождество (12.4.4) к равенству

$$a^{-n}b^{-1}a^n b = (a^{-1})^n(b^{-1}ab)^n = (a^{-1}b^{-1}ab)^n s^n, \quad (12.4.8)$$

где  $s$  — элемент коммутанта группы  $K(a, b^{-1}ab) \subset H(a, b)$ , получаем

$$(a^n, b) = (a, b)^n s_1^n. \quad (12.4.9)$$

Если теперь  $(a^n, b) = 1$ , то порядок  $a$  в фактор-группе по центру  $Z^1$  группы  $H(a, b)$  не больше  $n$ , откуда в силу свойства (3) в собственной подгруппе  $K(a, b^{-1}ab)$  группы  $H(a, b)$  при  $u = a$  любой коммутатор из подгруппы  $K$  включает элемент  $a$ , и его порядок не больше  $n$ . Элемент  $s_1$  в равенстве (12.4.9) равен произведению коммутаторов из подгруппы  $K$ , и в силу свойства (4) для подгруппы  $K$  порядок элемента  $s_1$  не больше  $n$ . Таким образом, если  $(a^n, b) = 1$ , то в (12.4.9)  $s_1^n = 1$ , откуда  $(a, b)^n = 1$ . Обратно, если  $(a, b)^n = 1$ ,

то в подгруппе  $K = K(a, a^{-1}b^{-1}ab) = K(u)$ , где  $u = (a, b)$ , порядок элемента  $u$  в  $P/Z^1$  ( $Z$  — центр подгруппы  $K$ ) не превосходит  $n$ , и в каждом коммутаторе встречается элемент  $u$ . Тогда в силу свойства (3) подгруппы  $K$  все коммутаторы этой подгруппы имеют порядок, не превосходящий  $n$ , откуда, используя свойство (4)

<sup>1)</sup> Здесь и дальше под порядком элемента  $a \in P$  в фактор-группе  $P/Z$  следует, конечно, понимать порядок класса смежности  $P$  по  $Z$ , содержащего  $a$ . — Прим. ред.

коммутанта  $K_2$  группы  $K$ , получаем, что порядок элемента  $s_1$  не больше  $n$ .

Таким образом, из условия  $(a, b)^n = 1$  следует, что  $s_1^n = 1$ , откуда  $(a^n, b) = 1$ . Этим установлено свойство (1) группы  $P$ , из которого сразу следует свойство (2). Свойство (3) получается повторным применением свойства (1). Если порядок элемента  $u$  в  $P/Z$ , где  $Z$  — центр группы  $P$ , равен  $n$ , то тем более  $(u^n, v) = 1$ , откуда  $(u, v)^n = 1$ . Полагая  $x = (u, v)$ , получаем  $x^n = 1$ , откуда  $(x, y)^n = 1$ .

Осталось доказать свойство (4) для группы  $P$ . Если  $a^n = 1$ ,  $b^n = 1$ , то в силу свойства (3) порядок любого коммутатора, в котором встречается элемент  $a$  или  $b$ , не превосходит  $n$ . Следовательно, элемент  $S_1$  из равенства (12.4.4) равен произведению коммутаторов, порядки которых не превосходят  $n$ ; применяя свойство (4) для собственной подгруппы  $P'$ , получаем, что порядок элемента  $S_1$  не больше, чем  $n$ . Следовательно,  $S_1^n = 1$ , и поэтому  $(ab)^n = 1$ . Таким образом, порядок произведения двух сомножителей не превосходит порядка каждого из сомножителей, откуда повторным применением этого свойства легко получить аналогичное утверждение для  $r$  сомножителей.

**Теорема 12.4.4.** *Если  $a^n = b^n$  при  $n = p^a$ , то  $(ab^{-1})^n = 1$ , и обратно.*

**Доказательство.** Согласно свойству (3) из теоремы 12.4.3, порядки всех коммутаторов группы  $H(a, b)$  не превосходят  $n$ . Следовательно, из равенств  $1 = a^n b^{-n} = (ab^{-1})^n s_1^n$  имеем  $s_1^n = 1$ , откуда  $(ab^{-1})^n = 1$ . Обратно, пусть  $a^n b^{-n} = (ab^{-1})^n s_1^n$ ,  $(ab^{-1})^n = 1$  и  $H(a, b) = H(a, ab^{-1})$ . Тогда из свойства (3) для элемента  $u = ab^{-1}$  получаем  $s_1^n = 1$ , откуда  $a^n = b^n$ .

**Теорема 12.4.5.** *В регулярной  $p$ -группе  $P$  элементы вида  $a^{p^a}$ , где  $a \in P$ , образуют характеристическую подгруппу  $C^\alpha(P)$ , а элементы, порядки которых не превышают  $p^a$ , — характеристическую подгруппу  $C_\alpha(P)$ .*

**Доказательство.** При  $n = p^a$  соотношение  $a^n b^n = (abS_2)^n$  теоремы 12.4.1. показывает, что множество  $C^\alpha(P)$  является подгруппой, которая, конечно, характеристична и даже вполне характеристична. Свойство (4) теоремы 12.4.3 говорит о том, что элементы, порядки которых не больше  $p^a$ , образуют подгруппу, являющуюся вполне характеристической.

## 12.5. Некоторые специальные $p$ -группы. Группы Гамильтона

**Теорема 12.5.1.** *Группы порядка  $p^n$ , обладающие циклической подгруппой индекса  $p$ , могут быть только следующих типов:*

*Абелевы,*

$n \geq 1$ , циклические:

$$1) a^{pn} = 1,$$

$n \geq 2$ :

$$2) a^{pn-1} = 1, b^p = 1, ba = ab.$$

*Неабелевы,*

$p$  нечетно,  $n \geq 3$ :

$$3) a^{pn-1} = 1, b^p = 1, ba = a^{1+pn-2}b,$$

$p = 2, n \geq 3$ :

4) обобщенная группа кватернионов:

$$a^{2^n-1} = 1, b^2 = a^{2^n-2}, ba = a^{-1}b;$$

$p = 2, n \geq 3$ :

5) группа диэдра;

$$a^{2^n-1} = 1, b^2 = 1, ba = a^{-1}b,$$

$p = 2, n \geq 4$ :

$$6) a^{2^n-1} = 1, b^2 = 1, ba = a^{1+2^n-2}b,$$

$p = 2, n \geq 4$ :

$$7) a^{2^n-1} = 1, b^2 = 1, ba = a^{-1+2^n-2}b.$$

*Доказательство.* Абелева группа порядка  $p^n$ , обладающая элементом порядка  $p^{n-1}$ , содержит базисный элемент порядка  $p^{n-1}$  или  $p^n$ . Следовательно, теорема доказана для упомянутых абелевых групп.

Рассмотрим теперь неабелевые группы порядка  $p^n$  с элементом порядка  $p^{n-1}$ . Пусть сначала число  $p$  нечетно. Если  $a^{p^{n-1}} = 1$ , то подгруппа  $\{a\}$ , имеющая индекс  $p$ , инвариантна, откуда при  $b \notin \{a\}$  имеем  $bab^{-1} = a^r$ , где  $r \not\equiv 1 \pmod{p^{n-1}}$ , так как рассматриваемая группа неабелева. Индукцией по  $i$  легко установить, что  $b^i ab^{-i} = a^{ri}$ , так как  $(bab^{-1})^j = ba^j b^{-1} = a^{rj}$  при любом  $j$ , и; в частности, для  $j = r$  имеем  $b^2 ab^{-2} = b(bab^{-1})b^{-1} = ba^r b^{-1} = a^{r^2}$ . Общий случай  $b^i ab^{-i} = a^{ri}$  легко получить при помощи индукции. Так как  $b^p \in \{a\}$ , имеем  $b^p ab^{-p} = a$ , откуда  $r^p \equiv 1 \pmod{p^{n-1}}$ . Так как  $p$  — нечетное число, отсюда следует, что  $r \equiv 1 + kp^{n-2} \pmod{p^{n-1}}$ , где  $k \not\equiv 0 \pmod{p}$ , так как  $r \not\equiv 1 \pmod{p^{n-1}}$ . Положим  $b_1 = b^i$ , где  $i$  определяется из сравнения  $ik \equiv 1 \pmod{p}$ . Тогда  $r^i \equiv (1 + kp^{n-2})^i \equiv 1 + ikp^{n-2} \equiv 1 + p^{n-2} \pmod{p^{n-1}}$ . Следовательно,  $b_1 ab_1^{-1} = b^i ab^{-i} = a^{ri} = a^{1+p^{n-2}}$ . Обозначим  $1 + p^{n-2}$  через  $h$ . Тогда  $(a^j b_1)^2 = a^j b_1 a^j b_1^{-1} b_1^2 = a^{j(1+h)} b_1^2$ , откуда индукцией выводим, что  $(a^j b_1)^t = a^{jt} b_1^t$ , где  $T = 1 + h + \dots + h^{t-1}$ . При

$t = p$  имеем  $1 + h + \dots + h^{p-1} \equiv p + p^{n-2}[1 + 2 + \dots + (p-1)] \equiv p + p^{n-1}(p-1)/2 \equiv p \pmod{p^{n-1}}$ , так как  $p$  нечетно. Таким образом,  $(a^j b_1)^p = a^{jp} b_1^p$ . Это соотношение можно было бы вывести также из собирательной формулы. Теперь  $b_1^p = a^u \in \{a\}$ , где  $u = pv$ , так как порядок элемента  $b_1$  не равен  $p^n$  и так как группа не циклическа. Если мы положим  $b_2 = a^{-v} b_1$ , то  $b_2^p = (a^{-v} b_1)^p = a^{-vp} b_1^p = a^{-pv} a^{pv} = 1$  и  $b_2 a b_2^{-1} = a^{-v} b_1 a b_1^{-1} a^v = a^{-v} a^{1+p^{n-2}} a^v = a^{1+p^{n-2}}$ . Таким образом, элементы  $a$  и  $b_2$  удовлетворяют отношениям теоремы в случае 3 для неабелевой группы с нечетным  $p$ .

Пусть теперь  $p = 2$ . Найдем неабелевые группы порядка  $2^n$ , содержащие элемент порядка  $2^{n-1}$ . Пусть  $a^{2^{n-1}} = 1$ ,  $b \notin \{a\}$ . Тогда  $bab^{-1} = a^r$ , где  $r^2 \equiv 1 \pmod{2^{n-1}}$ ,  $r \not\equiv 1 \pmod{2^{n-1}}$ . Это дает три значения  $r \pmod{2^{n-1}}$ :  $r = -1$ ,  $r = 1 + 2^{n-2}$ ,  $r = -1 + 2^{n-2}$ . Пусть  $b^2 = a^w \in \{a\}$ . Тогда, так как  $b(b^2)b^{-1} = b^2$ , мы имеем  $a^{wr} = a^w$ , следовательно, число  $w$  подчинено условию  $wr \equiv w \pmod{2^{n-1}}$ . Для  $r = -1$  находим  $-w \equiv w \pmod{2^{n-1}}$ , откуда  $a^w = 1$  или  $a^w = a^{2^{n-2}}$ . Таким образом, случаю  $r = -1$  соответствует обобщенная группа кватернионов или группа диэдра (типы 4 и 5) соответственно. При  $n = 3$ , как мы выяснили в § 4.4, это единственны группы.

Пусть теперь  $n \geq 4$  и  $ba = a^r b$ , где  $r = 1 + 2^{n-2}$ . Для элемента  $b^2 = a^w$  условие  $wr \equiv w \pmod{2^{n-2}}$  означает, что  $2^{n-2}w \equiv 0 \pmod{2^{n-1}}$ , т. е. что  $w = 2w_1$  — четное число. Определим число  $j$  из сравнения  $j(1 + 2^{n-3}) + w_1 \equiv 0 \pmod{2^{n-2}}$ . Тогда для  $b_1 = a^j b$  имеем  $b_1^2 = a^j(ba^j)b = a^{j(2+2^{n-2})}b^2 = a^{2[j(1+2^{n-3})+w_1]} = a^{2^{n-1}} = 1$ . Следовательно,  $b_1 a = a^{1+2^{n-2}} b_1$ , т. е. элементы  $a$  и  $b_1$  удовлетворяют соотношениям типа 6. Наконец, если  $n \geq 4$ ,  $ba = a^r b$ , где  $r = -1 + 2^{n-2}$ , то для элемента  $b^2 = a^w$  условие  $w \equiv rw \pmod{2^{n-1}}$  означает, что  $(-2 + 2^{n-2})w \equiv 0 \pmod{2^{n-1}}$ , откуда  $w \equiv 0 \pmod{2^{n-2}}$ . Таким образом,  $b^2 = 1$  или  $b^2 = a^{2^{n-2}}$ . Если  $b^2 = a^{2^{n-2}}$ , то, полагая  $b_1 = ab$ , получим  $b_1^2 = a(ba)b = a(a^{-1+2^{n-2}})b^2 = a^{2^{n-2}}a^{2^{n-2}} = 1$ . Таким образом, элементы  $a$  и  $b$  или  $a$  и  $b_1$  удовлетворяют требованиям типа 7.

То, что соотношения теоремы 12.5.1 определяют группы, легко проверяется при помощи теоремы 6.5.1 во всех случаях, кроме случая обобщенной группы кватернионов. В случае же обобщенной группы кватернионов это проверяется или непосредственно, или же с помощью теоремы 15.3.1.

**ТЕОРЕМА 12.5.2.**  *$p$ -группа, содержащая только одну подгруппу порядка  $p$ , является циклической или обобщенной группой кватернионов.*

**Доказательство.** Пусть  $P$  — группа порядка  $p^n$ , содержащая только одну подгруппу порядка  $p$ . Докажем индукцией по  $n$ , что  $P$  или циклическая группа, или обобщенная группа кватернионов. При  $n=1$  это очевидно. Пусть сначала число  $p$  нечетно. Тогда по предположению индукции подгруппа  $P_1$  индекса  $p$  циклическая, откуда в силу теоремы 12.5.1 следует, что  $P$  — группа одного из типов 1, 2 или 3 для нечетного  $p$ , но группы типов 2 и 3 содержат больше одной подгруппы порядка  $p$ . Следовательно,  $P$  — циклическая группа. Если при  $p=2$  группа  $P$  содержит циклическую подгруппу  $P_1$  индекса 2, то, согласно теореме 12.5.1, группа  $P$  принадлежит одному из типов 1—7 при  $p=2$ , причем группы каждого из этих типов, кроме циклической группы и обобщенной группы кватернионов, содержат больше одной подгруппы порядка 2. Таким образом,  $P$  — или циклическая группа, или обобщенная группа кватернионов.

Осталось рассмотреть случай, когда по предположению индукции каждая подгруппа  $P_1$  индекса 2 является обобщенной группой кватернионов. Покажем, что такого положения быть не может. Здесь  $n \geq 4$ . Пусть сперва  $n=4$  и  $Q$  — обобщенная группа кватернионов индекса 2, а  $c$  — элемент, не принадлежащий  $Q$ . Подгруппа  $Q$  определяется отношениями  $a^4=b^4=1$ ,  $a^2=b^2$ ,  $ba=a^{-1}b$ , а  $P=Q+Qc$ . Элемент  $c$ , порядок которого равен степени числа 2, должен трансформировать в себя по меньшей мере одну из трех подгрупп порядка 4 группы  $Q$ :  $\{a\}$ ,  $\{b\}$  и  $\{ab\}$ . Не ограничивая общности, можно считать, что этой подгруппой является  $\{a\}$ . Тогда  $c^{-1}ac=a$  или  $c^{-1}ac=a^{-1}$ . Если  $c^{-1}ac=a$ , то  $\{a, c\}$  — абелева подгруппа индекса 2, что противоречит условию. Если же  $c^{-1}ac=a^{-1}$ , то  $(cb)^{-1}a(cb)=a$ , и  $\{a, cb\}$  — абелева подгруппа индекса 2, что опять противоречит условию. Таким образом, случай  $n=4$  отпадает.

Пусть, наконец,  $n \geq 5$  и  $P_1$  — подгруппа индекса 2, являющаяся обобщенной группой кватернионов. Тогда  $P_1$  определяется отношениями  $a^{2^{n-2}}=1$ ,  $b^2=a^{2^{n-3}}$ ,  $ba=a^{-1}b$ , а  $P=P_1+P_1c$ . Пусть  $\{a\}$  — единственная подгруппа группы  $P_1$  порядка  $2^{n-2}$ , причем все элементы группы  $P_1$ , не принадлежащие подгруппе  $\{a\}$ , имеют порядок 4. Таким образом,  $c^{-1}ac=a^r$  и  $c^2=a^ib$  или  $c^2=a^i$ . Если  $c^2=a^ib$ , то  $c^{-2}ac^2=a^{-1}$  и  $r^2 \equiv -1 \pmod{2^{n-2}}$ , что невозможно. Если  $c^2=a^i$ , то  $\{a, c\}$  — подгруппа индекса 2, являющаяся по предположению обобщенной группой кватернионов. Тогда  $c^{-1}ac=a^{-1}$  и  $(cb)^{-1}a(cb)=a$ , т. е.  $\{cb, a\}$  — абелева подгруппа индекса 2, что противоречит условию. Этим завершается доказательство теоремы 12.5.2.

**Теорема 12.5.3.** Группа порядка  $p^n$ , содержащая только одну подгруппу порядка  $p^m$ , где  $1 < m < n$ , — циклическая.

*Доказательство.* Если  $m = n - 1$ , то группа  $P$  порядка  $p^n$  с единственной подгруппой порядка  $p^{n-1}$  порождается любым элементом  $x$ , не принадлежащим этой подгруппе, так как подгруппа  $\{x\}$  не содержится в этой единственной максимальной подгруппе, откуда  $\{x\} = P$ , т. е.  $P$  — циклическая группа. Этим теорема доказана для наименьшего показателя степени  $n = 3$ , удовлетворяющего условиям теоремы, и для произвольного  $n$ , если  $m = n - 1$ . Продолжим доказательство индукцией по  $n$ . При  $m = n - 1$  теорема уже доказана. Поэтому считаем, что  $m < n - 1$ .

Пусть  $P_1$  — единственная подгруппа порядка  $p^m$ , и пусть  $P_1$  содержится в максимальной подгруппе  $A$  порядка  $p^{n-1}$ . Так как  $1 < m < n - 1$ , то по индукции группа  $A$  — циклическая, и поэтому  $P_1$ , как ее подгруппа, — также циклическая группа. Любая подгруппа порядка  $p$  или  $p^2$  содержится в подгруппе порядка  $p^m$ , так как  $m \geq 2$ , а потому содержится и в  $P_1$ . Но подгруппа  $P_1$ , являясь циклической, содержит единственную подгруппу порядка  $p$  и единственную подгруппу порядка  $p^2$ . Таким образом, группа  $P$  содержит единственную подгруппу порядка  $p$  и единственную подгруппу порядка  $p^2$ . По теореме 12.5.2,  $P$  — циклическая группа или обобщенная группа кватернионов. Но последняя содержит больше одной подгруппы порядка 4. Следовательно,  $P$  — циклическая группа.

То, что любая подгруппа абелевой группы инвариантна, очевидно. Однако группа кватернионов представляет собой пример неабелевой группы, в которой любая подгруппа инвариантна. Будем называть группу  $H$  группой Гамильтона, если она неабелева и содержит только инвариантные подгруппы.

**Теорема 12.5.4.** *Группа Гамильтона представима как прямое произведение группы кватернионов, абелевой группы, каждый элемент которой конечного нечетного порядка, и абелевой группы показателя два.*

*Доказательство.* Пусть  $a$  и  $b$  — два элемента из группы Гамильтона  $H$ . Тогда  $c = (a, b) = (a^{-1}b^{-1}a)b = b^s = a^{-1}(b^{-1}ab) = a'$ , так как подгруппы  $\{a\}$  и  $\{b\}$  инвариантны. Заметим, что отсюда следует перестановочность коммутатора  $c$  с элементами  $a$  и  $b$ . В силу тождеств (10.2.1)

$$(a^2, b) = (a, b)(a, a) \quad (a, b) = (a, b)(c, a)(a, b) = (a, b)^2,$$

а по индукции отсюда легко получить, что

$$(a^l, b) = (a, b)^l = c^l.$$

Если элементы  $a$  и  $b$  не перестановочны, то  $c = a' \neq 1$  и, полагая  $l = r$  или  $l = -r$  (в зависимости от того, какое из этих чисел положительно), получаем, что коммутатор  $(a^l, b)$  равен

или  $(c, b)$ , или  $(c^{-1}, b)$ . В обоих случаях он равен 1, так как элементы  $c$  и  $b$  перестановочны:  $(a^i, b) = 1 = (a, b)^i = c^i$ . Следовательно,  $c^i = 1$ , откуда  $a^{ri} = 1$ ,  $b^{si} = 1$ . Поэтому два неперестановочных элемента группы  $H$  имеют конечные порядки. Если элемент  $x$  из  $H$  перестановчен с  $a$  и  $b$ , то элемент  $xa$  не перестановчен с  $b$ ; поэтому  $xa$ , а значит, и  $x$  имеют конечный порядок. Таким образом, порядок любого элемента группы  $H$  конечен.

Пусть  $a$  и  $b$  — неперестановочные элементы из  $H$ , причем  $a^N = 1$ ,  $b^M = 1$ , где  $N$  и  $M$  — минимальные из чисел, для которых эти условия выполняются. Если  $p$  — произвольный простой делитель числа  $N$ , то в силу минимальности  $N$  элемент  $a^p$  перестановчен с  $b$ , т. е.  $(a^p, b) = (a, b)^p = 1$ . Аналогичное утверждение справедливо для любого простого числа, которое делит  $M$ . Так как  $c = (a, b) \neq 1$ , существует только одно простое число, которое делит  $M$  и  $N$ , откуда  $M = p^m$ ,  $N = p^n$ . Таким образом,  $a^{p^n} = 1$ ,  $b^{p^m} = 1$ ,  $c = (a, b)$ ,  $c^p = 1$ , где в силу симметрии можно считать, что  $n \geq m$ . Далее, так как  $c \in \{a\}$  и  $c \in \{b\}$ , то  $c = a^{jp^{n-1}} = b^{kp^{m-1}}$ , где  $j, k \not\equiv 0 \pmod{p}$ .

В группе  $\{a, b\}$  группа  $\{c\}$  является коммутантом и, кроме того, содержится в центре. Следовательно, здесь все коммутаторы, веса которых больше двух, равны единице. Выведем по индукции формулу

$$(ab)^i = a^i b^i (b, a)^{i(i-1)/2}.$$

При  $i = 1$  она верна. Далее,

$$\begin{aligned} (ab)^{i+1} &= (ab)^i ab = a^i b^i (b, a)^{i(i-1)/2} ab = \\ &= a^i b^i ab (b, a)^{i(i-1)/2} = \\ &= a^i ab^i (b^i, a) b (b, a)^{i(i-1)/2} = \\ &= a^{i+1} b^i (b, a)^i b (b, a)^{i(i-1)/2} = \\ &= a^{i+1} b^{i+1} (b, a)^{i(i-1)/2}. \end{aligned}$$

Доказанная формула справедлива для любой группы  $\{a, b\}$ , при условии, что коммутатор  $(a, b)$  содержится в ее центре. Эта формула также вытекает из собирательной формулы.

Если  $b_1 = a^u b^k$ , где  $u = -jp^{n-m}$ , то  $\{a, b_1\} = \{a, b\}$ , откуда следует, что элемент  $b_1$  не перестановчен с  $a$ . Поэтому в силу выбора элемента  $b$  порядок  $b_1$  не меньше порядка элемента  $b$ . Только что установленная формула дает

$$\begin{aligned} b_1^p &= (a^u b^k)^p = a^{up} b^{kp} (b^k, a^u)^{p(p-1)/2} = \\ &= a^{pu} b^{kp} c^{-ukp(p-1)/2}, \end{aligned}$$

откуда  $b_1^{p^{m-1}} = a^{-jp^{n-1}} b^{kp^{m-1}} c^{jkp^{n-1}(p-1)/2} = c^{jkp^{n-1}(p-1)/2}$ . Здесь  $b_1^{p^{m-1}} \neq 1$ , но так как  $c^p = 1$ , последняя формула может выполняться только при  $p = 2$ ,  $n = 2$ . Таким образом, элементы  $a$  и  $b$  связаны соотношениями  $a^2 = b^2 = a^{-1}b^{-1}ab = c$ ,  $c^2 = 1$ , т. е.  $\{a, b\}$  — группа кватернионов. Итак, любая неабелева подгруппа группы  $H$  содержит группу кватернионов.

Покажем теперь, что группа  $H$  является объединением группы кватернионов  $Q$ , заданной отношениями  $a^4 = b^4 = 1$ ,  $a^2 = b^2$ ,  $ba = a^{-1}b$ , и ее централизатора  $Z$ . Если элемент  $x$  из  $H$  не перестановочен с элементом  $a$ , то  $x^{-1}ax = a^{-1}$  и элемент  $xb$  перестановочен с  $a$ . Аналогично, если элемент  $x$  (или  $xb$ ) не перестановочен с  $b$ , то элемент  $xa$  (или  $xba$ ) перестановочен с  $b$ . Следовательно, один из элементов  $x$ ,  $xb$ ,  $xa$ ,  $xba$  содержится в подгруппе  $Z$ . Поэтому  $H = Q \cup Z = QZ$ . Покажем, что подгруппа  $Z$  не содержит элементов порядка 4. Действительно, если  $x^4 = 1$ ,  $x \in Z$ , то  $(a, bx) \neq 1$ . Но так как  $(bx)^4 = 1$ , имеем  $a^{-1}(bx)a = (bx)^{-1}$ , откуда  $a^{-1}bax = b^{-1}x^{-1}$ . Следовательно,  $x^2 = 1$ . Так как подгруппа  $Z$  не содержит элементов порядка 4, она не содержит группу кватернионов, откуда следует, что  $Z$  — абелева группа, причем  $Z \cap Q = \{a^2\}$ . Согласно лемме Цорна, существует максимальная подгруппа  $Z_1$  группы  $Z$ , не содержащая  $a^2$ . Теперь легко убедиться в том, что  $Z = Z_1 + Z_1a^2$ ,  $H = Q \times Z_1$ . Подгруппа  $Z_1$  представима как прямое произведение абелевой группы  $U$ , состоящей из элементов нечетных порядков, и абелевой группы  $V$  показателя 2, так как  $Z_1$  не содержит элементов порядка 4. Таким образом,  $H = Q \times U \times V$ .

Обратно, группа  $Q \times U \times V$  является группой Гамильтона, причем подгруппа  $Q$  неабелева. Достаточно показать, что любая циклическая подгруппа  $\{quv\}$  инвариантна. Подгруппы  $U$  и  $V$  лежат в центре  $Q \times U \times V$ . Поэтому нам нужно только показать, что элементы  $a$  и  $b$  трансформируют подгруппу  $\{quv\}$  в себя. Действительно,  $a^{-1}(quv)a = q^iuv$ , где  $i = 1$  или 3. Порядок  $n$  элемента  $u$  нечетен, а порядок элемента  $v$  равен 2. Следовательно, сравнения  $r \equiv i \pmod{4}$  и  $r \equiv 1 \pmod{n}$  разрешимы и  $a^{-1}(quv)a = (quv)^r$ . Теорема доказана.

## Г л а в а 13

### ПРОДОЛЖЕНИЕ ТЕОРИИ АБЕЛЕВЫХ ГРУПП

#### 13.1. Аддитивные группы. Группы по модулю 1

Групповую операцию произвольной группы можно считать сложением. Общепринято записывать абелевы группы аддитивно, что особенно удобно в случае групп с операторами. Кроме того, ряд групп возникает естественным образом как группы сложения общезвестных систем объектов. Две из них мы здесь рассмотрим. Это аддитивная группа рациональных чисел, которую мы обозначим через  $r_+$ , и аддитивная группа действительных чисел, которую мы обозначим через  $R_+$ .

В случае аддитивной записи групповой операции мы соответственно изменим терминологию, т. е. будем говорить о суммах элементов, декартовых и прямых суммах и т. д.

Циклическая группа в аддитивной записи состоит из всех целых кратных  $na$  образующего элемента  $a$ . Группы  $r_+$  и  $R_+$  обе без кручения, так как из равенства  $na = 0$  следует, что  $a = 0$ . В бесконечной циклической группе, порожденной элементом  $a$ , нет элемента  $x$ , для которого  $2x = a$ . Так как для любого элемента  $a$  из  $r_+$  элемент  $x$ , удовлетворяющий уравнению  $2x = a$ , существует, то группа  $r_+$  не циклическа. Однако по своим свойствам она близка к циклической группе. Любое конечное множество элементов группы  $r_+$  порождает циклическую группу. Именно это свойство мы будем иметь в виду, говоря, что группа  $r_+$  локально циклическая или что это группа ранга один. Вообще будем говорить, что абелева группа имеет ранг  $k$ , если любая подгруппа, порожденная конечным числом элементов, обладает также системой образующих не более, чем из  $k$  элементов, причем некоторая подгруппа, порожденная конечным множеством элементов, обладает минимальной системой образующих точно из  $k$  элементов.

**Теорема 13.1.1.** Аддитивная группа рациональных чисел  $r_+$  локально циклическа.

**Доказательство.** Рассмотрим подгруппу группы  $r_+$ , порожденную конечным множеством элементов  $a_1/b_1, \dots, a_t/b_t$ . Ее элементами являются числа вида  $m_1a_1/b_1 + \dots + m_ta_t/b_t$ , где  $m_1, \dots, m_t$  — любые целые числа. Такое число можно представить в виде  $(m_1a_1b_2\dots b_t + \dots + m_ta_tb_1\dots b_{t-1})/b_1b_2\dots b_t$ . Легко про-

верить, что числители образуют аддитивную подгруппу аддитивной группы целых чисел, которая циклична. Следовательно, рассматриваемые числители образуют циклическую подгруппу, состоящую из всех целых кратных некоторого целого числа  $w$ . Таким образом, наша подгруппа состоит из всех чисел вида  $nw/b_1b_2\dots b_t$ , т. е. является циклической группой.

В группе  $R_+$  целые числа образуют подгруппу, которая, как и все подгруппы абелевой группы, инвариантна. В соответствующей фактор-группе все числа, отличающиеся друг от друга на целое число, отождествлены. Поэтому мы называем эту фактор-группу группой  $R_+ \pmod{1}$ . Аналогично группе  $r_+$  соответствует фактор-группа  $r_+ \pmod{1}$ , являющаяся, конечно, подгруппой группы  $R_+ \pmod{1}$ .

Группа  $r_+ \pmod{1}$  периодична, так как для рационального числа  $a/b$  ( $a$  и  $b$  — целые) имеем  $b(a/b) \equiv 0 \pmod{1}$ . По теореме 3.2.3 группа  $r_+ \pmod{1}$  представима как прямая сумма своих силовских подгрупп  $S(p)$ , которые мы будем обозначать  $Z(p^\infty)$ . Подгруппа  $Z(p^\infty)$  порождается бесконечным множеством  $1/p, 1/p^2, \dots, 1/p^t, \dots \pmod{1}$ . Элемент из  $Z(p^\infty)$  имеет вид  $m/p^n$ , где  $(m, p) = 1$ . Он порождает циклическую группу  $\{1/p^n\}$ . Следовательно, произвольная подгруппа группы  $Z(p^\infty)$  или конечна, или содержит бесконечно много элементов множества  $1/p, 1/p^2, \dots, 1/p^t, \dots \pmod{1}$  и потому совпадает со всей группой  $Z(p^\infty)$ . Таким образом,  $Z(p^\infty)$  — бесконечная группа; все собственные подгруппы которой — конечные циклические группы.

## 13.2. Характеры абелевых групп. Двойственность абелевых групп

Пусть  $A$  — произвольная абелева группа. Характером  $\chi$  группы  $A$  называется гомоморфизм этой группы в группу  $R_+ \pmod{1}$ . При этом

$$\chi(a_1) + \chi(a_2) = \chi(a_1 + a_2) \quad \text{для всех } a_1, a_2 \in A. \quad (13.2.1)$$

Здесь сложение  $a_1 + a_2$  — это сложение в группе  $A$ , а сложение значений характеров  $\chi(a_1) + \chi(a_2)$  — это сложение в группе  $R_+ \pmod{1}$ . Определим также сложение характеров. Если  $\chi_1$  и  $\chi_2$  — два характера группы  $A$ , то, по определению,

$$\chi_3(a) = \chi_1(a) + \chi_2(a) \quad \text{для всех } a \in A. \quad (13.2.2)$$

Тогда отображение  $\chi_3$  также является характером группы  $A$ , так как

$$\begin{aligned} \chi_3(a_1 + a_2) &= \chi_1(a_1 + a_2) + \chi_2(a_1 + a_2) = \\ &= \chi_1(a_1) + \chi_1(a_2) + \chi_2(a_1) + \chi_2(a_2) = \\ &= \chi_1(a_1) + \chi_2(a_1) + \chi_1(a_2) + \chi_2(a_2) = \\ &= \chi_3(a_1) + \chi_3(a_2). \end{aligned} \quad (13.2.3)$$

Характер  $\chi_3$  называется суммой характеров  $\chi_1$  и  $\chi_2$ :

$$\chi_3 = \chi_1 + \chi_2. \quad (13.2.4)$$

Легко проверить, что при таком определении сложения характеров они образуют аддитивную группу  $A^*$ , нулевым элементом которой является характер, отображающий все элементы группы  $A$  в нуль.

**Теорема 13.2.1.** Группа характеров  $A^*$  конечной абелевой группы  $A$  изоморфна группе  $A$ .

**Доказательство.** Для любого гомоморфизма справедливо равенство  $\chi(0) = 0$ . Следовательно, для элемента  $a$  конечного порядка  $m$  мы имеем  $m\chi(a) = \chi(ma) = \chi(0) = 0$ . Поэтому число  $\chi(a)$  может принимать только одно из значений  $0, 1/m, \dots, (m-1)/m$ . Очевидно, что для конечной абелевой группы характер полностью определяется его действием на базисные элементы. Пусть  $a_i (i = 1, \dots, r)$  — базис группы  $A$ , причем порядок элемента  $a_i$  равен  $n_i$ , а порядок группы  $A$  равен  $n = n_1 n_2 \dots n_r$ . Так как  $\chi(a_i)$  может принимать не более  $n_i$  значений, существует не более  $n = n_1 n_2 \dots n_r$  различных характеров группы  $A$ . Однако легко заметить, что их ровно  $n$ . Действительно, если положить  $\chi_i(a_i) = 1/n_i$  и  $\chi_i(a_j) = 0$ , если  $i \neq j$ , то можно показать, что для любого  $i = 1, \dots, r$  этим определяется характер и что соответствие  $a_i \mapsto \chi_i$  является изоморфизмом между группами  $A$  и  $A^*$ . Заметим, однако, что изоморфизм между  $A$  и  $A^*$  не определен однозначно, а зависит от выбора базиса группы  $A$ .

Следующая теорема справедлива для абелевой группы произвольного порядка, конечного или бесконечного.

**Теорема 13.2.2.** Пусть  $H$  — подгруппа абелевой группы  $A$ . Тогда группа тех характеров группы  $A$ , для которых  $\chi(h) = 0$  при любом  $h \in H$ , изоморфна группе характеров фактор-группы  $A/H$ .

**Доказательство.** Если характер отображает в нуль любой элемент из  $H$ , то он переводит все элементы из смежного класса  $H+x$  в одно и то же число. Сопоставляя этому смежному классу это общее для всех его элементов значение из  $R_+ \pmod{1}$ , мы получим, как легко видеть, характер фактор-группы  $A/H$ . Обратно, произведение двух гомоморфизмов  $A \rightarrow A/H$  и  $A/H \rightarrow R_+ \pmod{1}$  дает характер группы  $A$ , при котором произвольный элемент из подгруппы  $H$  отображается сперва в нуль фактор-группы  $A/H$ , а затем в нуль группы  $R_+ \pmod{1}$ .

**Следствие 13.2.1.** Если  $a$  — отличный от нуля элемент конечной абелевой группы  $A$ , то существует такой характер  $\chi$  группы  $A$ , что  $\chi(a) \neq 0$ .

Действительно, если бы это было не так, то любой характер группы  $A$  был бы характером фактор-группы  $A/\{a\}$  и, согла-

сно теореме 13.2.1, группа  $A^*$  была бы изоморфна и группе  $A$ , и группе  $A/\{a\}$ , что невозможно, так как порядок фактор-группы  $A/\{a\}$  меньше порядка группы  $A$ .

Двойственностью между группами  $A$  и  $B$  называется взаимно однозначное соответствие  $H \rightleftarrows K$  между подгруппами  $H$  группы  $A$  и подгруппами  $K$  группы  $B$ , которое меняет знак включения на обратный, т. е. если  $H_1 \rightleftarrows K_1$  и  $H_2 \rightleftarrows K_2$ , то из включения  $H_1 \supset H_2$  следует включение  $K_1 \subset K_2$ , и наоборот. Существует естественная двойственность между конечной абелевой группой  $A$  и ее группой характеров  $A^*$ , как показывает следующая теорема.

**Теорема 13.2.3.** *Междуду конечной абелевой группой  $A$  и группой ее характеров  $A^*$  существует следующая двойственность  $H \rightleftarrows K$ : данной подгруппе  $H$  группы  $A$  соответствует подгруппа  $K$  группы  $A^*$ , состоящая из всех характеров, для которых  $\chi(h) = 0$  для любого элемента  $h \in H$ ; данной подгруппе  $K$  группы  $A^*$  соответствует подгруппа  $H$ , состоящая из всех элементов группы  $A$ , для которых  $\chi(h) = 0$  для любого характера  $\chi \in K$ . Группа  $A$  двойственна себе.*

**Доказательство.** Каждой подгруппе  $H$  группы  $A$  поставим в соответствие подгруппу  $H^*$  группы  $A^*$ , состоящую из всех таких характеров  $\chi$ , что  $\chi(h) = 0$  для любого элемента  $h \in H$ . Если  $H_1 \neq H_2$  — две различные подгруппы группы  $A$ , то одна из них (скажем,  $H_1$ ) содержит элемент  $b$ , не содержащийся в другой. Тогда, в силу теоремы 13.2.2,  $H_2^*$  — группа характеров фактор-группы  $A/H_2$ , и, согласно следствию 13.2.1, существует такой характер  $\chi \in H_2^*$ , что  $\chi(b) \neq 0$ . Следовательно,  $H_1^* \neq H_2^*$ . Так как группы  $A$  и  $A^*$  конечны и изоморфны, отсюда следует, что отображение  $H \rightarrow H^*$  является взаимно однозначным соответствием между подгруппами групп  $A$  и  $A^*$  и, в частности, что любая подгруппа  $K$  группы  $A^*$  совпадает с подгруппой  $H^*$ , соответствующей некоторой вполне определенной подгруппе  $H$  группы  $A$ . Если  $H_1 \rightleftarrows K_1 = H_1^*$  и  $H_2 \rightleftarrows K_2 = H_2^*$ , то из включения  $H_1 \supset H_2$  следует  $K_1 \subset K_2$ , так как из равенства  $\chi(h) = 0$  для любого элемента  $h \in H_1$  следует, что  $\chi(h) = 0$  для любого элемента  $h \in H_2 \subset H_1$ . Аналогично из того, что  $K_1 \subset K_2$ , следует включение  $H_1 \supset H_2$ . Таким образом, соответствие, установленное этой теоремой, является двойственностью между группами  $A$  и  $A^*$ . Двойственность группы  $A$  себе следует из изоморфизма групп  $A$  и  $A^*$ .

**Теорема 13.2.4.** *Периодическая абелева группа с конечными силовскими подгруппами двойственна себе.*

**Доказательство.** Пусть  $A$  — периодическая абелева группа с конечными силовскими подгруппами  $S(p)$ . Тогда группа  $S(p)$ , будучи конечной абелевой группой, двойственна себе. Положим  $H_p \rightleftarrows H_p^d$ , где через  $H_p^d$  обозначена подгруппа, соответствующая

подгруппе  $H_p$  группы  $S(p)$  при некотором дуальном отображении  $d$ . Если теперь  $H$  — произвольная подгруппа группы  $A$ , то  $H$  — прямая сумма своих силовских подгрупп  $H_p$ . Тогда полагаем  $H^d = \sum_p H_p$ .

Как легко проверить, соответствие  $H \rightarrow H^d$  является двойственностью группы  $A$ . Заметим, что эти рассуждения не проходят для прямых сумм любых конечных абелевых групп. Действительно, такая прямая сумма может содержать подгруппы, не являющиеся прямой суммой подгрупп слагаемых. Как было показано Бэрром [6], абелевые группы, двойственные себе, исчерпываются группами, о которых идет речь в теореме.

### 13.3. Полные группы

Аддитивная абелева группа  $A$  называется *полной*<sup>1)</sup>, если для любого элемента  $a \in A$  и любого целого числа  $n$  существует такой элемент  $x \in A$ , что  $nx = a$ .

Теорема 13.3.1. *Полная группа является прямым слагаемым любой содержащей ее абелевой группы  $A$ .*

*Доказательство.* Пусть абелева группа  $A$  содержит полную подгруппу  $D$ . Мы должны установить существование такой подгруппы  $B$ , что

$$A = D \oplus B, \text{ т. е. } D \cap B = 0 \text{ и } D \cup B = A. \quad (13.3.1)$$

Для доказательства этого удобно воспользоваться леммой Цорна, о которой шла речь в § 1.8. Если  $U_1 \subset U_2 \subset U_3 \subset \dots$  — возрастающая цепь таких подгрупп группы  $A$ , что  $D \cap U_i = 0$ , то подгруппа  $U = \bigcup_i U_i$  также обладает свойством  $D \cap U = 0$ . Следовательно, согласно лемме Цорна, группа  $A$  содержит максимальную подгруппу  $K$  со свойством  $K \cap D = 0$ . Утверждается, что подгруппа  $K$  является искомой группой  $B$ . Для доказательства достаточно проверить, что  $K \cup D = A$ . Пусть  $x$  — элемент группы  $A$ , не принадлежащий подгруппе  $K \cup D$ . Тогда в силу свойства максимальности подгруппы  $K$  подгруппа  $\{x\} \cup K$  имеет ненулевое пересечение с  $D$ . Следовательно, для некоторого неотрицательного целого числа  $n$  и элемента  $k \in K$  имеем  $nx + k = d \in D$ ,  $d \neq 0$ . Здесь  $n \neq 0$ , так как  $D \cap K = 0$ . Кроме того,  $n \neq 1$ , так как в противном случае мы бы имели, что  $x \in K \cup D$ . Так как  $D$  — полная группа, то  $d = nd_1$  для некоторого  $d_1 \in D$ , откуда  $n(x - d_1) = -k$ . Полагая  $x_1 = x - d_1$ , находим, что  $x_1 \notin K \cup D$ , так как в противном случае  $x \in K \cup D$ . Элементы из подгруппы  $K \cup \{x_1\}$  имеют вид  $mx_1 + k$ ,  $0 \leq m < n$ . Отсюда опять в силу

<sup>1)</sup> Автор пользуется термином „divisible group“ — „группа с делением“. — Прим. перев.

максимальности подгруппы  $K$  подгруппы  $\{x_1\} \cup K$  и  $D$  имеют общий ненулевой элемент  $n_1x_1 + k_1 = d = n_1d_2$ , где  $n_1 < n$ ,  $d, d_2 \in D$ . Далее, при  $x_2 = x_1 - d_2$  имеем  $n_1x_2 = -k_1 \in K$  и  $x_2 \notin K \cup D$ , так как в противном случае  $x_1 \in K \cup D$ . Продолжив этот процесс, мы дойдем до  $n_i = 1$ . Тогда  $x_i, x_{i-1}, \dots, x_1$  и  $x$  окажутся элементами из подгруппы  $K \cup D$ , что противоречит условию. Итак,  $K \cup D = A$ , и теорема доказана.

В книге Капланского [1]<sup>1)</sup> можно найти доказательство того факта, что любая полная группа представима как прямая сумма групп, изоморфных группе  $r_+$ , или группе  $Z(p^\infty)$ .

### 13.4. Сервантовые подгруппы

Будем говорить, что  $H$  — *сервантовая* подгруппа абелевой группы  $A$ , если для произвольного целого  $n$  и  $h \in H$  из существования элемента  $x \in A$ , для которого  $nx = h \in H$ , следует существование элемента  $h_1 \in H$ , такого, что  $nh_1 = h$ . Таким образом, определяющим свойством сервантовой подгруппы является свойство относительной полноты: деление в подгруппе  $H$  возможно, если оно возможно во всей группе. Полная группа, конечно, является сервантовой подгруппой любой абелевой группы, которая ее содержит. Прямое слагаемое группы также является сервантовой подгруппой. Хотя полные группы всегда бесконечны, существуют сервантовые подгруппы конечных групп, и поэтому это понятие полезно при изучении конечных групп.

Периодическая подгруппа<sup>2)</sup> абелевой группы является сервантовой, так как решение уравнения  $nx = h$ , где  $h$  — элемент конечного порядка, должно быть также элементом конечного порядка. Объединение возрастающей цепочки сервантовых подгрупп — опять сервантная подгруппа, так как произвольный элемент  $h$  этого объединения является элементом одной из групп цепи, и потому уравнение  $nx = h$  имеет решение в подгруппе, являющейся объединением групп цепи.

Теорема 13.4.1 показывает, что в очень многих случаях сервантная подгруппа является прямым слагаемым.

**Теорема 13.4.1.** Пусть  $A$  — абелева группа,  $H$  — ее сервантная подгруппа и фактор-группа  $A/H$  представима как прямая сумма циклических групп. Тогда подгруппа  $H$  является прямым слагаемым группы  $A$ .

*Доказательство.* Сначала докажем лемму.

**Лемма 13.4.1.** Если  $H$  — сервантная подгруппа группы  $A$  и  $y \in A/H$ , то существует элемент  $x \in A$ , порядок которого

<sup>1)</sup> См. также Курош [2], гл VII. — *Прим. ред.*

<sup>2)</sup> Подразумевается максимальная периодическая подгруппа, т. е. совокупность всех элементов конечного порядка. — *Прим. ред.*

равен порядку элемента  $u$  и образом которого при гомоморфизме  $A \rightarrow A/H$  служит  $u$ .

Действительно, если  $u$  — элемент бесконечного порядка, то любой элемент, являющийся его прообразом, будет искомым. Если же  $nu = 0$  и  $u \rightarrow y$ , то  $nu \rightarrow 0$  и  $nu = h \in H$ . Но тогда, в силу основного свойства подгруппы  $H$ ,  $h = nh_1$ ,  $h_1 \in H$ . Пусть  $x = u - h_1$ . Тогда  $x \rightarrow u$  и  $nx = n(u - h_1) = nu - nh_1 = h - h = 0$ , что и требовалось доказать.

Теперь теорема доказывается довольно просто. Пусть группа  $A/H$  — прямая сумма циклических групп, порожденных базисными элементами  $y_i$ ,  $i \in I$ . Выберем в группе  $A$  такие элементы  $x_i$ , что  $x_i \rightarrow y_i$ , причем порядки элементов  $x_i$  равны порядкам соответствующих  $y_i$ . Это возможно в силу леммы. Пусть  $K$  — подгруппа, порожденная элементами  $x_i$ . Если соотношение  $n_{i_1}x_{i_1} + \dots + n_{i_s}x_{i_s} = h \in H$  имеет место в группе  $A$ , то в фактор-группе  $A/H$  имеем  $n_{i_1}y_{i_1} + \dots + n_{i_s}y_{i_s} = 0$ , а так как  $y_i$  — базисные элементы группы  $A/H$ , отсюда следует, что  $n_{i_1}y_{i_1} = \dots = n_{i_s}y_{i_s} = 0$ . Но в силу равенства порядков элементов  $x_i$  и  $y_i$  это означает, что  $n_{i_1}x_{i_1} = \dots = n_{i_s}x_{i_s} = 0$ , т. е.  $h = 0$ . Следовательно,  $K \cap H = 0$ . Кроме того,  $K \cup H = A$ , так как подгруппа  $K$  содержит по одному элементу из каждого смежного класса группы  $A$  по подгруппе  $H$ . Таким образом,  $A = H \oplus K$ , и теорема доказана.

### 13.5. Общие замечания

Для более детального изучения абелевых групп читателю рекомендуется монография Капланского [1] и книга Куроша [2]. В книге Капланского особенно полезен обзор литературы.

Теорема 3.2.3 сводит в общем случае изучение периодических групп к изучению примарных групп. Одним из главных результатов для примарных групп является теорема Ульма, которая вполне описывает счетные примарные абелевые группы с помощью некоторой системы кардинальных чисел — так называемых „инвариантов Ульма“.

Прямая сумма бесконечных циклических групп называется *свободной абелевой группой*. Любая абелева группа с  $r$  образующими является гомоморфным образом свободной абелевой группы с  $r$  образующими. Любая подгруппа прямой суммы циклических групп есть прямая сумма циклических групп и, в частности, подгруппа свободной абелевой группы есть снова свободная абелева группа.

Как отмечалось в § 13.3, любая полная группа является прямой суммой групп, изоморфных группе  $\mathbb{Z}_{(p)}$  или группам типа  $\mathbb{Z}(p^\infty)$  для различных  $p$ . Произвольную абелеву группу можно погрузить в полную группу, и поэтому, в определенном смысле, изучение абелевых групп сводится к изучению подгрупп полных групп.

Так, группа без кручения (т. е. апериодическая) ранга 1 является подгруппой группы  $r_+$ .

Абелева группа, содержащая элементы как конечного, так и бесконечного порядка, называется *смешанной*. Как показывают примеры, смешанная группа не всегда представима в виде прямой суммы периодической подгруппы и группы без кручения. Но поскольку периодическая подгруппа сервантна, теорема 13.4.1 часто дает возможность разложить смешанную группу в прямую сумму периодической части и некоторой другой группы.

## Г л а в а 14

### МОНОМИАЛЬНЫЕ ПРЕДСТАВЛЕНИЯ И ПЕРЕМЕЩЕНИЕ

#### 14.1. Мономиальные подстановки

Рассмотрим множество  $S$  символов  $u_1, \dots, u_n$ , которые разрешается умножать слева на элементы группы  $H$  по следующим правилам:

$$1u_i = u_i, \quad (14.1.1)$$

где  $1$  — единица группы  $H$ , и

$$h_1(h_2u_i) = (h_1h_2)u_i.$$

Мономиальной подстановкой  $M$  называется отображение вида  $u_i \rightarrow h_{ij}u_j$ ,  $i = 1, \dots, n$ ,  $j = j(i)$ , где  $u_i \rightarrow u_j$  — подстановка множества  $S$ . Произведение двух отображений  $M_1$  и  $M_2$  определяется так: если  $M_1$  — отображение  $u_i \rightarrow h_{ij}u_j$  и  $M_2$  — отображение  $u_j \rightarrow h_{jk}u_k$ , то  $M_1M_2$  есть отображение  $u_i \rightarrow (h_{ij}h_{jk})u_k$ . При таком определении эти отображения образуют группу, единицей которой является отображение  $u_i \rightarrow u_i$ . Если сопоставить отображению  $M_1: u_i \rightarrow h_{ij}u_j$  матрицу  $(h_{ij})$ , в которой  $i$ -я строка и  $j$ -й столбец состоят из нулей, кроме места  $(i, j)$ , где стоит элемент  $h_{ij}$ , то умножению отображений будет соответствовать обычное перемножение соответствующих матриц.

В группе  $M$  всех мономиальных подстановок отображения  $u_i \rightarrow h_{ii}u_i$  образуют инвариантную подгруппу  $D$ , а фактор-группа  $M/D$  изоморфна симметрической группе степени  $n$ . Более обще, пусть  $G$  — подгруппа группы  $M$ . Если  $g$  из группы  $G$  является отображением  $u_i \rightarrow h_{ij}u_j$ , то  $g \rightarrow g^*: u_i \rightarrow u_j$  — гомоморфизм группы  $G$  на некоторую группу подстановок, ядром которого является подгруппа  $G \cap D$ .

Будем говорить, что группа  $G$  мономиальных подстановок транзитивна, если соответствующая группа подстановок транзитивна.

Теорема 14.1. Пусть группа  $G$  содержит подгруппу  $K$  и  $G = K + Kx_2 + \dots + Kx_n$ . Пусть также  $K \rightarrow H$  — гомоморфизм подгруппы  $K$  на группу  $H$ . Тогда транзитивное мономиальное представление группы  $G$  над группой  $H$  осуществляется следующим образом: для элемента  $g \in G$  пусть  $x_i g = k_{ij} x_j$ ,  $i = 1, \dots, n$ ,  $j = j(i)$ ,  $k_{ij} \in K$ ; пусть также  $h_{ij}$  —

образ элемента  $k_{ij}$  при гомоморфизме  $K \rightarrow H$ , тогда отображение  $\pi(g): u_i \rightarrow h_{ij}u_j$  является транзитивным мономиальным представлением группы  $G$  над группой  $H$ . Обратно, любое транзитивное мономиальное представление есть или представление подобного типа, или сопряженное такому представлению относительно группы  $D$ .

**Доказательство.** Пусть  $G = K + Kx_2 + \dots + Kx_n$  — разложение группы  $G$  по подгруппе  $K$ , и пусть  $K \rightarrow H$  — гомоморфизм группы  $K$  на группу  $H$ . Пусть  $g_1$  и  $g_2$  — два произвольных элемента группы  $G$ . Если  $x_i g_1 = k_{ij} x_j$  и  $x_j g_2 = k_{js} x_s$ , то  $x_i (g_1 g_2) = k_{ij} k_{js} x_s$ , откуда видно, что для соответствующих мономиальных подстановок справедливо равенство  $\pi(g_1 g_2) = \pi(g_1) \pi(g_2)$ , т. е. имеем представление группы  $G$  (конечно, не обязательно точное). Соответствующая группа подстановок является группой подстановок левых смежных классов, исследованной в § 5.3, которая, конечно, транзитивна.

Обратно, рассмотрим произвольное транзитивное мономиальное представление  $R$  группы  $G$ , т. е. для любого элемента  $g \in G$  имеем  $g \rightarrow \pi(g): u_i \rightarrow h_{ij}u_j$ . Выберем одну букву  $u_1$  и рассмотрим все такие элементы  $k \in G$ , что  $\pi(k): u_1 \rightarrow h_{11}u_1$  при  $h_{11} \in H$ . Они образуют подгруппу  $K$ . В силу транзитивности представления  $R$  для каждого  $i = 2, \dots, n$  существует такой элемент  $x_i$ , что  $\pi(x_i): u_1 \rightarrow h_{1i}u_i$ . Теперь легко видеть, что

$$G = K + Kx_2 + \dots + Kx_n. \quad (14.1.2)$$

Если  $R$  трансформируем элементом  $d: u_1 \rightarrow u_1, \dots, u_i \rightarrow h_{1i}^{-1}u_i$ , то при представлении  $d^{-1}Rd$  имеем  $d^{-1}\pi(x_i)d: u_1 \rightarrow u_i$ . Рассмотрим представление  $R^* = d^{-1}Rd$ . Если при  $k \in K$  отображение  $\pi(k)$  переводит  $u_1$  в  $hu_1$ , то  $\pi(x_i^{-1}kx_j)$  переводит  $u_i$  в  $hu_j$ , и обратно. Таким образом, каждый элемент  $h$ , на который происходит умножение при представлении  $R^*$ , участвует в представлении подгруппы  $K$ . Эти элементы  $h$  могут составить собственную подгруппу  $H_1$  исходной группы  $H$ . Однако если  $\pi(k)$  переводит  $u_1$  в  $hu_1$ , то отображение  $k \rightarrow h$  является гомоморфизмом  $K$  на  $H_1$ . Более того, если  $\pi(g)$  переводит  $u_i$  в  $h_{ij}u_j$ , то  $\pi(x_i g x_j^{-1})$  переводит  $u_1$  в  $h_{ij}u_j$ , откуда  $x_i g x_j^{-1} = k_{ij} \in K$  и отображение  $k_{ij} \rightarrow h_{ij}$  является гомоморфизмом группы  $K$  на  $H_1$ .

Заметим попутно, что замена представителей левых смежных классов группы  $G$  по подгруппе  $K$  приводит к другому мономиальному представлению, сопряженному с первым относительно группы  $D$ .

## 14.2. Перемещение

Пусть имеем мономиальное представление  $R$  группы  $G$  над группой  $H$ :

$$\pi(g): u_i \rightarrow h_{ij} u_j, \quad i = 1, \dots, n, \quad j = j(i), \quad (14.2.1)$$

где число  $n$  конечно. Тогда, как легко заметить, отображение

$$g \rightarrow \prod_{i=1}^n h_{ij} \pmod{H'} \quad (14.2.2)$$

является гомоморфизмом группы  $G$  в фактор-группу  $H/H'$ , где  $H'$  — коммутант группы  $H$ . Рассмотрим частный случай, когда  $H=K$ :

$$G = K + Kx_2 + \dots + Kx_n. \quad (14.2.3)$$

Если  $\varphi(z) = x_j$  для  $z = kx_j$ ,  $k \in K$ , то

$$V_{G \rightarrow K}(g) \equiv \prod_{i=1}^n x_i g \varphi(x_i g)^{-1} \pmod{K'} \quad (14.2.4)$$

и отображение  $V_{G \rightarrow K}(g)$  является гомоморфизмом группы  $G$  в группу  $K/K'$ . Этот гомоморфизм называется *перемещением* (по-английски: transfer; по-немецки: Verlagerung) группы  $G$  в группу  $K$ . Если  $H$  — гомоморфный образ группы  $K$ , то отображение (14.2.2) является гомоморфным отображением образа перемещения, так как при гомоморфизме  $K \rightarrow H$  фактор-группа  $K/K'$  отображается на  $H/H'$  ( $K'$  — вполне характеристическая подгруппа группы  $K$ ). Основные свойства перемещения дает теорема 14.2.1.

**Теорема 14.2.1.**

1) Отображение  $g \rightarrow V_{G \rightarrow K}(g)$  является гомоморфизмом  $G$  в фактор-группу  $K/K'$ .

2) Перемещение  $V_{G \rightarrow K}(g)$  не зависит от выбора представителей  $x_i$ .

3) Если  $G \supset K \supset T$ , то  $V_{G \rightarrow T}(g) = V_{K \rightarrow T}[V_{G \rightarrow K}(g)]$ .

**Доказательство.** Как уже отмечалось, первое свойство является следствием теории мономиальных представлений. Однако мы докажем все три свойства, исходя прямо из определения перемещения (14.2.4). Относительно первого свойства заметим, что если  $x_i g_1 = k_{ij} x_j$  ( $i = 1, \dots, n$ ),  $x_j g_2 = k_{js} x_s$  ( $j = 1, \dots, n$ ), то

$$V_{G \rightarrow K}(g_1) \equiv \prod_i k_{ij} \pmod{K'}, \quad V_{G \rightarrow K}(g_2) \equiv \prod_j k_{js} \pmod{K'}$$

и

$$V_{G \rightarrow K}(g_1 g_2) \equiv \prod_i (k_{is}^*) \pmod{K'}, \quad \text{где } k_{is}^* = k_{ij} k_{js}.$$

Докажем второе свойство. Пусть представители смежных классов первой и второй систем связаны соотношением  $x_i^* = a_i x_i$  и  $x_i g = k_{ij} x_j$ . Тогда  $x_i^* g = a_i x_i g = a_i k_{ij} x_j = a_i k_{ij} a_j^{-1} x_j^*$ . При первом выборе представителей  $V(g) \equiv \prod_t k_{ij} \pmod{K'}$ , а при втором  $V(g) \equiv \prod_t (a_i k_{ij} a_j^{-1}) \equiv \prod_t a_i \cdot \prod_t k_{ij} \cdot \prod_t a_j^{-1} \equiv \prod_t k_{ij} \pmod{K'}$ .

Установим, наконец, третье свойство.

Пусть

$$\begin{aligned} G &= K + Kx_2 + \dots + Kx_n, \\ K &= T + Ty_2 + \dots + Ty_m. \end{aligned} \quad (14.2.5)$$

Тогда

$$\begin{aligned} G &= T + Ty_2 + \dots + Ty_m + \\ &\quad + \dots \dots \dots \dots \dots \dots \dots \\ &\quad + Tx_i + Ty_2 x_i + \dots + Ty_m x_i + \\ &\quad + \dots \dots \dots \dots \dots \dots \dots \\ &\quad + Tx_n + Ty_2 x_n + \dots + Ty_m x_n. \end{aligned} \quad (14.2.6)$$

Пусть теперь для  $g \in G$   $x_i g = k_{ij} x_j$  и  $y_r k_{ij} = t_{ijrs} y_s$ . Таким образом,  $y_r x_i g = t_{ijrs} y_s x_j$ . Отсюда  $V_{G \rightarrow T}(g) \equiv \prod_{l,r} t_{ijrs} \pmod{T'}$  и

$$V_{G \rightarrow K}(g) \equiv \prod_t k_{ij} \pmod{K'}$$
. Далее,  $V_{K \rightarrow T}(k_{ij}) \equiv \prod_r t_{ijrs} \pmod{T'}$ .

Следовательно,

$$\begin{aligned} V_{K \rightarrow T}(g) &\equiv \prod_t V_{K \rightarrow T}(k_{ij}) \pmod{T'} \equiv V_{K \rightarrow T}(\prod_t k_{ij}) \pmod{T'} \equiv \\ &\equiv V_{K \rightarrow T}[V_{G \rightarrow K}(g)]. \end{aligned}$$

Заметим, что так как перемещение  $K$  на  $T$  отображает  $K'$  в единицу, имеет смысл говорить о перемещении  $V_{G \rightarrow K}(g)$  в  $T$ , несмотря на то, что речь идет об элементе фактор-группы  $K/K'$ , а не самой группы  $K$ .

### 14.3. Теорема Бернсайда

**ТЕОРЕМА 14.3.1.** *Если силовская подгруппа  $P$  конечной группы  $G$  содержится в центре своего нормализатора, то группа  $G$  обладает таким нормальным делителем  $H$ , что в качестве представителей смежных классов по  $H$  можно выбрать элементы группы  $P$ .*

*Доказательство.* Сначала докажем следующую лемму.

**Лемма 14.3.1.** *Если два множества  $K_1$  и  $K_2$  инвариантны в силовской подгруппе  $P$  группы  $G$  и сопряжены в  $G$ , то они сопряжены и в подгруппе  $N_G(P)$ .*

Действительно, пусть  $x^{-1}K_1x = K_2$ ,  $x \in G$ . Так как множество  $K_1$  инвариантно в  $P$ , то множество  $K_2 = x^{-1}K_1x$  инвариантно в  $x^{-1}Px = Q$ . Таким образом, подгруппы  $P$  и  $Q$  содержатся в нормализаторе множества  $K_2$  и, следовательно, являясь силовскими подгруппами, сопряжены в  $N_G(K_2)$ . Итак,  $y^{-1}Qy = P$ , где  $y$  — такой элемент, что  $y^{-1}K_2y = K_2$ . Поэтому при  $z = xy$  имеем  $z^{-1}Pz = P$ ,  $z^{-1}K_1z = K_2$ , и лемма доказана.

Теперь перейдем к доказательству теоремы. Так как подгруппа  $P$  содержится в центре нормализатора  $N_G(P)$ ,  $P$  — абелева группа и  $P' = 1$ . Рассмотрим перемещение  $V_{G \rightarrow P}$ . Пусть  $u \in P$ , вычислим  $V_{G \rightarrow P}(u)$ . Для этого возьмем в качестве представителей смежных классов по  $P$  элементы вида  $x_i, x_iu, \dots, x_iu^{r-1}$ , где  $x_iu^r \in Px_i$  и  $x_iu^j \notin Px_i$  при  $j < r$ . При этом  $x_iu^{j-1} \cdot u \cdot (x_iu^j)^{-1} = x_iu^ju^{-j}x_i^{-1} = 1$  для  $j < r$  и  $x_iu^{r-1} \cdot u \cdot (x_iu^r)^{-1} = x_iu^rx_i^{-1}$ . Следовательно, для каждого цикла длины  $r$  в представлении элемента  $u$  подстановкой множества левых смежных классов по  $P$  в произведении для перемещения  $V_{G \rightarrow P}(u)$  встречается член  $x_iu^rx_i^{-1}$ , а остальные члены равны единице. Таким образом,  $V_{G \rightarrow P}(u) = \prod_i x_iu^rx_i^{-1}$ . Далее, элемент  $x_iu^rx_i^{-1} \in P$  сопряжен с  $u^r$

в группе  $G$ , а так как  $P$  — абелева группа, оба элемента инвариантны в  $P$ . Для  $y \in N_G(P)$ , по лемме,  $x_iu^rx_i^{-1} = y^{-1}u^ry$ . По условию, подгруппа  $P$  содержится в центре своего нормализатора, откуда  $y^{-1}u^ry = u^r$ . Следовательно,  $V_{G \rightarrow P}(u) = \prod_i u^r = u^n$ , где  $n = [G : P]$  — сумма длин всех циклов. Поскольку  $P$  — силовская подгруппа порядка, скажем,  $p^s$ , отсюда ясно, что  $p \nmid n = [G : P]$ . Таким образом, при перемещении  $G$  на подгруппу  $P$  последняя изоморфно отображается на себя и  $V_{G \rightarrow P}(G) = P$ , так как, очевидно,  $V_{G \rightarrow P}(G)$  содержится в  $P$ . Ядром этого гомоморфизма является группа  $H$  индекса  $p^s$  в группе  $G$  и порядка  $n = [G : P]$ . Следовательно,  $H$  — инвариантная подгруппа индекса  $p^s$ , и поэтому элементы из  $P$  могут быть выбраны в качестве представителей смежных классов по  $H$ .

**Следствие 14.3.1.** *Порядок конечной простой группы или делится на 12, или же, если  $p$  — наименьшее простое число, делящее  $n$ , делится на  $p^3$ .*

**Доказательство.** Пусть  $p$  — наименьшее простое число, которое делит порядок простой группы  $G$ . Предположим, что силовская  $p$ -подгруппа  $P$  имеет порядок  $p$  или  $p^2$  и, следовательно, абелева. Тогда по доказанной теореме, если только нормализа-

тор  $N_G(P)$  не индуцирует нетривиального автоморфизма подгруппы  $P$ , группа  $G$  обладает фактор-группой, изоморфной подгруппе  $P$ . Если порядок подгруппы  $P$  равен  $p$ , то порядок ее группы автоморфизмов равен  $p-1$ , т. е. меньше  $p$ . Если подгруппа  $P$  циклическая порядка  $p^2$ , то порядок ее группы автоморфизмов равен  $p(p-1)$ , а если она не циклическая порядка  $p^2$ , то этот порядок равен  $(p^2-p)(p^2-1)=p(p-1)^2(p+1)$ . Ни одно из этих чисел не делится на простое число, которое больше  $p$ , если  $p$  нечетно, так как  $p+1=2[(p+1)/2]$ , и, следовательно, нормализатор  $N_G(P)$  индуцирует в  $P$  только тождественный автоморфизм. Если же  $p=2$ , то в последнем случае  $p+1=3$ , и нормализатор  $N_G(P)$  может индуцировать в  $P$  автоморфизм порядка 3; но тогда порядок нормализатора  $N_G(P)$  делится на 12.

#### 14.4. Теоремы Ф. Холла, Грюна и Виландта

Основная цель данного параграфа — установить связь между силовскими  $p$ -подгруппами группы  $G$  и фактор-группами  $G/k$ , порядок которых равен степени числа  $p$ .

Для формулировок и доказательств нам понадобятся понятия сильной и слабой замкнутости.

**Определение.** Пусть  $H$  — подгруппа группы  $G$ , а  $B$  — подгруппа  $H$ . Будем говорить, что подгруппа  $B$  сильно замкнута в  $H$  (по отношению к  $G$ ), если  $H \cap B^x \subseteq B$ , где  $B^x = x^{-1}Bx$ , а  $x$  — любой элемент из  $G$ , и слабо замкнута в  $H$ , если из включения  $B^x \subseteq H$  следует, что  $B^x = B$ .

Говорят, что группа  $G$   $p$ -нормальна, если центр  $Z$  силовой  $p$ -подгруппы  $P$  является центром любой другой силовой  $p$ -подгруппы  $P_1$ , которая его содержит. Это свойство — частный случай слабой замкнутости; оно равносильно требованию слабой замкнутости центра  $Z$  группы  $P$  в группе  $P$  относительно  $G$ . Действительно, предположим, что группа  $G$   $p$ -нормальна. Пусть  $x \in G$  — такой элемент, что  $Z^x \subseteq P$ . Тогда  $Z \subseteq P_1 = P^{x^{-1}}$ . В силу  $p$ -нормальности группы  $G$  получим, что  $Z$  — центр подгруппы  $P_1$ . Но тогда  $Z^x$  — центр подгруппы  $P_1^x = P$ , откуда  $Z^x = Z$  и поэтому центр  $Z$  слабо замкнут в  $P$ . Обратно, предположим, что центр  $Z$  слабо замкнут в подгруппе  $P$  и что  $Z \subseteq P_1$ , где  $P_1$  — другая силовая  $p$ -подгруппа. Тогда для некоторого элемента  $x \in G$  имеем  $P_1^x = P$ . Поэтому  $Z^x \subseteq P$ . В силу условия слабой замкнутости  $Z = Z^x$ . Но если  $Z_1$  — центр подгруппы  $P_1$ , то  $Z_1^x =$  центр подгруппы  $P_1^x = P$ . Следовательно,  $Z_1^x = Z = Z^x$ , и  $Z = Z_1$  — центр подгруппы  $P_1$ , т. е. группа  $G$   $p$ -нормальна.

Ясно, что из сильной замкнутости следует слабая замкнутость. Слабо замкнутая подгруппа  $B$  группы  $H$  инвариантна в  $H$ . Под-

группа группы  $H$ , порожденная всеми элементами, являющимися решениями некоторого уравнения  $x^k = 1$ , слабо замкнута, а если эти решения образуют подгруппу  $X$ , то последняя сильно замкнута в  $H$ . Последнее свойство выполняется, если  $p$ -группа  $H$  регулярна, а также при некоторых других условиях.

В дальнейшем иногда будем писать  $V(g)$  вместо  $V_{G \rightarrow H}(g)$ . Если

$$G = H + Hx_2 + \dots + Hx_n,$$

то

$$V(g) \equiv \prod_{i=1}^n x_i g \varphi(x_i g)^{-1} \pmod{H'}$$

Можно заменить сравнения по модулю  $H'$  сравнениями по модулю  $H_0$ , где  $H_0$  — произвольная подгруппа группы  $H$ , содержащая  $H'$ , так что фактор-группа  $H/H_0$  абелева. Встречающиеся ниже сравнения берутся по модулю  $H_0$ .

Для элемента  $g \in G$  и чисел  $i = 1, \dots, n$  определяем числа  $i_g$  из условия  $x_i g x_i^{-1} \in H$ . Тогда при фиксированном  $g$  соответствие  $i \rightarrow i_g$  — подстановка  $\pi(g)$  транзитивного представления группы  $G$  подстановками левых смежных классов по подгруппе  $H^1$ ). Таким образом, имеем

$$V(g) \equiv \prod_i x_i g x_{i_g}^{-1}.$$

Подстановка  $\pi(g)$  разлагается на ряд циклов, включая циклы длины 1, соответствующие буквам, остающимся на месте. Выберем по одному символу из каждого цикла и обозначим множество выбранных символов через  $C_H(g)$ . Если  $i \in C_H(g)$ , то пусть  $r_i$  — порядок цикла, в котором встречается символ  $i$ . Тогда

$$\sum_{i \in C_H(g)} r_i = n,$$

т. е. сумма длин всех циклов равна  $n$ .

Лемма 14.4.1.

$$V(g) \equiv \prod_{i \in C_H(g)} x_i g^{r_i} x_i^{-1},$$

где  $x_i g^{r_i} x_i^{-1}$  — наименьшая степень элемента  $x_i g x_i^{-1}$ , содержащаяся в подгруппе  $H$ .

*Доказательство.* В подстановке  $\pi(g)$  цикл, начинающийся символом  $i$ , состоит из символов  $i, i_g, \dots, i_g^{r_i-1}$ , различных между собой; в качестве представителей соответствующих смеж-

<sup>1)</sup> В дальнейшем автор пользуется также обозначением  $ig$  вместо  $i_g$ .  
Прим. ред.

ных классов по  $H$  можно взять элементы  $x_i, x_i g, \dots, x_i g^{r_i-1}$ . Тогда все сомножители перемещения  $V(g)$ , соответствующие циклу с элементом  $i$ , образуют произведение

$$(x_i g)(x_i g)^{-1} \cdot (x_i g) g (x_i g^2)^{-1} \cdot (\dots) \cdot (x_i g^{r_i-1}) g x_i^{-1} = x_i g^{r_i} x_i^{-1},$$

потому что  $\varphi(x_i g^s) = x_i g^s$ ,  $s = 1, \dots, r_i - 1$ ,  $\varphi(x_i g^{r_i}) = x_i$ . Так как  $x_i g^s \notin Hx_i$  при  $s < r_i$ , элемент  $x_i g^{r_i} x_i^{-1}$  является наименьшей степенью произведения  $x_i g x_i^{-1}$ , которая принадлежит  $H$ .

Будем называть произведение всех циклов длины один *диагональным сомножителем*  $d(g)$  перемещения  $V(g)$  и записывать

$$d(g) \equiv \prod_{\substack{i=1 \\ i \neq g}} x_i g x_i^{-1} \pmod{H_0}.$$

Здесь так же, как и для  $V(g)$ , произведение  $d(g)$  по модулю  $H_0$  не зависит от порядка сомножителей и выбора представителей  $x_i$  смежных классов.

**Лемма 14.4.2.** *Если  $u$  и  $v$  — сопряженные элементы группы  $G$ , то  $d(u) = d(v)$  и  $d(u^{-1}) = [d(u)]^{-1}$ .*

*Доказательство.* Пусть  $v = t^{-1}ut$ . Тогда равенство  $iu = i$  равносильно равенству  $itv = it$ , откуда, по определению,

$$\begin{aligned} d(v) &\equiv \prod_{i=iu} x_{it} v x_{it}^{-1} \equiv \prod_{i=lu} (x_{it} t^{-1} x_i^{-1})(x_{iux_i^{-1}})(x_{it} x_{it}^{-1}) \equiv \\ &\equiv \prod_{i=lu} (x_i u x_i^{-1}) \equiv d(u). \end{aligned}$$

Действительно, элементы  $x_{it} t^{-1} x_i^{-1}$  и  $x_{it} x_{it}^{-1}$  лежат в  $H$  и взаимно обратны. Кроме этого, равенство  $i = iu$  равносильно равенству  $i = iu^{-1}$ , откуда

$$d(u^{-1}) \equiv \prod_{i=lu} s_i u^{-1} s_i^{-1} \equiv \left( \prod_{i=lu} s_i u s_i^{-1} \right)^{-1} \equiv [d(u)]^{-1}.$$

Для элемента  $h \in H$  определим функцию  $d^*(h) \equiv h^{-1}d(h)$ . Тогда, по лемме 14.4.2,  $h \equiv d(h)[d^*(h)]^{-1} \equiv d(h)d^*(h^{-1})$  и  $d(h') \equiv d(x_i h' x_i^{-1})$ , и поэтому, если  $x_i h' x_i^{-1} \in H$ , имеем

$$x_i h' x_i^{-1} \equiv d(h') d^*(x_i h'^{-1} x_i^{-1}) \equiv h' d^*(h') d^*(x_i h'^{-1} x_i^{-1});$$

и, наконец, применяя лемму 14.4.1, получаем лемму.

**Лемма 14.4.3.** *Если  $h \in H$ , то*

$$V(h) \equiv h^n \prod_{i \in C_H(h)} d^*(h'^i) d^*(x_i h'^{-r_i} x_i^{-1}).$$

**Следствие 14.4.1.** Если  $d^*(h) \in H_0$  для всех  $h \in H$ , то для любого элемента  $h \in H$  справедливо равенство  $V(h) = h^n$ .

Пусть  $p$  — простое число,  $G_1$  — некоторая конечная группа, а  $G = u_p(G_1)$  — группа, порожденная всеми элементами из  $G_1$ , порядки которых взаимно просты с  $p$ . Таким образом,  $G_1/G$  — максимальная  $p$ -фактор-группа группы  $G_1$ . Пусть  $P_1$  — силовская  $p$ -подгруппа группы  $G_1$ ,  $N_1$  — ее нормализатор, а  $H_1$  — произвольная подгруппа группы  $G_1$ , содержащая  $N_1$ . Положим  $P = P_1 \cap G$ ,  $N = N_1 \cap G$ ,  $H = H_1 \cap G$ , так что  $G_1 = GP_1 = GN_1 = GH_1$ , а  $P_1/P = N_1/N = H_1/H = G_1/G$ . Подгруппа  $G$  вполне характеристична в  $G_1$ ,  $P$  — силовская  $p$ -подгруппа группы  $G$ , подгруппа  $N$  содержится в нормализаторе группы  $P_1$  и  $G$ , а следовательно, и в нормализаторе подгруппы  $P_1 \cap G = P$ . Далее,  $u_p(G) = G$ , так как подгруппа  $G$  порождается элементами, порядки которых взаимно просты с  $p$ . Однако не исключена возможность, что  $u_p(H) \subset H$ . Предположим, что последнее действительно имеет место. Тогда  $u_p(H)$  — вполне характеристическая подгруппа группы  $H$ , а  $H$  — инвариантна в  $H_1$ . Так как  $H_1/H$  —  $p$ -группа, очевидно, что  $u_p(H) = u_p(H_1)$ . Положим

$$\begin{aligned} H_0 &= H^p \cup (H, H_1) \cup u_p(H) = \\ &= H^p (H, H_1) u_p(H), \end{aligned}$$

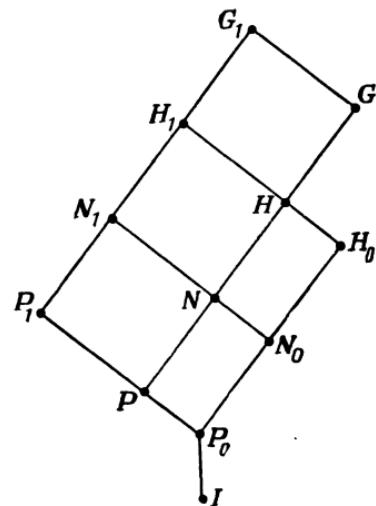


Рис. 6. Теорема Ф. Холла.

где  $H^p$  — подгруппа, порожденная  $p$ -ми степенями элементов из  $H$ , а  $(H, H_1)$  — подгруппа, порожденная коммутаторами  $(h, h_1)$ ,  $h \in H$ ,  $h_1 \in H_1$ . Так как все три подгруппы  $H^p$ ,  $(H, H_1)$  и  $u_p(H)$  инвариантны в  $H$ , то их объединение совпадает с их произведением. Так как  $u_p(H) = u_p(H_1)$ , фактор-группа  $H_1/u_p(H)$  является  $p$ -группой и потому нильпотента. Таким образом, фактор-группа  $(H, H_1)/u_p(H)$  строго содержится в группе  $H/u_p(H)$ . Более того, так как подгруппа  $H^p$  содержится в любой такой подгруппе  $T$ , что  $H \supset T \supset (H, H_1) u_p(H)$  при  $[H : T] = p$ , то в случае  $u_p(H) \subset H$  подгруппа  $H_0$  также является собственной инвариантной подгруппой группы  $H$  и фактор-группа  $H/H_0$  есть  $p$ -группа. Рассмотрим следующую задачу: какие элементы подгруппы  $P$  надо присоединить к  $H_0$ , чтобы получить группу  $H$ ?

**Лемма 14.4.4.** Группа  $H$  порождается подгруппой  $H_0$  и множеством всех элементов вида  $d^*(u)$ ,  $u \in P$ .

*Доказательство.* Как и прежде, имеем

$$\begin{aligned} G &= H + Hx_2 + \dots + Hx_n, \\ d(u) &\equiv \prod_{i=lu} x_i u x_i^{-1} (\text{mod } H_0), \\ d^*(u) &\equiv u^{-1}d(u) (\text{mod } H_0). \end{aligned}$$

В силу включений  $H_0 \supseteq (H, H_1) \supseteq (H, H) = H'$  фактор-группа  $H/H_0$  абелева. Так как  $u \in P \subseteq H$ , очевидно, все элементы  $d^*(u)$  принадлежат  $H$ . Таким образом,  $K = \{d^*(u) | u \in P\} \cup H_0 \subseteq H$ . Чтобы доказать обратное включение  $H \subseteq K$ , воспользуемся тем обстоятельством, что, ввиду абелевости  $p$ -группы  $H/H_0$ ,  $V(w) \equiv 1 \pmod{H_0}$  для любого элемента  $w \in G$ , порядок которого взаимно прост с  $p$ . Но по построению группы  $G$  порождается этими элементами, откуда  $V(u) \equiv 1 \pmod{H_0}$  для любого  $u \in G$ . Тогда тем более  $V(u) \in K$  для любого  $u \in P$ . Отсюда, согласно лемме 14.4.3, для  $u \in P$  получаем

$$V(u) \equiv u^n \prod_{i \in C_H(u)} d^*(u^{r_i}) d^*(x_i u^{-r_i} x_i^{-1}),$$

где  $d^*(u^{r_i}) \in K$  по определению,  $v = x_i u^{-r_i} x_i^{-1}$  — элемент из  $H$ , порядок которого равен степени  $p$ . Следовательно,  $y^{-1}vy \in P$  для некоторого  $y \in H$ , откуда  $d^*(v) = v^{-1}d(v) = x^{-1}d(y^{-1}vy)$  (лемма 14.4.2). Поэтому

$$d^*(v) \equiv v^{-1}y^{-1}vyd^*(y^{-1}vy) \equiv (v, y)d^*(y^{-1}vy).$$

Но, по определению,  $(v, y) \in H' \subseteq H_0$  и  $d^*(y^{-1}vy) \in K$ , откуда  $d^*(v) = d^*(x_i u^{-r_i} x_i^{-1}) \in K$ . Отсюда следует для  $u \in P$ :  $u^n \equiv V(u) \in K$ . Но  $(n, p) = 1$ , и любой элемент из  $P$  является  $n$ -й степенью некоторого элемента из  $P$ . Таким образом,  $P \subseteq K$ , а так как  $H/H_0$  —  $p$ -группа, а  $P$  — силовская  $p$ -подгруппа группы  $H$ , получаем  $H = H_0 \cup P \subseteq K$ . Итак,  $H = K$ , и лемма доказана.

Так как  $G \triangleleft G_1$ ,  $H = H_1 \cap G$  и  $G \cup H_1 = G_1$ , можно взять в качестве представителей левых смежных классов группы  $G_1$  по  $H_1$  представителей левых смежных классов группы  $G$  по  $H$ :  $G_1 = H_1 + H_1 x_2 + \dots + H_1 x_n$ . Следовательно, записывая  $G_1$  как сумму двойных смежных классов по  $H_1$  и  $P_1$ , получаем

$$G_1 = H_1 + H_1 t_1 P_1 + \dots + H_1 t_s P_1,$$

где  $1, t_1, \dots, t_s$  — некоторые из элементов  $1, x_2, \dots, x_n$ . Пусть  $\pi_i$  ( $i = 1, \dots, s$ ) — транзитивные представления группы  $P_1$  подстановками смежных классов по  $H_1$ , из которых состоит двойной смежный класс  $H_1 t_i P_1$ . Степень подстановок  $\pi_i$  больше единицы, так как в противном случае  $H_1 t_i P_1 = H_1 t_i$ , откуда  $t_i P_1 t_i^{-1} \subseteq H_1$ ,

но тогда, по теореме Силова,  $t_i P_1 t_i^{-1} = u^{-1} P_1 u$  для некоторого элемента  $u \in H_1$ . Поэтому  $ut_i \in N_1 \subseteq H_1$ , откуда  $t_i \in H_1$ , что противоречит выбору элемента  $t_i$ . Таким образом, представление группы  $P_1$  не тождественно, и его ядро  $K_i$  строго содержитс в  $P_1$ , причем фактор-группа  $P_1/K_i$  точно представляется подстановками  $\pi_i$ . Так как  $P_1/K_i$  —  $p$ -группа, ее центр не равен единице. Следовательно, мы можем выбрать элемент  $z_i \in P_1$  так, чтобы подстановка  $\pi_i(z_i)$  имела порядок  $p$  и содержалась в центре группы  $\pi_i(P_1)$ , т. е. была перестановочна с любой подстановкой  $\pi_i(u)$  для  $u \in P_1$ . Любой элемент из центра транзитивной группы подстановок, оставляющий на месте один символ, действует тождественно и на всех других символах. Поэтому подстановка  $\pi_i(z_i)$  не оставляет на месте ни одного смежного класса по  $H_1$  и состоит исключительно из циклов длины  $p$ . Для любого элемента  $u \in P \subseteq P_1$  подстановка  $\pi_i(u)$  перестановочна с  $\pi_i(z_i)$ , и поэтому, если подстановка  $\pi_i(u)$  отображает в себя некоторый смежный класс, скажем,  $H_1 x_{j+1}$ , содержащийся в двойном смежном классе  $H_1 t_i P_1$ , она должна также оставлять на месте классы  $H_1 x_{j+1}, \dots, H_1 x_{j+p}$  того цикла подстановки  $\pi_i(z_i)$ , которому принадлежит класс  $H_1 x_{j+1}$ . Следовательно, для  $u \in P$

$$d(u) \equiv u \cdot \prod d_j(u) \pmod{H_0},$$

где

$$d_j(u) = h_1 h_2 \dots h_p$$

и

$$h_k = x_{j+k} u x_{j+k}^{-1}, \quad k = 1, \dots, p,$$

а  $x_{j+1}, \dots, x_{j+p}$ , как и выше, — представители смежных классов из цикла подстановки  $\pi_i(z_i)$  для некоторого  $i$ . Здесь элемент  $u = 1 \cdot u \cdot 1^{-1}$  является единственным сомножителем произведения  $d(u)$ , принадлежащим подгруппе  $H_1$ . Заметим также, что при  $x_{j+k} u x_{j+k}^{-1} = h_k \in H_1$ ,  $x_{j+k} \in G$ ,  $u \in P$ , имеем  $h_k \in G$ , откуда  $h_k \in H_1 \cap G = H$ , и поэтому эти элементы действительно входят сомножителями в произведение  $d(u)$ . Из равенства  $d^*(u) = u^{-1} d(u)$  следует, что

$$d^*(u) \equiv \prod_j d_j(u) \pmod{H_0}.$$

Отсюда и из леммы 14.4.4 сразу же вытекает

**Лемма 14.4.5.** Группа  $H$  порождается подгруппой  $H_0$  и элементами  $d_j(u)$ ,  $u \in P$ .

Рассмотрим подробнее один из элементов  $d_j(u)$ , положив для удобства  $w_k = x_{j+k}$ ,  $k = 1, \dots, p$ . Имеем

$$H_1 w_k z_i = H_1 w_{k+1},$$

где индексы берутся по модулю  $p$ . Поэтому  $w_k z_i = y_k w_{k+1}$ , где  $y_k \in H_1$ . Кроме того,  $w_k u w_k^{-1} = h_k$ ,  $d_j(u) = h_1 \dots h_p$ . Теперь

$$\begin{aligned} w_k(u, z_i) w_k^{-1} &= w_k u^{-1} w_k^{-1} \cdot w_k z_i^{-1} u z_i \cdot w_k^{-1} = \\ &= h_k^{-1} y_{k-1}^{-1} w_{k-1} u w_{k-1}^{-1} \cdot w_{k-1} z_i w_k^{-1} = \\ &= h_k^{-1} y_{k-1}^{-1} h_{k-1} \cdot y_{k-1} = \\ &= h_k^{-1} h_{k-1} (h_{k-1}, y_{k-1}). \end{aligned}$$

Но  $y_i \in H_1$ , а  $h_i \in H$ . В силу этого, а также в силу включения  $(H_1, H) \subseteq H_0$  справедливо сравнение

$$w_k(u, z_i) w_k^{-1} \equiv h_k^{-1} h_{k-1} \pmod{H_0}.$$

Но подгруппа  $P$  инвариантна в  $P_1$ , откуда  $(u, z_i) \in P$ , и поэтому для  $u_i = (u, z_i)$  диагональные сомножители в произведении  $d(u_i)$  из смежных классов  $H w_k$ ,  $k = 1, \dots, p$ , равны  $h_k^{-1} h_{k-1} \pmod{H_0}$ ,  $k = 1, \dots, p$ . Таким образом, из сравнений  $w_k u w_k^{-1} \equiv h_k \pmod{H_0}$ ,  $k = 1, \dots, p$ , получаем  $w_k(u, z_i) w_k^{-1} \equiv h_k^{-1} h_{k-1} \pmod{H_0}$ ,  $k = 1, \dots, p$ . Теперь при  $u = u_0$  имеем  $u_1 = (u, z_i)$ ,  $u_2 = (u_1, z_i)$  и, рекуррентно,  $u_{s+1} = (u_s, z_i)$ . Мы видели, что если  $w_k u_s w_k^{-1} \equiv h_{k,s} \pmod{H_0}$ ,  $k = 1, \dots, p$ , то

$$w_k u_{s+1} w_k^{-1} \equiv h_{k-s} h_{k,s}^{-1} \equiv h_{k+1,s} \pmod{H_0}.$$

Следовательно, применяя индукцию по  $s$ , получаем

$$w_k u_s w_k^{-1} \equiv h_{k-s} h_{k-s+1}^{(-s)} h_{k-s+2}^{(-s-1)} \dots h_k^{(-1)^s}.$$

Здесь показателями степени являются биномиальные коэффициенты, взятые с чередующимися знаками. Из свойств биномиальных коэффициентов и из включения  $H^p \subseteq H_0$  следует, что

$$w_k u_{p-1} w_k^{-1} \equiv h_1 h_2 \dots h_p \equiv d_j(u) \pmod{H_0}.$$

Таким образом,

$$d_j(u) \equiv w_k(u, \overbrace{z_i, \dots, z_i}^{p-1}) w_k^{-1} \pmod{H_0},$$

где  $u \in P$ ,  $z_i \in P_1$ . Обозначим  $e_p(u, z_i) = (u, \overbrace{z_i, \dots, z_i}^{p-1})$ , тогда из леммы 14.4.5 следует, что группа  $H$  может быть получена присоединением к группе  $H_0$  определенных элементов из  $H$  вида  $x_{j+k} e_p(u, z_i) x_{j+k}^{-1}$  (для всех  $u \in P$ ), т. е. присоединением определенных диагональных сомножителей элементов  $e_p(u, z_i)$  для  $i = 1, \dots, s$  и всех

$u \in P$ . Так как эти сомножители — элементы группы  $H$ , порядки которых равны степени  $p$ , а  $P$  — силовская  $p$ -подгруппа группы  $H$ , то мы можем трансформировать их элементами из  $H$  так, чтобы они попали в  $P$ . По модулю  $H_0$  трансформация не изменит наши элементы, так как фактор-группа  $H/H_0$  абелева. Этим доказана наша основная теорема.

**Теорема 14.4.1.** (Ф. Холл.) Пусть  $G_1$  — конечная группа,  $P_1$  — ее силовская  $p$ -подгруппа,  $N_1$  — нормализатор подгруппы  $P_1$ , а  $H_1$  — подгруппа, содержащая  $N_1$ . Пусть  $G = u_p(G_1)$  — подгруппа, порожденная всеми элементами группы  $G_1$ , порядки которых взаимно просты с  $p$ ; положим  $H = G \cap H_1$ ,  $N = G \cap N_1$ ,  $P = G \cap P_1$ . Тогда  $u_p(H_1) = u_p(H)$ , и если  $u_p(H) \neq H$ , то  $H_0 = H^p(H_1, H) u_p(H)$  — собственная подгруппа группы  $H$ , причем последняя может быть получена присоединением к  $H_0$  определенных элементов из  $H$ , сопряженных с элементами

$e_p(u, z_i) = (u, \overbrace{z_i, \dots, z_i}^{p-1})$ , где  $u \in P$  и  $z_i$ ,  $i = 1, \dots, s$ , — элементы из  $P_1$ . Пусть

$$G_1 = H_1 P_1 + H_1 t_1 P_1 + \dots + H_1 t_s P_1$$

— разложение группы  $G_1$  в сумму двойных смежных классов по подгруппам  $H_1$  и  $P_1$ , и пусть  $\pi_i$ ,  $i = 1, \dots, s$ , — транзитивные представления подгруппы  $P_1$  на смежных классах по  $H_1$ , из которых состоит двойной смежный класс  $H_1 t_i P_1$ . Тогда степени представлений  $\pi_i$  не равны единице и можно выбрать элемент  $z_i$  так, чтобы  $\pi_i(z_i)$  была подстановкой порядка  $p$ , принадлежащей центру группы  $\pi_i(P_1)$ .

**Следствие 14.4.2.** Если  $e_p(u, z) = 1$  для всех  $u, z \in P_1$ , то  $u_p(N_1) = N = u_p(G_1) \cap N_1$  и  $G_1 / u_p(G_1) = N_1 / u_p(N_1)$ . В частности, это имеет место, если класс нильпотентности подгруппы  $P_1$  меньше  $p$ .

Здесь мы считали, что  $H_1 = N_1$  и, значит,  $H = N$ .

Пусть  $Q_1$  — слабо замкнутая подгруппа группы  $P_1$ . Тогда, как мы уже отмечали, подгруппа  $Q_1$  инвариантна в нормализаторе  $N_1$  группы  $P_1$ , и поэтому мы можем взять нормализатор подгруппы  $Q_1$  в качестве подгруппы  $H_1 \supseteq N_1$ . Тогда предыдущая теорема является уточнением теоремы Виландта [3].

**Теорема 14.4.2.** (Холл — Виландт.) Пусть  $P_1$  — силовская  $p$ -подгруппа группы  $G_1$  и  $Q_1$  — слабо замкнутая подгруппа группы  $P_1$ . Пусть  $N_1$  — нормализатор подгруппы  $P_1$ , а  $H_1$  — нормализатор подгруппы  $Q_1$ . Тогда каждое из условий

1)  $e_p(u, z) = 1$  для всех  $u \in P_1$  и всех  $z \in Q_1$ ,

2)  $e_{p-1}(u, z) = 1$  для всех  $u, z \in Q_1$ ,

3)  $Q_1 \subseteq Z_{p-1}(P_1)$ , где  $Z_{p-1}(P_1)$  —  $(p-1)$ -й центр группы  $P_1$ , дает равенство  $u_p(H_1) = H = u_p(G_1) \cap H_1$ , откуда в свою очередь вытекает, что  $G_1/u_p(G_1) = H_1/u_p(H_1)$ .

*Доказательство.* Как и в доказательстве теоремы 14.4.1, пусть  $K_i$  — ядро представления  $\pi_i$  группы  $P_1$  на смежных классах по  $H_1$  из двойного класса  $H_1t_iP_1$ . Предположим, если это возможно, что  $Q_1 \not\subseteq K_i$ . Тогда  $H_1t_iQ_1 = H_1t_i$  и  $t_iQ_1t_i^{-1} \subseteq H_1$ . Следовательно,  $t_iQ_1t_i^{-1}$  —  $p$ -подгруппа группы  $H_1$ , и существует такой элемент  $y \in H_1$ , что  $y^{-1}t_iQ_1t_i^{-1}y \subseteq P_1$ , где  $P_1$  — силовская  $p$ -подгруппа, также содержащаяся в  $H_1$ . В силу слабой замкнутости  $Q_1$  это означает, что  $y^{-1}t_iQ_1t_i^{-1}y = Q_1$ , а поэтому  $y^{-1}t_i \in H_1$ , так как  $H_1$  — нормализатор подгруппы  $Q_1$  и  $t_i \in H_1$ , что невозможно. Итак,  $Q_1 \not\subseteq K_i$ . Подгруппа  $Q_1$  инвариантна в  $P_1$ , и поэтому образ ее в группе  $P_1/K_i$  является инвариантной подгруппой и должен, следовательно, содержать элементы ее центра. Поэтому мы можем выбрать требуемые элементы  $z_i$  в подгруппе  $Q_1$ . Это дает первое условие. Заметим, что в этом условии было бы достаточно взять  $u \in P = P_1 \cap G$ , но, вообще говоря, нам заранее не известно, какая из подгрупп группы  $P_1$  совпадает с  $P$ . Из третьего условия следует первое, так как если  $Q_1 \subseteq Z_{p-1}(P_1)$ , то  $z \in \overbrace{Z_{p-1}(P_1)}^{p-1}$

$(u, z) \in Z_{p-2}(P_1)$ ,  $(u, z, z) \in Z_{p-3}$ , ...,  $e_p(u, z) = (u, \overbrace{z, \dots, z}^{p-1}) = 1$ . Так как  $e_p(u, z) = e_{p-1}(u_1, z)$ , где  $u_1 = (u, z)$  и  $u_1 \in Q_1$ , если  $u \in P$ , то, следовательно, первое условие вытекает также из второго.

**Следствие 14.4.3.** Пусть  $Q_1$  — характеристическая подгруппа группы  $P_1$ . Если она не слабо замкнута в  $P_1$ , то существует другая силовская  $p$ -подгруппа  $P_2$ , которая содержит подгруппу  $Q_1$ , но в которой  $Q_1$  не инвариантна. Этот случай имеет место, если  $Q_1$  удовлетворяет одному из условий (1), (2), (3) теоремы, а группы  $G_1/u_p(G_1)$  и  $H_1/u_p(H_1)$  не изоморфны.

*Доказательство.* Так как подгруппа  $Q_1$  характеристична в  $P_1$ , то  $Q_1$  инвариантна в  $N_1$ . Следовательно, нормализатор  $N_1$  содержится в нормализаторе подгруппы  $Q_1$ . Если  $Q_1$  не слабо замкнута в  $P_1$ , то  $x^{-1}Q_1x \subseteq P_1$  для некоторого элемента  $x$ , но  $x^{-1}Q_1x \neq Q_1$ . Если бы подгруппа  $x^{-1}Q_1x$  была инвариантна в  $P_1$ , то в силу леммы 14.3.1 подгруппы  $Q_1$  и  $x^{-1}Q_1x$  были бы взаимно сопряжены в группе  $N_1$ , что невозможно. Следовательно, подгруппа  $x^{-1}Q_1x$  содержится в группе  $P_1$ , но не инвариантна в ней, и поэтому подгруппа  $Q_1$  содержится в  $P_2 = xP_1x^{-1}$ , но также не инвариантна в ней. Если подгруппа  $Q_1$  удовлетворяет одному из условий (1), (2), (3) теоремы, то теорема может быть неверной только в случае, если подгруппа  $Q_1$  не слабо замкнута в  $P_1$ .

Следующие теоремы несколько проще, чем предыдущие.

**Теорема 14.4.3.** Пусть  $P$  — силовская  $p$ -подгруппа группы  $G$ ,  $G'$  — коммутант группы  $G$ . Тогда

$$V_{G \rightarrow P}(G) \cong P/P \cap G'.$$

*Доказательство.* Так как  $V_{G \rightarrow P}(G)$  — гомоморфизм группы  $G$  в  $p$ -группу  $P/P'$ , то любой элемент, порядок которого взаимно прост с  $p$ , отображается в единицу. Так как  $G$  порождается подгруппой  $P$  и силовскими подгруппами, принадлежащими другим простым числам, то  $V(G) = V(P)$ . Пусть

$$G = P + Px_2 + \dots + Px_n.$$

По лемме 14.4.1 для  $u \in P$

$$V(u) \equiv \prod_{i \in C_P(u)} x_i u^{r_i} x_i^{-1} \pmod{P'},$$

$$V(u) \equiv \prod_{i \in C_P(u)} u^{r_i} (u^{r_i} x_i^{-1}) \pmod{P'}$$

и

$$V(u) \equiv \prod_{i \in C_P(u)} u^{r_i} \equiv u^n \pmod{G'}.$$

Следовательно, так как  $(n, p) = 1$ ,  $V(u) \not\equiv 1 \pmod{G'}$ , если  $u \notin P$ ,  $u \notin G'$ . Но так как группа  $V(G)$  абелева,  $V(G') \equiv 1$ . Следовательно, ядро гомоморфизма  $P \rightarrow V_{G \rightarrow P}(P)$  равно точно  $P \cap G'$ , и поэтому  $V_{G \rightarrow P}(G) \cong P/P \cap G'$ .

**Теорема 14.4.4.** (ПЕРВАЯ ТЕОРЕМА ГРЮНА [1].) Пусть  $P$  — силовская  $p$ -подгруппа группы  $G$ . Тогда  $V_{G \rightarrow P}(G) \cong P/P^*$ , где

$$P^* = [P \cap N_G(P)] \bigcup_{z \in G} (P \cap z^{-1}P'z).$$

*Доказательство.* Из теоремы 14.4.3 мы знаем, что  $V_{G \rightarrow P}(G) \cong P/P \cap G'$ . По построению группа  $P^*$  является объединением подгрупп, содержащихся в группе  $P \cap G'$ , откуда  $P^* \subseteq P \cap G'$ . Покажем, что  $P \cap G' \subseteq P^*$ . Для этого достаточно доказать, что любой элемент  $u$  из группы  $P \cap G'$  содержится также в  $P^*$ . Это доказательство проведем индукцией по порядку элемента  $u$ . Очевидно, что  $1 \in P^*$ . Пусть

$$G = P + Py_2P + \dots + Py_sP$$

— разложение группы  $G$  в сумму двойных смежных классов по  $P$ . Пусть  $u \in P \cap G'$ . Тогда, по лемме 14.4.1,

$$V(u) \equiv \prod_{i \in C_P(u)} x_i u^{r_i} x_i^{-1} \pmod{P'},$$

причем произведение элементов, соответствующих смежному классу  $PyP$ , равно

$$w = \prod_k yv_k u^{r_k} v_k^{-1} y^{-1},$$

где  $v_1 = 1$ ,  $v_k \in P$ , а  $\sum_k r_k = p^t$ , если класс  $PyP$  состоит из  $p^t$  левых смежных классов по  $P$ . При исследовании сомножителя  $w$  мы различаем два случая: 1)  $t \geq 1$  в  $p^t$ ; 2)  $t = 0$ ,  $p^t = 1$ .

Случай 1. В этом случае

$$w \equiv yu^{p^t} y^{-1} (\text{mod } yP'y^{-1}).$$

Значению  $v_1 = 1$  в произведении  $w$  соответствует сомножитель  $yu^{p^b} y^{-1} \in P$ , а так как  $b \leq t$ , то  $yu^{p^t} y^{-1} \in P$ . Но и  $w \in P$ , поэтому

$$w \equiv yu^{p^t} y^{-1} (\text{mod } P \cap yP'y^{-1})$$

и тем более

$$w \equiv yu^{p^t} y^{-1} (\text{mod } P^*).$$

Так как  $u \in P \cap G'$ , то  $V(u) \equiv 1 \pmod{P'}$ , откуда  $V(yu^{p^t} y^{-1}) \equiv 1 \pmod{P'}$ . Но тогда элемент  $yu^{p^t} y^{-1}$ , так как он принадлежит  $P$ , содержится в ядре  $P \cap G'$ , а так как  $t > 1$ , его порядок меньше порядка элемента  $u$ , откуда в силу предположения индукции  $yu^{p^t} y^{-1} \in P^*$ . Также в силу индукции  $u^{p^t} \in P^*$ , откуда

$$w \equiv yu^{p^t} y^{-1} \equiv 1 \equiv u^{p^t} \pmod{P^*}.$$

Случай 2. Здесь  $PyP = Py$  и потому  $Py \subseteq N_G(P)$ ; имеем

$$w \equiv yuy^{-1} \equiv u \pmod{N'_G(P)}$$

и

$$w \equiv u \pmod{P \cap N'_G(P)},$$

откуда  $w \equiv u \pmod{P^*}$ . Следовательно, во всех случаях

$$w_j \equiv u^{p^{t_j}} \pmod{P^*},$$

где  $w_j$  — сомножитель в произведении  $V(u)$  для смежного класса  $Py_j P$ , который содержит  $p^{t_j}$  левых смежных классов по  $P$ . Поэтому

$$V(u) \equiv u^n \pmod{P^*},$$

где  $n = [G : P]$  — число, взаимно простое с  $p$ . Но  $V(u) \equiv 1$  для  $u \in P \cap G'$ , т. е.  $V(u) \in P' \subseteq P^*$ . Таким образом,  $u^n \equiv 1 \pmod{P^*}$  и, следовательно,  $u \in P^*$ , что и требовалось доказать.

**Теорема 14.4.5.** (Вторая теорема Грюна.) *Если группа  $G$   $p$ -нормальна, то наибольшая абелева  $p$ -группа, являющаяся*

*фактор-группой группы  $G$ , изоморфна такой же фактор-группе для нормализатора центра силовской  $p$ -подгруппы.*

*Доказательство.* Пусть  $P$  — силовская  $p$ -подгруппа группы  $G$ ,  $Z$  — ее центр. Пусть  $G'(p) \trianglelefteq G'$  — такая наименьшая инвариантная подгруппа группы  $G$ , что фактор-группа  $G/G'(p)$  — абелева  $p$ -группа. Тогда  $G = G'(p) \cup P$ , так как порядок подгруппы  $G'(p)$  должен делиться на все степени  $p_i^{\alpha_i}$ , т. е.  $p_i^{\alpha_i} \mid (G : 1)$  для всех простых чисел  $p_i$ , отличных от  $p$ . Положим  $G^* = P \cup G'$ , тогда  $G'(p) \cup G^* = G$ .  $G^* \cap G'(p) = G'$ , так как фактор-группа  $G^*/G'$  содержит только  $p$ -элементы, а фактор-группа  $G'(p)/G'$  содержит только элементы, порядки которых взаимно просты с  $p$ . По теореме 2.4.1,  $G/G'(p) \cong G^*/G' \cong P/P \cap G'$ . Пусть  $N$  — нормализатор  $P$ , а  $H$  — нормализатор центра  $Z$  подгруппы  $P$ . Так как  $Z$  — характеристическая подгруппа в  $P$ ,  $H \trianglelefteq N$ . Если теперь  $H'(p)$  — такая наименьшая инвариантная подгруппа в  $H$ , что  $H/H'(p)$  — абелева  $p$ -группа, то, как и для группы  $G$ ,  $H/H'(p) \cong P/P \cap H'$ . Следовательно, чтобы доказать нашу теорему, мы должны установить равенство  $P \cap G' = P \cap H'$ . Очевидно, что  $G \trianglelefteq H$ ,  $G' \trianglelefteq H'$ , откуда  $P \cap G' \trianglelefteq P \cap H'$ . Достаточно доказать, следовательно, включение в другую сторону:  $P \cap H' \trianglelefteq P \cap G'$ . В силу первой теоремы Грюна

$$P \cap G' = (P \cap N') \bigcup_{x \in G} (P \cap x^{-1}P'x).$$

Так как  $H \trianglelefteq N$ ,  $P \cap H' \trianglelefteq P \cap N'$ . Мы должны показать также, что  $P \cap H' \trianglelefteq P \cap x^{-1}P'x$  для любого  $x \in G$ . Обозначим  $P \cap x^{-1}P'x$  через  $M$ . Тогда  $Z \subseteq N_G(M)$  и  $x^{-1}Zx \subseteq N_G(M)$ , так как  $x^{-1}Zx$  — центр подгруппы  $x^{-1}Px$ . При этом подгруппа  $Z$  содержится в силовской подгруппе  $R$  группы  $N_G(M)$ , а  $x^{-1}Zx$  — в силовской подгруппе  $S$  той же группы. Следовательно, для некоторого элемента  $y \in N_G(M)$  подгруппы  $Z$  и  $y^{-1}x^{-1}Zxy$  лежат в одной и той же силовской подгруппе  $Q$  группы  $G$ , содержащей  $R$ . В силу свойства  $p$ -нормальности подгрупп,  $Z$  и  $y^{-1}x^{-1}Zxy$  являются центром группы  $Q$ , т. е. они совпадают. Таким образом,  $Z = y^{-1}x^{-1}Zxy$  и, значит,  $xy = h \in N_G(Z) = H$ . Но  $y \in N_G(M)$ , откуда

$$M = y^{-1}My = y^{-1}Py \cap y^{-1}x^{-1}P'xy = y^{-1}Py \cap h^{-1}P'h \subseteq H.$$

Таким образом,  $M = P \cap x^{-1}P'x \subseteq P \cap H'$ , и теорема доказана.

Теорема Ф. Холла дает возможность улучшить также и вторую теорему Грюна, отбросив требование абелевости.

**Теорема 14.4.6.** (Холл — Грюн.) *Если группа  $G$   $p$ -нормальна, то наибольшая фактор-группа группы  $G$ , являющаяся  $p$ -группой, изоморфна такой же фактор-группе для нормализатора центра силовской  $p$ -подгруппы.*

**Доказательство.** Пусть в обозначениях теоремы 14.4.2  $G_1$  — наша группа  $G$ ,  $P_1$  — силовская  $p$ -подгруппа,  $Q_1$  — центр подгруппы  $P_1$ ,  $H_1$  — нормализатор центра  $Q_1$ . Тогда  $p$ -нормальность группы  $G_1$ , как отмечалось, означает, что подгруппа  $Q_1$  слабо замкнута в  $P_1$ . Так как  $Q_1 = Z(P_1)$ , третье условие теоремы 14.4.2 выполняется и, следовательно,  $G_1/u_p(G_1) \cong H_1/u_p(H_1)$ . Это максимальные фактор-группы, являющиеся  $p$ -группами; тем самым теорема доказана.

Мы можем также уточнить теорему Бернсайда. При каких условиях силовская  $p$ -подгруппа  $P$  группы  $G$  изоморфна фактор-группе группы  $G$ ? Иначе говоря, когда имеет место изоморфизм  $G/u_p(G) \cong P$ ? Предположим, что это свойство выполняется. Пусть  $u_p(G) = B$ ; тогда подгруппа  $B$  состоит из всех элементов, порядки которых взаимно просты с  $p$ . При этом  $B \cap P = 1$ ,  $B \cup P = BP = G$ . Если  $Q$  — произвольная подгруппа группы  $P$ , то  $B \cup Q = BQ$  — подгруппа, содержащая  $Q$  и все элементы, порядки которых взаимно просты с  $p$ . Подгруппа  $B$  инвариантна в группе  $BQ$ . Положим  $W = N_{BQ}(Q)$ . Тогда пересечение  $W \cap B$  состоит из элементов группы  $W$ , порядки которых не делятся на  $p$ . Ясно, что  $W \cap B \triangleleft W$  и что  $Q \triangleleft W$ . Но тогда  $W = (W \cap B) \times Q$ . Следовательно, любой элемент, порядок которого взаимно прост с  $p$  и который перестановочен с подгруппой  $Q$ , перестановочен почленно с каждым ее элементом. Это свойство, являющееся, как мы только что показали, следствием изоморфизма  $G/u_p(G) \cong P$ , также и достаточно для этого изоморфизма. В этом и состоит усиление теоремы Бернсайда (теоремы 14.3.1).

**Теорема 14.4.7.** *Группа  $G$  обладает фактор-группой  $G/u_p(G)$ , изоморфной силовской  $p$ -подгруппе  $P$ , тогда и только тогда, когда для любой подгруппы  $Q$  группы  $P$  элемент, порядок которого взаимно прост с  $p$  и который перестановочен с подгруппой  $Q$  в целом, перестановочен с ней поэлементно.*

**Доказательство.** Применим индукцию по порядку группы  $G$ ; утверждение очевидно, если  $G = P$ . Покажем, что группа  $G$   $p$ -нормальна. Пусть  $Z$  — центр группы  $P$ . Согласно следствию из теоремы 14.4.2, если группа  $G$  не  $p$ -нормальна, то центр  $Z$  содержится в другой силовской  $p$ -группе  $P_2$ , но не инвариантен в ней. Тогда по теореме 4.2.5 существует подгруппа  $Q$  группы  $P$ , перестановочная в целом, но не перестановочная поэлементно с некоторым элементом, порядок которого взаимно прост с  $p$ . Это противоречит условию. Поэтому группа  $G$   $p$ -нормальна. Согласно теореме 14.4.6,  $G/u_p(G) \cong H/u_p(H)$ , где  $H$  — нормализатор центра  $Z$ . Если  $H$  — собственная подгруппа  $G$ , то по индукции  $H/u_p(H) \cong P$ , и теорема доказана.

Поэтому рассмотрим случай, когда  $G = H$  и, следовательно,  $Z \triangleleft G$ . Если группа  $G/Z$  содержит  $p$ -группу  $Q/Z$ , которая перестановочна в целом, но не поэлементно с элементом, порядок которого взаимно прост с  $p$ , то это же самое справедливо для ее полного прообраза  $Q$ . Поэтому наше условие справедливо для  $G/Z$ , и, следовательно, группа  $G/Z$  обладает такой инвариантной подгруппой  $K/Z$ , что соответствующая фактор-группа изоморфна группе  $P/Z$ . Так как подгруппа  $K$  содержится в нормализаторе центра  $Z$  и порядок группы  $K/Z$  взаимно прост с  $p$ , подгруппа  $K$  содержит также и в централизаторе центра  $Z$ . Следовательно,  $K = Z \times K_1$ , где порядок подгруппы  $K_1$  не делится на  $p$ . Но подгруппа  $K_1 = u_p(K) = u_p(G)$  состоит исключительно из элементов, порядки которых взаимно просты с  $p$ . Итак,  $G/u_p(G) \cong P$ , что и требовалось доказать.

## Глава 15

### РАСШИРЕНИЯ ГРУПП И КОГОМОЛОГИЯ В ГРУППАХ

#### 15.1. Композиция инвариантной подгруппы и фактор-группы

Вообще говоря, всякая группа  $G$ , содержащая заданную группу  $U$  в качестве подгруппы, называется *расширением* группы  $U$ . Расширения групп были обстоятельно изучены Рейнольдом Бэрром [11]. Здесь мы ограничимся случаями, когда группа  $U$  инвариантна в группе  $G$ .

Отто Шрейер [1, 2] первый рассмотрел проблему построения всех групп  $G$  с заданными инвариантной подгруппой  $N$  и фактор-группой  $H \cong G/N$ . Всегда существует, по меньшей мере одна такая группа, так как прямое произведение  $N$  и  $H$  обладает этим свойством.

Предположим сперва, что подобная группа  $G$  нам дана, и изучим ее подробно. Элементы фактор-группы  $H \cong G/N$  будем обозначать символами  $1, u, v, \dots, w$ . Каждый элемент  $x \in H$  соответствует смежному классу группы  $G$  по  $N$ . Выберем представитель  $\bar{x}$  смежного класса  $xN$ , соответствующего элементу  $x$ , причем условимся в качестве представителя класса  $N$  выбирать всегда единицу 1 группы  $G$ . Тогда

$$G = N + \bar{u}N + \bar{v}N + \dots + \bar{w}N, \quad (15.1.1)$$

и при любом выборе представителей  $\bar{u}$  при гомоморфизме  $G \rightarrow H$  имеем

$$\bar{u} \rightarrow u, \quad \bar{u} \in G, \quad u \in H. \quad (15.1.2)$$

Тогда отображение

$$a \mapsto \bar{u}^{-1}a\bar{u} = a^u, \quad (15.1.3)$$

где  $a \in N$ , является автоморфизмом подгруппы  $N$ , так как  $N$  — инвариантная подгруппа. Кроме того,

$$\bar{u} \cdot \bar{v} = \bar{uv} (u, v), \quad (15.1.4)$$

где  $(u, v) \in N$ , так как при гомоморфизме  $G \rightarrow H$ ,  $\bar{u} \rightarrow u$ ,  $\bar{v} \rightarrow v$ . Множество всех элементов  $(u, v)$ , определенных равенствами (15.1.4), назовем *системой факторов*. Таким образом, строение группы  $G$  зависит от следующих четырех данных:

- 1) инвариантной подгруппы  $N$ ,

- 2) фактор-группы  $H$ ,
- 3) автоморфизмов подгруппы  $N$ :  $a \mapsto a^u$ ,  $a \in N$ ,  $u \in H$ ,
- 4) системы факторов  $(u, v) \in N$ ,  $u, v \in H$ .

Необходимо подчеркнуть, что, вообще говоря, автоморфизмы и система факторов, определенные равенствами (15.1.3) и (15.1.4), зависят от выбора представителя  $\bar{u}$  смежного класса  $\bar{u}N$ , соответствующего элементу  $u \in H$ .

Автоморфизмы и система факторов должны удовлетворять определенным условиям. Трансформируя элемент  $a \in N$ , получаем

$$(a^u)^v = (u, v)^{-1} (a^{uv}) (u, v). \quad (15.1.5)$$

Так как в группе  $G$   $(\bar{u} \bar{v}) \bar{w} = \bar{u} (\bar{v} \bar{w})$ , то

$$(\bar{u} \bar{v}) \bar{w} = [\bar{u} \bar{v} (u, v)] \bar{w} = \bar{u} \bar{v} \cdot \bar{w} (u, v)^w = \bar{u} \bar{v} \bar{w} (uv, w) (u, v)^w.$$

а также

$$\bar{u} (\bar{v} \bar{w}) = \bar{u} [\bar{v} \bar{w} (v, w)] = \bar{u} \bar{v} \bar{w} (u, vw) (v, w).$$

Отсюда следует

$$(uv, w) (u, v)^w = (u, vw) (v, w). \quad (15.1.6)$$

Для произведения двух элементов  $\bar{u}a$  и  $\bar{v}b$  группы  $G$  имеем

$$(\bar{u}a) (\bar{v}b) = \bar{u} \bar{v} a^v b = \bar{u} \bar{v} (u, v) a^v b,$$

т. е.

$$(\bar{u}a) (\bar{v}b) = \bar{u} \bar{v} (u, v) a^v b. \quad (15.1.7)$$

То, что представителем  $N$  является единица, согласно (15.1.4) дает

$$(u, 1) = 1 = (1, v) \quad (15.1.8)$$

для всех  $u, v \in H$ .

Обратно, свойства (15.1.5) и (15.1.6) автоморфизмов и системы факторов обеспечивают существование группы  $G$  с инвариантной подгруппой  $N$  и фактор-группой  $G/N \cong H$ . Действительно, введем символы  $\bar{u}a$ ,  $u \in H$ ,  $a \in N$ , составляющие множество  $G$ . В нем определим бинарную операцию умножения следующим образом:

$$\bar{u}a \cdot \bar{v}b = \bar{u} \bar{v} (u, v) a^v b. \quad (15.1.9)$$

Используя (15.1.5) и (15.1.6), легко показать, что это умножение ассоциативно. Действительно,

$$\begin{aligned} (\bar{u}a \cdot \bar{v}b) \cdot \bar{w}c &= \bar{u} \bar{v} (u, v) a^v b \cdot \bar{w}c = \bar{u} \bar{v} \bar{w} (uv, w) (u, v)^w (a^v)^w b^w c = \\ &= \bar{u} \bar{v} \bar{w} (uv, w) (u, v)^w (v, w)^{-1} a^{vw} (v, w) b^w c = \\ &= \bar{u} \bar{v} \bar{w} (u, vw) a^{vw} (v, w) b^w c = \\ &= \bar{u}a \cdot \bar{v}w (v, w) b^w c = \\ &= \bar{u}a \cdot (\bar{v}b \cdot \bar{w}c). \end{aligned}$$

Удобно (однако, как читатель может проверить, не обязательно) принять, кроме соотношений (15.1.5) и (15.1.6), также равенство

$$(1, 1) = 1 \quad (15.1.10)$$

как частный случай равенства (15.1.8). Если в соотношении (15.1.5) мы полагаем  $u = v = 1$  и применяем тождество (15.1.10), то получаем  $(a^1)^1 = a^1$ , а так как  $a^1 = c$  — произвольный элемент из группы  $N$ , получим, что  $c^1 = c$  для всех  $c \in N$ . Теперь в равенстве (15.1.6) полагаем  $u = v = 1$ . Тогда  $1 = (1, 1)^w = (1, w)$ . Аналогично из равенств  $v = w = 1$  находим  $(u, 1) = 1$ ,  $\bar{1} \cdot 1 \cdot wc = \bar{w}(1, w)c = \bar{w}c$  и  $\bar{u}a \cdot \bar{1} \cdot 1 = \bar{u}(u, 1)a = \bar{u}a$ , поэтому элемент  $\bar{1} \cdot 1$  является единицей системы  $G$ . Так как  $a \xrightarrow{\bar{1}} a^w$  — автоморфизм группы  $N$ , существует такой элемент  $d \in N$ , что  $d^w = (w^{-1}, w)^{-1}c^{-1}$  для данных  $c \in N$  и  $w \in K$ . Следовательно, для любого элемента  $\bar{w}c \in G$  справедливо равенство  $\bar{w}^{-1}d \cdot \bar{w}c = \bar{1}(w^{-1}, w)d^w c = \bar{1} \cdot 1$ , т. е. любой элемент из  $G$  обладает левым обратным. Таким образом,  $G$  — группа. Правило умножения (15.1.9) в этой группе таково, что отображение

$$\bar{u}a \rightarrow u \quad (15.1.11)$$

является гомоморфизмом группы  $G$  на  $H$ , ядро которого состоит из всех элементов вида  $\bar{1}a$ . Так как

$$\bar{1}a \cdot \bar{1}b = \bar{1}(1, 1)ab = \bar{1}ab,$$

то соответствие  $\bar{1}a \xrightarrow{\bar{1}} a$  — изоморфизм между этим ядром и группой  $N$ . Так как  $\bar{u}\bar{1} \cdot \bar{1}a = \bar{u}(u, 1)a = \bar{u}a$ , можно взять элементы  $\bar{u} = \bar{u}\bar{1}$  в качестве представителей смежных классов по  $N$  и рассматривать элемент  $\bar{u}a$  как произведение  $\bar{u}$  на  $a$ . Сформулируем полученные результаты в виде теоремы.

**Теорема 15.1.1.** (ШРЕЙЕР.) *Пусть дана группа  $G$ , содержащая нормальный делитель  $N$ , и пусть  $H$  — фактор-группа  $G/N$ . Если выбрать представители  $\bar{u}$  в классах  $\bar{u}N \rightarrow u \in H$ , причем  $\bar{1} = 1$ , то тем самым будут определены автоморфизмы  $\bar{u}$  и система факторов, удовлетворяющие следующим тождествам:*

$$(a^u)^v = (u, v)^{-1}(a^{uv})(u, v), \quad a, (u, v) \in N; \quad u, v \in H;$$

$$(uv, w)(u, v)^w = (u, vw)(v, w); \quad (1, 1) = 1.$$

*Обратно, если для каждого элемента  $u \in H$  задан автоморфизм  $a \xrightarrow{\bar{u}} a^u$  группы  $N$  и для этих автоморфизмов и системы факторов  $[(u, v) \in N]$ ,  $u, v \in H$ , выписанные выше соотношения справедливы, то элементы  $\bar{u}a$ ,  $u \in H$ ,  $a \in N$  с законом*

умножения  $\bar{u}a \cdot \bar{v}b = \bar{uv}(u, v)a^vb$  образуют группу  $G$  с инвариантной подгруппой  $N$  и фактор-группой  $G/N$ , изоморфной  $H$ .

Если не требовать, чтобы выполнялось равенство  $(1, 1) = 1$ , то теорема еще остается справедливой, если в качестве единицы группы  $G$  взять элемент  $\bar{1}(1, 1)^{-1}$ .

Единственное расширение  $G$ , определенное группами  $N$  и  $H$ , автоморфизмами  $a \rightarrow a^u$  и системой факторов  $(u, v)$ , будем обозначать  $E[N, H, a^u, (u, v)]$ .

Если изменить систему представителей смежных классов по  $N$  в  $G$ , положив

$$\bar{\bar{u}} = \bar{u}\alpha(u), \quad u \in H, \quad \alpha(u) \in N, \quad (15.1.12)$$

где  $\bar{1} = \bar{1} = 1$ , т. е.  $\alpha(1) = 1$ , то получим новые автоморфизмы

$$a \rightarrow a^{u^1} = \bar{\bar{u}}^{-1}a\bar{\bar{u}} = \alpha(u)^{-1}a^u\alpha(u) \quad (15.1.13)$$

и новую систему факторов  $(u, v)^1$ , для которой

$$\begin{aligned} \bar{\bar{u}} \cdot \bar{\bar{v}} &= \bar{u}\alpha(u)\bar{v}\alpha(v) = \bar{uv}(u, v)\alpha(u)^v\alpha(v) = \\ &= \bar{\bar{uv}}(u, v)^1 = \bar{uv}\alpha(uv)(u, v)^1. \end{aligned} \quad (15.1.14)$$

#### ОПРЕДЕЛЕНИЕ. Два расширения

$$E_1 = E(N, H, a^u, (u, v)) \text{ и } E_2 = E(N, H, a^{u^1}, (u, v)^1)$$

называются эквивалентными, если их автоморфизмы и системы факторов связаны соотношениями

$$\begin{aligned} a^{u^1} &= \alpha(u)^{-1}a^u\alpha(u), \\ (u, v)^1 &= \alpha(uv)^{-1}(u, v)\alpha(u)^v\alpha(v), \end{aligned}$$

где  $\alpha(u)$  — функция на элементах  $u \in H$  со значениями в  $N$ , причем  $\alpha(1) = 1$ . Эквивалентность двух расширений будем обозначать так:  $E(N, H, a^u, (u, v)) \sim E(N, H, a^{u^1}, (u, v)^1)$ . Отношение эквивалентности расширений  $E_2$  и  $E_1$  сводится к изменению системы представителей смежных классов по  $N$  в той же самой группе  $G$ , и поэтому ясно, что это в обычном смысле этого слова эквивалентность, т. е. она обладает свойством симметричности, рефлексивности и транзитивности.

Если представители  $\bar{\bar{u}}$  смежных классов по  $N$  могут быть выбраны так, что

$$\bar{\bar{uv}} = \bar{\bar{u}}\bar{\bar{v}}, \quad (15.1.15)$$

т. е.  $(u, v)^1 = 1$ <sup>1)</sup>, то они образуют группу, изоморфную группе  $H$ . Эти группы можно отождествить. В этом случае говорят, что

<sup>1)</sup> Тождественно для всех  $u$  и  $v$ . — Прим. ред.

$G$  — расщепляемое расширение группы  $N$ , или, что  $G$  — полуправильное произведение группы  $N$  и  $H$ .

Теорема 15.1.2. Расширение  $G = E[N, H, a^u, (u, v)]$  группы  $N$  расщепляемо тогда и только тогда, когда можно найти такую функцию  $\alpha(u) \in N$ ,  $u \in H$ , что

$$(u, v)\alpha(u)^v\alpha(v) = \alpha(uv)$$

для всех  $u, v \in H$ .

Доказательство. Если представители смежных классов выбраны так, что  $G = E(N, H, a^u, (u, v))$  — расщепляемое расширение  $N$ , то  $(u, v)^1 = 1$  и, полагая  $\bar{u} = u\alpha(u)$ , имеем

$$(u, v)\alpha(u)^v\alpha(v) = \alpha(uv). \quad (15.1.16)$$

Обратно, если существует такая функция  $\alpha(u)$ , что тождество (15.1.16) справедливо, то из условия  $a^{u^1} = \alpha(u)^{-1}a^u\alpha(u)$  определяем автоморфизмы  $a^{u^1}$ , соответствующие представителям  $\bar{u} = u\alpha(u)$ . Теперь расширение  $E[N, H, a^{u^1}, (u, v)^1] = G$  существует и эквивалентно расширению, для которого  $(u, v)^1 = 1$  для всех  $u, v \in H$ . Следовательно, оно расщепляемо.

## 15.2. Центральные расширения

Предположим, что все факторы  $(u, v)$  расширения группы  $A$  при помощи группы  $H$  лежат в центре  $B$  группы  $A$ . В этом случае говорят, что расширение  $E[A, H, a^u, (u, v)]$  — центральное расширение группы  $A$  при помощи группы  $H$ . Так, если  $A$  — абелева группа, то  $B = A$  и все расширения группы  $A$  — центральные расширения.

Для центральных расширений соотношение (15.1.5) принимает вид

$$(a^u)^v = a^{uv}. \quad (15.2.1)$$

Из этого равенства следует, что автоморфизмы  $a \rightarrow a^u$  группы  $A$  образуют группу, гомоморфную  $H$ . Пусть  $\chi$  — один из гомоморфизмов группы  $H$  в группу автоморфизмов группы  $A$ . Если заменить систему представителей  $\bar{u}$  при помощи функции  $\alpha(u)$  со значениями из центра  $B$ , то автоморфизмы при этом не изменятся. Следовательно, для таких расширений эти автоморфизмы не изменяются при переходе к другой системе представителей смежных классов по  $N$  и образуют группу, гомоморфную  $H$ . (Следуя Бэрю [1], будем называть их  $H$ - $\chi$ -расширениями.) Этим закончено рассмотрение условий (15.1.5) для случая центральных расширений, и нам нужно только рассмотреть условия (15.1.6):

$$(uv, w)(u, v)^w = (u, vw)(v, w). \quad (15.2.2)$$

Для эквивалентного расширения

$$(u, v)^1 = \alpha(uv)^{-1} (u, v) \alpha(u)^v \alpha(v), \quad (15.2.3)$$

где  $\alpha(u) \in B$ .

Если системы факторов  $(u, v)_1$  и  $(u, v)_2$  удовлетворяют требованию (15.2.2), то элементы  $(u, v)_3$ , определяемые как произведения.

$$(u, v)_3 = (u, v)_1 (u, v)_2, \quad u, v \in H, \quad (15.2.4)$$

также удовлетворяют требованию (15.2.2) и образуют систему факторов, определяющую некоторое  $H$ - $\chi$ -расширение группы  $A$ . При таком определении произведения систем факторов существует единичный элемент, а именно система факторов, состоящая из элементов  $(u, v) = 1$ , и обратный элемент — система факторов, состоящая из элементов  $(u, v)^{-1}$ . Более того, для эквивалентных систем факторов  $(u, v)_1^* \sim (u, v)_1$  и  $(u, v)_2^* \sim (u, v)_2$  имеем  $(u, v)_1^* (u, v)_2^* \sim \sim (u, v)_1 (u, v)_2$ . Следовательно, совокупность всех систем факторов  $H$ - $\chi$ -расширений группы  $A$  образует абелеву группу, даже если отождествлять эквивалентные системы факторов. Эту абелеву группу с отождествленными эквивалентными элементами будем называть *группой расширений*.

Если группа  $H$  конечна, определим функцию

$$f(v) = \prod_u (u, v). \quad (15.2.5)$$

Перемножая равенства (15.2.2) для всех  $u \in H$ , получаем

$$f(w) f(v)^w = f(vw) (v, w)^n, \quad (15.2.6)$$

где  $n$  — порядок группы  $H$ . Отсюда в силу формулы (15.2.3) имеем, что

$$(v, w)^n = 1. \quad (15.2.7)$$

Если  $m$  — число, кратное порядку любого элемента из  $B$ , то также

$$(v, w)^m = 1, \quad (15.2.8)$$

так как  $(u, v) \in B$ . Итак, доказана следующая теорема:

**Теорема 15.2.1.** *Порядок любого элемента группы расширений делит порядок группы  $H$ , а также наименьшее общее кратное порядков элементов группы  $B$ .*

**Следствие 15.2.1.** *Если  $m$  и  $n$  — взаимно простые числа, то все  $H$ - $\chi$ -расширения группы  $A$  эквивалентны полупрямому произведению  $A$  на  $H$ .*

Эту теорему мы используем при доказательстве теоремы 15.2.2 о расширениях, не обязательно центральных.

**Теорема 15.2.2.** Пусть  $G$  — группа конечного порядка  $m$ , содержащая инвариантную подгруппу  $K$  порядка  $t$  и обладающая фактор-группой  $H = G/K$  порядка  $n$ , причем числа  $t$  и  $n$  взаимно просты. Тогда расширение  $G$  группы  $K$  расщепляемо.

**Доказательство.** Достаточно показать, что группа  $G$  обладает подгруппой порядка  $n$ . Применим индукцию по  $m$ . Теорема тривиальна при  $m = 1$ . Пусть  $m > 1$  и  $p$  — простое число, которое делит  $m$ . Все силовские подгруппы  $S_p$  группы  $G$  содержатся в  $K$ , так как  $K$  — инвариантная подгруппа, содержащая по меньшей мере одну силовскую подгруппу  $S_p$ , а все силовские  $p$ -подгруппы сопряжены. Таким образом, число силовских подгрупп  $S_p$  в группе  $G$  равно их числу в группе  $K$ . Значит, в силу теоремы 1.6.1,  $[G : N_G(S_p)] = [K : N_K(S_p)]$ , откуда  $[N_G(S_p) : N_K(S_p)] = [G : K] = n$ , где  $N_G(S_p)$  и  $N_K(S_p)$  — нормализаторы подгруппы  $S_p$  соответственно в группах  $G$  и  $K$ . При этом, конечно,  $N_K(S_p) = N_G(S_p) \cap K$ , и по теореме 2.4.1  $N_K(S_p)$  — инвариантная подгруппа в  $N_G(S_p)$ . Если  $N_G(S_p)$  — собственная подгруппа группы  $G$ , то по предположению индукции она содержит подгруппу порядка  $n$ .

Поэтому мы можем предположить, что  $G = N_G(S_p)$  и, следовательно,  $K = N_K(S_p)$ . Если  $S_p$  — собственная подгруппа группы  $K$ , то по индукции группа  $G$  содержит подгруппу порядка  $[G : S_p]$ , изоморфную фактор-группе  $G/S_p$ , и, таким образом, подгруппу, изоморфную группе  $G/K$ , порядка  $n$ , что доказывает теорему в этом случае. Следовательно, осталось рассмотреть случай, когда  $K = S_p$ . Если группа  $S_p$  абелева, то  $G$  — ее центральное расширение, и в силу следствия из теоремы 15.2.1  $G$  — расщепляемое расширение группы  $S_p$ , и теорема доказана. Если группа  $S_p$  не абелева, то ее центр  $Z$  является собственной характеристической подгруппой, которая, следовательно, инвариантна в группе  $G$ . Теперь в силу предположения индукции группа  $G/Z$  содержит подгруппу  $U/Z$  порядка  $n$ . Но  $Z$  — инвариантная подгруппа индекса  $n$  в подгруппе  $U$  группы  $G$ , следовательно (опять по индукции) подгруппа  $U$  содержит подгруппу порядка  $n$ , и теорема полностью доказана.

### 15.3 Циклические расширения

Пусть  $H$  — циклическая группа конечного порядка  $m$ , порожденная элементом  $x$ . Пусть

$$1, x, x^2, \dots, x^{m-1} \quad (15.3.1)$$

— ее элементы. В расширении  $G$  группы  $N$  при помощи группы  $H$  выберем в качестве представителя смежного класса по  $N$ , соответствующего элементу  $x$ , некоторый элемент  $\bar{x}$  и возьмем в ка-

честве представителей классов, соответствующих элементам  $x^2, \dots, x^{m-1}$ , элементы  $\bar{x}^2, \dots, \bar{x}^{m-1}$  соответственно. Тогда

$$G = N + N\bar{x} + \dots + N\bar{x}^{m-1}. \quad (15.3.2)$$

При этом

$$\bar{x}^m = \alpha, \quad (15.3.3)$$

где  $\alpha$  — некоторый элемент из  $N$ . Отсюда для автоморфизма  $a \mapsto a^x$  группы  $N$  следует

$$a^{x^m} = \alpha^{-1}a\alpha, \quad \alpha \in N. \quad (15.3.4)$$

Кроме того, из тождества

$$\bar{x}^{-1}\bar{x}^m\bar{x} = \bar{x}^m \quad (15.3.5)$$

следует, что

$$\alpha^x = \alpha. \quad (15.3.6)$$

Покажем, что соотношения (15.3.4) и (15.3.6) полностью определяют расширение группы  $N$  при помощи  $H$ .

**Теорема 15.3.1.** *Пусть  $H$  — циклическая группа конечного порядка  $m$ . Тогда расширение  $G$  группы  $N$  при помощи группы  $H$  существует тогда и только тогда, когда существует автоморфизм  $a \mapsto a^x$  группы  $N$  и элемент  $\alpha \in N$  такие, что (1)  $m$ -я степень этого автоморфизма является внутренним автоморфизмом группы  $N$  с элементом  $\alpha$  в качестве трансформирующего элемента, и (2) этот автоморфизм на элемент  $\alpha$  действует тождественно.*

**Доказательство.** Как мы уже показали, если искомое расширение существует, то автоморфизм  $a \mapsto a^x$  и элемент  $\alpha$  удовлетворяют условиям (15.3.4) и (15.3.6). Теперь нужно доказать, что соотношений (15.3.4) и (15.3.6) достаточно для построения расширения. Группа  $H$  состоит из элементов  $x^i$ ,  $i = 0, 1, \dots, m-1$ . Определим автоморфизмы группы  $N$  и систему факторов следующим образом:

$$a^{x^0} = a, \quad a^{x^i} = a^{(x^{i-1})x}, \quad i = 1, \dots, m-2, \quad (15.3.7)$$

$$(x^i, x^j) = 1, \quad \text{если } i+j \leq m-1, \quad (15.3.8.1)$$

$$(x^i, x^j) = \alpha, \quad \text{если } m \leq i+j. \quad (15.3.8.2)$$

Легко проверить, что для них соотношения (15.1.5) и (15.1.6) выполняются, а, следовательно, по теореме 15.1.1 расширение вполне определено.

Если  $H$  — циклическая группа бесконечного порядка, можно положить  $(x^i, x^j) = 1$  для всех  $i$  и  $j$ ; а что касается автоморфизма  $a \mapsto a^x$ , то оказывается, что в этом случае на него не накладываются никакие ограничения. Это означает, что  $x^i = \bar{x}^i$  для всех  $i$ .

## 15.4. Определяющие отношения и расширения

В предыдущем параграфе мы видели, что в случае циклической группы  $H$  условия существования расширения группы  $N$  очень просты. Это соответствует простым определяющим отношениям в группе  $H$ . В этом параграфе мы увидим, как условия существования расширения при помощи некоторой группы  $H$  зависят от определяющих отношений группы  $H$  в самом общем случае.

Пусть группа  $H$  с образующими элементами  $x, y, z, \dots$  задана определяющими отношениями:

$$\varphi_i(x, y, z, \dots) = 1, \quad i = 1, 2, \dots, r.$$

Можно считать, что каждый элемент  $h \in H$  представлен определенным словом  $h = h(x, y, z, \dots)$  от образующих и обратных к ним элементов. Если  $G$  — расширение группы  $N$  при помощи  $H$ , то можно выбрать в качестве представителей смежных классов по  $N$  соответствующие слова от  $\bar{x}, \bar{y}, \bar{z}, \dots$  так, чтобы при гомоморфизме  $G \rightarrow H$

$$\bar{x} \rightarrow x, \quad h(\bar{x}, \bar{y}, \dots) \rightarrow h(x, y, \dots). \quad (15.4.2)$$

Пусть теперь  $F_1$  — свободная группа с образующими  $\bar{x}, \bar{y}, \bar{z}, \dots$ , соответствующими образующим  $x, y, z, \dots$  группы  $H$ . Тогда имеем гомоморфизмы

$$\begin{aligned} x &\rightarrow \bar{x} \rightarrow x, \\ y &\rightarrow \bar{y} \rightarrow y, \\ &\dots \end{aligned} \quad (15.4.3)$$

которые отображают

$$F_1 \rightarrow \bar{H} \rightarrow H, \quad (15.4.4)$$

где  $\bar{H}$  — подгруппа группы  $G$ , порожденная элементами  $\bar{x}, \bar{y}, \bar{z}, \dots$  и, следовательно, содержащая по меньшей мере по одному элементу из каждого смежного класса по  $N$ . Следовательно,  $G = \bar{H} \cup N$ . Поэтому если  $F_2$  — свободная группа, гомоморфным образом которой является группа  $N$ , то мы можем образовать свободную группу  $F = F_1 \cup F_2$  и определить гомоморфизмы

$$\begin{aligned} F &\rightarrow G \rightarrow H, \quad F = F_1 \cup F_2, \\ F_1 &\rightarrow \bar{H} \rightarrow H, \\ F_2 &\rightarrow N \rightarrow 1. \end{aligned} \quad (15.4.5)$$

Любой элемент  $\bar{h} \in \bar{H}$  индуцирует автоморфизм в группе  $N$ :

$$\bar{h}^{-1}a\bar{h} = a^h, \quad \bar{h} \in \bar{H}, \quad a \in N. \quad (15.4.6)$$

При отображении  $F_1 \rightarrow H$  мы имеем  $H = F_1/W$ , где  $W$  — наименьшая инвариантная подгруппа, содержащая элементы  $\varphi_i(\bar{x}, \bar{y}, \dots)$ . Следовательно, при отображении  $\bar{H} \rightarrow H$  элементы  $\varphi_i(\bar{x}, \bar{y}, \dots)$  переходят в единицу. Таким образом,

$$\varphi_i(\bar{x}, \bar{y}, \dots) = \alpha_i \in N. \quad (15.4.7)$$

В свободной группе  $F$  имеет место тождество

$$u_1 u_2 \dots u_r = z_1 z_2 \dots z_s,$$

если  $u$  и  $z$  — такие слова, для которых приведенные слова совпадают. При гомоморфизме  $F$  на  $G$  любое тождество сохраняется и подгруппы  $W$  и  $F_2$  отображаются в  $N$ . Так, из любого тождества относительно слов из инвариантной подгруппы, порожденной подгруппами  $W$  и  $F_2$ , при помощи соотношений (15.4.6) и (15.4.7) получаются условия, налагаемые на элементы  $\alpha_i$  и автоморфизмы  $a \not\sim a^h$ , которые можно интерпретировать как условия существования расширения  $G$  группы  $N$  при помощи  $H$ . Так как элемент  $\bar{u}\bar{v}^{-1}\bar{u}\bar{v}$  принадлежит пересечению  $N \cap \bar{H}$ , то он является образом в группе  $G$  элемента из  $W$ , т. е. произведением элементов, сопряженных с элементами вида  $\varphi_i(\bar{x}, \bar{y}, \dots) = \alpha_i$ . Следовательно, любой фактор  $(u, v) = \bar{u}\bar{v}^{-1}\bar{u}\bar{v}$  является образом в  $\bar{H}$  некоторого элемента из  $W$ , и если  $\bar{u} = h_1(\bar{x}, \bar{y}, \dots)$ ,  $\bar{v} = h_2(\bar{x}, \bar{y}, \dots)$ ,  $\bar{u}\bar{v} = h_3(\bar{x}, \bar{y}, \dots)$ , то фактор  $(u, v)$  является образом элемента

$$h_3(x, y, \dots)^{-1} h_1(x, y, \dots) h_2(x, y, \dots) \quad (15.4.8)$$

из  $W$ .

Условиями теоремы 15.1.1 являются тождества в свободной группе  $F$ , выраженные как условия, налагаемые на систему факторов и автоморфизмы согласно (15.4.6) и (15.4.7). Так, соотношение (15.1.5)

$$(a^u)^v = (u, v)^{-1} (a^{uv}) (u, v)$$

есть лишь видоизменение тождества

$$\bar{v}^{-1} (\bar{u}^{-1} a \bar{u}) \bar{v} = (\bar{u}\bar{v}^{-1}\bar{u}\bar{v})^{-1} (\bar{u}\bar{v}^{-1} a \bar{u}\bar{v}) (\bar{u}\bar{v}^{-1}\bar{u}\bar{v}) \quad (15.4.9)$$

при помощи равенства (15.4.6) и замены элементов из  $W$  элементами из  $N$ . Аналогично соотношение (15.1.6)

$$(uv, w)(u, v)^w = (u, vw)(v, w)$$

есть лишь видоизмененное тождество

$$(\bar{u}\bar{v}\bar{w}^{-1}\bar{u}\bar{v}\bar{w}) \bar{w}^{-1} (\bar{u}\bar{v}^{-1}\bar{u}\bar{v}) \bar{w} = (\bar{u}\bar{v}\bar{w}^{-1}\bar{u}\bar{v}\bar{w}) (\bar{v}\bar{w}^{-1}\bar{v}\bar{w}). \quad (15.4.10)$$

Таким образом, условия существования расширения группы  $N$  при помощи группы  $H$  являются лишь видоизменениями тождеств в группе  $F$ . Отметим, что определяющие отношения группы  $N$  в оба условия не входят. Эти условия можно рассматривать как данные для нахождения элементов  $\alpha_i \in N$  и автоморфизмов группы  $N$ , соответствующих определяющим отношениям группы  $H$ . Оба эти условия становятся тривиальными, если  $H$  — свободная группа, так как тогда в любом случае мы можем выбрать представители так, чтобы  $uv = \bar{u}\bar{v}$ , т. е. чтобы факторы были равны единице, и даже потребовать, чтобы автоморфизмы составляли группу.

На практике бывает трудно найти тождества в группе  $F$ , соответствующие условиям существования расширения. В следующем параграфе мы найдем их для центральных расширений группы  $N$  при помощи группы  $H$ .

## 15.5. Групповые кольца и центральные расширения<sup>1)</sup>

Рассмотрим центральное расширение группы  $N$  с центром  $C$  при помощи конечной группы  $H$ . Предположим, как и в § 15.2, что автоморфизмы удовлетворяют соотношению

$$(a^u)^v = a^{uv}. \quad (15.5.1)$$

Мы условились, что факторы  $(u, v) = \bar{u}\bar{v}^{-1}\bar{u}\bar{v}$  принадлежат  $C$ . Согласно лемме 7.2.2 (для правых смежных классов), эти элементы порождают такую подгруппу  $T$  группы  $\bar{H}$ , что  $\bar{H}/T = H$ . Но если

$$\varphi_i(x, y, \dots) = 1 \quad (15.5.2)$$

— определяющие отношения группы  $H$ , то

$$\varphi_i(\bar{x}, \bar{y}, \dots) = \alpha_i \in C, \quad (15.5.3)$$

так как очевидно, что элементы  $\alpha_i$  принадлежат подгруппе  $T$ , порожденной элементами из  $C$ .

Если  $r$  и  $s$  — эндоморфизмы группы  $C$ , то мы можем определить эндоморфизм  $r + s$ , положив

$$a^r a^s = a^{r+s}. \quad (15.5.4)$$

Таким образом, в силу (15.5.1) и (15.5.4) групповое кольцо  $H^*$  группы  $H$  можно рассматривать как кольцо операторов группы  $C$ . При этом групповое кольцо  $H^*$  состоит из элементов вида

$$c_1 h_1 + \dots + c_n h_n, \quad (15.5.5)$$

<sup>1)</sup> См. М. Холл [1].

где  $h_1, \dots, h_n$  — элементы из  $H$ , а  $c_1, \dots, c_n$  — целые числа. Сложение элементов из  $H^*$  производится покомпонентно, а умножение определяется умножением в  $H$ :  $h_i h_g = h_k$  и подчиняется обоим дистрибутивным законам. Легко проверить, что  $H^*$  — ассоциативное кольцо и что его единицей является единица группы  $H$ .

Будем говорить, что абелева группа  $A$  с кольцом операторов  $H^*$  *операторно свободна*, если она обладает таким базисом  $a_1, a_2, \dots, a_r$ , что любой элемент из  $A$  имеет вид

$$a = a_1^{z_1} a_2^{z_2} \dots a_r^{z_r}, \quad z_i \in H^*, \quad (15.5)$$

и такое представление единственно. Так, из  $a = 1$  следует, что  $z_1 = z_2 = \dots = z_r = 0$ .

**Теорема 15.5.1.** Единственным расширением  $G$  операторами свободной группы  $A$  при помощи конечной группы  $H$  является полуправильное произведение  $A$  на  $H$ .

*Доказательство.* Произвольный элемент  $b$  группы  $A$  однозначно записывается в виде

$$b = a_1^{z_1} a_2^{z_2} \dots a_r^{z_r}, \quad z_i \in H^*.$$

Если  $z_i = c_{i1} h_1 + \dots + c_{in} h_n$ ,  $i = 1, \dots, r$ , то положим

$$(b; h_j) = a_1^{c_{1j}} a_2^{c_{2j}} \dots a_r^{c_{rj}}.$$

Тогда при  $t = h_1, h_2, \dots, h_n$  элемент  $b$  имеет единственное представление

$$b = \prod_t (b; t)^t, \quad t = h_1, \dots, h_n. \quad (15.5.7)$$

Для системы факторов получаем теперь

$$(u, v) = \prod_t (u, v; t)^t, \quad (15.5.8)$$

и тождество (15.1.6) в силу однозначности представления (15.5.7) принимает вид

$$(uv, w; t)(u, v; tw^{-1}) = (u, vw; t)(v, w; t). \quad (15.5.9)$$

Если мы теперь положим  $\bar{u} = \bar{u} \prod_t (u, t^{-1}; 1)^{-t}$  для всех  $u \in H$ , то, пользуясь равенством (15.5.9), можно проверить, что

$$\bar{\bar{u}}\bar{v} = \bar{u}\bar{v}. \quad (15.5.10)$$

Таким образом, новые представители образуют группу, а  $G$  — полуправильное произведение групп  $A$  и  $H$ .

Согласно результатам §15.4, условиями существования центрального расширения группы  $N$  при помощи группы  $H$  являются условия (15.5.1) и условия вида

$$\prod_i \alpha_i^{u_i} = 1, \quad u_i \in H^*, \quad (15.5.11)$$

где  $\varphi_i(\bar{x}, \bar{y}, \dots) = \alpha_i$ , как и в равенстве (15.5.3). Теперь предположим, что  $N$  — операторно свободная группа. Мы знаем тогда, что значения  $\alpha_i = 1$ ,  $i=1, \dots, r$ , удовлетворяют равенству (15.5.11), а все другие решения (этого равенства) получаются другим выбором представителей в смежных классах. Если положить  $\bar{x} = \bar{\xi}x$ ,  $\bar{y} = \bar{\eta}y, \dots$ , то  $\varphi_i(\bar{\xi}x, \bar{\eta}y, \dots) = 1$ . Используя равенство

$$\bar{az} = \bar{z}\bar{a}z, \quad a \in N, \quad (15.5.12)$$

получаем

$$1 = \varphi_i(\bar{\xi}x, \bar{\eta}y, \dots) = \varphi_i(\bar{x}, \bar{y}, \dots) \bar{\xi}^x \bar{\eta}^y \dots \quad (15.5.13)$$

Таким образом, элементы  $\alpha_i^{-1} = \bar{\xi}^x \bar{\eta}^y \dots$  также удовлетворяют условию (15.5.11), так как эти значения получены изменением представителей в полупрямом произведении. Выбирая  $\xi, \eta, \dots$  в качестве независимых базисных элементов группы  $N$ , получаем следующие соотношения в кольце  $H^*$ :

$$\sum_i x_i u_i = 0, \quad \sum_i y_i u_i = 0, \dots, \quad i = 1, \dots, r. \quad (15.5.14)$$

Элементы  $x_i, y_i, \dots$  кольца  $H^*$  легко определить из соотношений  $\varphi_i(x, y, \dots) = 1$ , определяющих группу  $H$ , пользуясь тождеством (15.5.12). Следовательно, элементы  $u_i$  в равенстве (15.5.11) не произвольны, а подчинены условиям (15.5.14). Если мы сумеем доказать обратное утверждение, что элементы  $u_i$ , удовлетворяющие условиям (15.5.14), обращают в тождества соотношения (15.5.11), то мы тем самым сведем изучение условий (15.5.11) к решению уравнений (15.5.14). Дадим доказательство этого факта с помощью метода Магнуса [2].

**Теорема 15.5.2.** Для данных групп  $H$  и  $N$  условия существования центрального расширения группы  $N$  при помощи  $H$  следующие: 1) автоморфизмы  $a \mapsto a^h$ , соответствующие элементам из  $H$ , удовлетворяют условию (15.5.1), 2) существуют элементы  $\alpha_i$ , принадлежащие центру  $C$  группы  $N$ , для которых  $\varphi_i(\bar{x}, \bar{y}, \dots) = \alpha_i, i = 1, \dots, r$ , где  $\varphi_i(x, y, \dots) = 1$  — определяющие отношения группы  $H$ , и 3) элементы  $\alpha_i$  обладают свойством (15.5.11), где  $u_i$  — элементы, удовлетворяющие равенствам (15.5.14) в кольце  $H^*$ .

*Доказательство.* Ранее нами уже установлены все утверждения теоремы, кроме последнего, что любое множество элементов  $u_i$ , удовлетворяющих уравнениям (15.5.14), обладает свойством (15.5.11).

Рассмотрим (как и в § 15.4) свободную группу  $F_1$ , порожденную элементами  $x, y, \dots$ ; пусть  $H = F_1/W$ , где  $W$  — наименьшая инвариантная подгруппа, содержащая элементы  $\varphi_i(x, y, \dots)$ . Пусть  $W'$  — производная подгруппа группы  $W$ . Тогда  $W'$  — инвариантная подгруппа группы  $F_1$ , так как она является характеристической подгруппой инвариантной подгруппы  $W$ . Фактор-группа  $T = F_1/W'$  обладает следующими свойствами: (1) она порождается элементами  $x, y, \dots$ ; (2) она содержит такую инвариантную подгруппу  $V = W/W'$ , что  $T/V = H$ , и (3) группа  $V$  абелева. Наконец, ясно, что любая группа с этими свойствами является гомоморфным образом группы  $T$ , так как любая такая группа должна быть гомоморфным образом группы  $F_1$ , и при этом элементы подгруппы  $W'$  отображаются в единицу. Для доказательства теоремы мы воспользуемся леммой, доказательство которой приведем после доказательства теоремы.

**Лемма 15.5.1.** Пусть даны матрицы вида  $\begin{pmatrix} h & 0 \\ L & 1 \end{pmatrix}$ , где  $h \in H$ ,  $L$  — линейная форма от некоторого числа переменных с коэффициентами из  $H^*$ , которые умножаются согласно следующему правилу:

$$\begin{pmatrix} h_1 & 0 \\ L_1 & 1 \end{pmatrix} \begin{pmatrix} h_2 & 0 \\ L_2 & 1 \end{pmatrix} = \begin{pmatrix} h_1 h_2 & 0 \\ L_1 h_2 + L_2 & 1 \end{pmatrix}.$$

Тогда элементам  $x, y, \dots$  соответствуют матрицы вида  $\bar{x} = \begin{pmatrix} x & 0 \\ t_x & 1 \end{pmatrix}, \dots$ , и эти матрицы порождают группу, изоморфную группе  $T = F_1/W'$ .

Заметим, что, так как матрицы  $\begin{pmatrix} 1 & 0 \\ L & 1 \end{pmatrix}$  порождают аддитивную и тем самым абелеву группу, эта группа является, во всяком случае, гомоморфным образом группы  $T$ .

При центральном расширении  $\bar{H}$  — гомоморфный образ  $T$ . Следовательно, если соотношение

$$\varphi_i(\bar{x}, \bar{y}, \dots)^{u_i} = 1, \quad u_i \in H^*, \quad (15.5.15)$$

имеет место в группе  $T$ , то соответствующее равенство (15.5.11) выполняется в группе  $\bar{H}$ .

Предположим, что лемма уже доказана. Тогда мы имеем в  $T$  элементы подгруппы  $V$  следующего вида:

$$\varphi_i(\bar{x}, \bar{y}, \dots) = \begin{pmatrix} 1, & 0 \\ L_i, & 1 \end{pmatrix}, \quad i = 1, \dots, r, \quad (15.5.16)$$

где  $L_i$  — линейная форма от переменных  $t_x, t_y, \dots$  с коэффициентами из кольца  $H^*$ . Присоединим к подгруппе  $V$  элементы

$$\xi = \begin{pmatrix} 1, & 0 \\ t_\xi, & 1 \end{pmatrix}, \quad \eta = \begin{pmatrix} 1, & 0 \\ t_\eta, & 1 \end{pmatrix}, \dots, \quad (15.5.17)$$

где  $t_\xi, t_\eta, \dots$  — новые переменные. Пусть  $\bar{u}$  имеет то же значение, как и выше ( $u \in H$ ), тогда

$$\bar{u}^{-1} \xi \bar{u} = \begin{pmatrix} 1, & 0 \\ t_\xi u, & 1 \end{pmatrix}. \quad (15.5.18)$$

Таким образом, присоединив элементы вида (15.5.17) к подгруппе  $V$ , мы присоединили тем самым операторно свободную группу. Далее,

$$\xi \bar{x} = \begin{pmatrix} x, & 0 \\ t_\xi x + t_x, & 1 \end{pmatrix}. \quad (15.5.19)$$

После этого получаем  $\varphi_i(\xi \bar{x}, \eta \bar{y}, \dots)$  в виде (15.5.16), при этом в  $L_i$   $t_x$  заменяется на  $t_\xi x + t_x$  и т. д. Следовательно, из тождества

$$\varphi_i(\xi \bar{x}, \eta \bar{y}, \dots) = \varphi_i(\bar{x}, \bar{y}, \dots) \xi^x \eta^y \dots \quad (15.5.20)$$

и линейности формы  $L_i$  получаем

$$\xi^x \eta^y \dots = \begin{pmatrix} 1, & 0 \\ L_i(t_\xi x), & 1 \end{pmatrix}. \quad (15.5.21)$$

Поэтому если равенства (15.5.14) имеют место, то

$$\sum_i L_i(t_\xi x) u_i = 0. \quad (15.5.22)$$

Так как здесь  $t_\xi$  — символы, не связанные никакими соотношениями, отсюда следует, что

$$\sum_i L_i u_i = 0 \quad (15.5.23)$$

при любых аргументах линейных форм  $L_i$ . Применяя это соотношение к элементам (15.5.16), получаем

$$\prod_i \varphi_i(\bar{x}, \bar{y}, \dots)^{u_i} = 1. \quad (15.5.24)$$

Так как это равенство справедливо в группе  $T$ , оно справедливо также в  $\bar{H}$ , и, следовательно, мы показали, что  $\prod_i \alpha_i^{u_i} = 1$  в группе  $\bar{H}$ , как только имеют место равенства (15.5.14) в  $H^*$ . Следовательно, соотношение (15.5.11) является следствием соотношений (15.5.14), что и завершает доказательство теоремы. Осталось только доказать сформулированную выше лемму.

*Доказательство леммы.* Предположим, что в фактор-группе  $H = F_1/W$  представители смежных классов по подгруппе  $W$  выбраны так, что каждый из них является первым в своем классе относительно некоторого лексикографического упорядочения элементов свободной группы  $F_1$ . Тогда этот лексикографический порядок можно перенести на группу  $H$ : если  $h = h(x, y, \dots)$  — первый<sup>1)</sup> элемент смежного класса  $Wh$ , то будем считать  $h = h(x, y, \dots) \in H$  каноническим представлением элемента  $h$ . Таким образом, одно и то же слово может употребляться и для представления элемента из  $H$  и для соответствующего представления смежного класса по  $W$ . Мы можем, следовательно, говорить о длине элемента из  $H$  как о длине его канонического представления. Рассмотрим теперь отображения

$$\bar{x} \rightarrow \begin{pmatrix} x, & 0 \\ t_x, & 1 \end{pmatrix}, \quad \bar{y} \rightarrow \begin{pmatrix} y, & 0 \\ t_y, & 1 \end{pmatrix}, \dots,$$

где  $x, y$  — образующие группы  $H$ , и правило умножения матриц имеет вид

$$\begin{pmatrix} h_1, & 0 \\ L_1, & 1 \end{pmatrix} \begin{pmatrix} h_2, & 0 \\ L_2, & 1 \end{pmatrix} = \begin{pmatrix} h_1 h_2, & 0 \\ L_1 h_2 + L_2, & 1 \end{pmatrix}.$$

Здесь  $h_1, h_2 \in H$ , а  $L_1, L_2$  — линейные формы от символов  $t_x, t_y, \dots$  с коэффициентами из кольца  $H^*$ . Как отмечалось выше, группа  $K$ , порожденная этими матрицами, является, во всяком случае, гомоморфным образом группы  $T$ , так как отображение  $\begin{pmatrix} h, & 0 \\ L, & 1 \end{pmatrix} \rightarrow h$ , очевидно, является гомоморфизмом  $K$  на  $H$ , и ядро этого гомоморфизма состоит из элементов вида  $\begin{pmatrix} 1, & 0 \\ L, & 1 \end{pmatrix}$ , которые образуют аддитивную абелеву группу.

Согласно теореме 7.3.6,  $W$  — свободная подгруппа группы  $F_1$  со свободными образующими  $c_{ij}$

$$c_{ij} = h_i x h_j^{-1} \neq 1, \quad h_j = \varphi(h_i x), \quad (15.5.25)$$

где  $x$  — образующий группы  $F_1$ .

<sup>1)</sup> В смысле лексикографического порядка. — Прим. ред.

Более того, по лемме 7.2.3 слово  $h_i$  не может кончаться сомножителем  $x^{-1}$ , а слово  $h_j$  — сомножителем  $x$ . Группа  $W'$  порождается всеми коммутаторами элементов  $c_{ij}$ , а фактор-группа  $W/W'$  — свободная абелева группа с базисом  $c_{ij}$  по модулю  $W'$ . Если мы сможем показать, что элементы  $c_{ij}$ , соответствующие элементам  $\bar{h}_i x \bar{h}_j^{-1}$ , независимы в группе  $K$ , то из предыдущих утверждений мы получим, что  $K$  — точное представление группы  $T = F_1/W'$ . При отображении  $F_1 \rightarrow H$  имеем  $c_{ij} \rightarrow 1$ ,  $h_i \rightarrow h_i$ ,  $h_j \rightarrow h_j$  и  $x \rightarrow x$ . Поэтому в группе  $H$   $h_i x = h_j$ . Пусть теперь

$$\begin{aligned}\bar{h}_i &\rightarrow \begin{pmatrix} h_i & 0 \\ L(h_i) & 1 \end{pmatrix}, \quad \bar{x} \rightarrow \begin{pmatrix} x & 0 \\ t_x & 1 \end{pmatrix}, \\ \bar{h}_j &\rightarrow \begin{pmatrix} h_j & 0 \\ L(h_j) & 1 \end{pmatrix}.\end{aligned}$$

Тогда

$$\begin{aligned}\bar{c}_{ij} &\rightarrow \begin{pmatrix} h_i x h_j^{-1} & 0 \\ L(h_i) x h_j^{-1} + t_x h_j^{-1} - L(h_j) h_j^{-1} & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 0 \\ L(h_i) h_i^{-1} + t_x h_j^{-1} - L(h_j) h_j^{-1} & 1 \end{pmatrix}, \quad (15.5.26)\end{aligned}$$

так как  $h_i x = h_j$  в группе  $H$ .

Мы должны подробнее рассмотреть линейную форму  $L(h_i)$ , входящую в матрицу, соответствующую элементу  $\bar{h}_i$ . Пусть

$$\bar{x} \rightarrow \begin{pmatrix} x & 0 \\ t_x & 1 \end{pmatrix}, \quad \bar{x}^{-1} \rightarrow \begin{pmatrix} x^{-1} & 0 \\ -t_x x^{-1} & 1 \end{pmatrix}.$$

Положим  $q(a) = t_a$ , если  $a = x$  — образующий элемент, и  $q(a) = -t_{a^{-1}} a$ , если  $a^{-1} = x$  — образующий элемент. Если  $\bar{h} = a_1 a_2 \dots a_r$  — произвольное слово, где каждый элемент  $a_i$  — это один из элементов  $\bar{x}$ ,  $\bar{y}$ ,  $\dots$  или  $\bar{x}^{-1}$ ,  $\bar{y}^{-1}$ ,  $\dots$ , то имеем

$$\bar{h} \rightarrow \begin{pmatrix} h & 0 \\ L(h) & 1 \end{pmatrix},$$

где

$$L(h) = q(a_1) a_2 \dots a_r + q(a_2) a_3 \dots a_r + \dots + q(a_{r-1}) a_r + q(a_r), \quad (15.5.27)$$

здесь  $h = a_1 a_2 \dots a_r$ .

Это выражение для  $L(h)$  устанавливается индукцией по  $r$  при помощи правила перемножения матриц: Отметим, что из



формулы (15.5.27) вытекает следующее тождество:

$$L(h)h^{-1} = q(a_1)a_1^{-1} + q(a_2)a_2^{-1}a_1^{-1} + \dots + q(a_r)a_r^{-1}a_{r-1}^{-1} \dots a_1^{-1}. \quad (15.5.28)$$

Если элемент  $h$  представлен в канонической форме, то  $q(a_i)$  умножается здесь на элемент, обратный произведению  $a_1a_2 \dots a_i$ , который в силу шрейеровского свойства представителей смежных классов по  $W$  тоже представлен в каноническом виде. Таким образом, в качестве базиса группового кольца  $H^*$  удобно брать обратные элементы от канонических представлений элементов группы  $H$ .

Каждому образующему  $c_{ij}$  группы  $W$  однозначно соответствуют некоторые элементы  $h_j$  и  $x$ . Поэтому мы можем сопоставить элементу  $c_{ij}$  произведение  $t_x h_j^{-1}$ . Это выражение можно охарактеризовать тем, что слово  $h_j$  представлено канонически, а слово  $h_j x^{-1}$ , хоть и является редуцированным словом, не имеет канонического вида, так как равно каноническому представлению элемента  $h_i$ . Но в (15.5.23) линейная форма  $L(h_i)h_i^{-1} + t_x h_j^{-1} = L(h_j)h_j^{-1}$  не содержит других членов этого типа. Действительно, в силу свойств (15.5.25) другие слагаемые в произведении  $L(h_i)h_i^{-1}$  или  $L(h_j)h_j^{-1}$  имеют вид  $q(a_k)a_k^{-1} \dots a_1^{-1}$ , где  $a_1 \dots a_k$  — начальный отрезок слова  $h_i$  или  $h_j$ , и поэтому в силу шрейеровского свойства слов  $h$  слово  $a_1 \dots a_k$  само является каноническим представлением некоторого элемента  $h$ . Если  $a_k = y$  — образующий элемент, то  $q(a_k)a_k^{-1} \dots a_1^{-1} = t_y y^{-1} \dots a_1^{-1} = t_y h^{-1}$ , где слово  $h$  кончается элементом  $y$ , так что слово  $hy^{-1}$  редуцировано. Но если  $a_k = y^{-1}$ , где  $y$  — образующий элемент, то  $q(a_k)a_k^{-1} \dots a_1^{-1} = -ty \cdot a_{k-1}^{-1} \dots a_1^{-1} = -tyh^{-1}$ , где слово  $hy^{-1} = a_1 \dots a_k$  записано в каноническом виде. Таким образом, слагаемое  $t_x h_j^{-1}$  — единственный член такого типа в линейной форме, сопоставляемой элементу  $c_{ij}$ , причем различным элементам вида  $c_{ij}$  соответствуют различные такие члены. Следовательно, линейные формы  $L(c_{ij})$  линейно независимы, и элементы  $c_{ij}$  порождают свободную абелеву группу, которая, конечно, изоморфна группе  $W/W'$ . Поэтому группа  $K$ , порожденная матрицами, соответствующими элементам  $x, y, \dots$ , является точным представлением группы  $T = F_1/W'$ , и лемма доказана.

## 15.6. Двойные модули

Пусть  $\Omega$  — произвольная мультиликативная группа и  $A$  — двойной  $\Omega$ -модуль, т. е. аддитивная абелева группа, удовлетворяющая следующим условиям:

1) группа  $\Omega$  является одновременно группой левых и правых операторов, так что  $\xi a$  и  $a\xi$  — однозначно определенные элементы из  $A$  для  $a \in A$ ,  $\xi \in \Omega$ ;

2) дистрибутивность:

$$\xi(a_1 + a_2) = \xi a_1 + \xi a_2,$$

$$(a_1 + a_2)\xi = a_1\xi + a_2\xi,$$

откуда

$$\begin{aligned} \xi a &= \xi(-a), & -a\xi &= (-a)\xi, \\ \xi 0 &= 0\xi = 0; \end{aligned}$$

3)  $1a = a1 = a$ , где  $1$  — единица группы  $\Omega$ ;

4) ассоциативность:  $\xi(\eta a) = (\xi\eta)(a)$ ,  $(\xi a)\eta = \xi(a\eta)$ ,  $(a\xi)\eta = a(\xi\eta)$ .

Эти условия должны выполняться для любых элементов  $a$ ,  $a_1$ ,  $a_2 \in A$  и  $\xi, \eta \in \Omega$ .

По существу, двойной  $\Omega$ -модуль — это то же самое, что аддитивная абелева группа с элементами  $(\xi, \eta)$  группы  $\Omega \times \Omega$  в качестве дистрибутивных операторов.

В приложениях часто случается, что операторы из группы действуют тривиально с одной стороны, например, слева. Это означает, что  $\xi a = a$  для всех  $\xi \in \Omega$  и  $a \in A$ . В этом случае мы просто не будем учитывать левосторонние операторы. В таком случае назовем операторы односторонними.

Пусть, например,  $A$  — инвариантная абелева подгруппа некоторой группы  $G$ , а  $\Omega = G/A$ . Если  $\xi = Au_\xi$ , то элемент  $u_\xi^{-1}au_\xi$  зависит только от  $a$  и  $\xi$ , но не от выбора представителя  $u_\xi$ . Поэтому мы можем записать, что  $a^\xi = u_\xi^{-1}au_\xi$ . Это пример группы односторонних операторов, причем группа  $A$  записана также мультипликативно. В теории же когомологий удобнее пользоваться аддитивной записью группы  $A$ .

## 15.7. Коцепи, кограницы и группы когомологий<sup>1)</sup>

Пусть  $A$  — двойной  $\Omega$ -модуль. Определим группу  $C^n = C^n(A, \Omega)$  как аддитивную группу всех функций  $f$  от  $n$  переменных, пробегающих независимо друг от друга множество  $\Omega$ , со значениями в  $A$ , причем

$$f(\xi_1, \dots, \xi_n) = 0, \quad (15.7.1)$$

если хоть один из аргументов  $\xi_i$  равен 1. Элементы группы  $C^n$  называются *n-мерными коцепиями*.  $C^0 = A$ , по определению, и 0-мерной коцепией является просто произвольный элемент из  $A$ .

<sup>1)</sup> См. Эйленберг, Маклейн [1, 2] и Маклейн [2] (см. также Боревич и Фаддеев [1]. — Прим. перев.).

*Кограничный оператор*  $\delta$  отображает каждую группу  $C^n$  в следующую группу  $C^{n+1}$  по правилу:

$$\begin{aligned} (\delta f)(\xi_0, \xi_1, \dots, \xi_n) &= \xi_0 f(\xi_1, \dots, \xi_n) + \\ &+ \sum_{t=1}^n (-1)^t f(\xi_0, \xi_1, \dots, \xi_{t-2}, \xi_{t-1}\xi_t, \xi_{t+1}, \dots, \xi_n) + \\ &+ f(\xi_0, \xi_1, \dots, \xi_{n-1}) \xi_n. \end{aligned} \quad (15.7.2)$$

Здесь  $f \in C^n$  и, очевидно,  $\delta f \in C^{n+1}$ . Отображение  $f \rightarrow \delta f$  является гомоморфизмом по отношению к операции сложения. Действительно полезными в теории групп оказываются только случаи  $n = 0, 1, 2$ . В этих случаях оператор  $\delta$  кограницы определяется следующими формулами:

$$\begin{aligned} (\delta f)(\xi) &= \xi f - f\xi = \xi a - a\xi, \text{ так как } f = a \in A, \\ (\delta f)(\xi, \eta) &= \xi f(\eta) - f(\xi\eta) + f(\xi)\eta, \\ (\delta f)(\xi, \eta, \zeta) &= \xi f(\eta, \zeta) - f(\xi\eta, \zeta) + f(\xi, \eta\zeta) - f(\xi, \eta)\zeta. \end{aligned} \quad (15.7.3)$$

**Теорема 15.7.1.** *Если  $f$  — произвольная коцепь, то  $\delta^2 f = 0$ .*

*Доказательство.* Пусть  $f \in C^{n-2}$ . Тогда  $\delta f \in C^{n-1}$ . Поэтому, когда мы, пользуясь определениями, выражаем  $(\delta^2 f)(\xi_1, \xi_2, \dots, \xi_n)$  как сумму значений  $\delta f$ , то получаем  $n+1$  слагаемых с чередующимися знаками:

$$u_0 - u_1 + u_2 - \dots + (-1)^n u_n.$$

Каждый элемент  $u_i$  в свою очередь представляется знакопеременной суммой  $n$  значений функции  $f$ :

$$\begin{aligned} u_i &= u_{i0} - u_{i1} + \dots + (-1)^{i-1} u_{i, i-1} + (-1)^i u_{i, i+1} + \dots \\ &\quad \dots + (-1)^{i+j-1} u_{i, i+j} + \dots \end{aligned}$$

Следовательно,

$$\delta^2 f(\xi_1, \dots, \xi_n) = \sum_{i < j} (-1)^{i+j-1} u_{ij} + \sum_{i > j} (-1)^{i+j} u_{ij},$$

где числа  $i$  и  $j$  пробегают значения от 1 до  $n$ . Но, как легко проверить,  $u_{ij} = u_{ji}$  для всех  $i$  и  $j$ , и указанная выше сумма равна нулю.

Если  $f \in C^n$  и  $\delta f = 0$ , то элемент  $f$  называется *n-мерным коциклом*. Эти коциклы образуют ядро  $Z^n = Z^n(A, \Omega)$  гомоморфизма группы  $C^n$  в  $C^{n+1}$ , индуцируемого отображением  $\delta$ .

Если  $f \in C^n$  и существует такой элемент  $g \in C^{n-1}$ , что  $\delta g = f$ , то элемент  $f$  называется *n-мерной кограницей*. Эти кограницы составляют образ  $B^n = B^n(A, \Omega)$  группы  $C^{n-1}$  при отображении  $\delta$ . По определению,  $B^0 = 0$ .

Согласно теореме, каждая кограница есть коцикл, так что  $B^n \subseteq Z^n$  для всех  $n$ . Фактор-группа  $Z^n/B^n$  называется  $n$ -мерной группой когомологий двойного  $\Omega$ -модуля  $A$  и обозначается

$$H^n(A, \Omega) = Z^n/B^n.$$

При определении коцепей  $f(\xi_1, \dots, \xi_n)$  мы наложили на них требование (15.7.1), согласно которому коцель равна нулю, если хоть один из аргументов равен единице. Во многих случаях такое ограничение желательно, как, например, в применении к фактор-системам, о которых шла речь выше. Назовем такие коцепи *нормализованными*. Если же ограничение (15.7.1) не вводится, говорят о *ненормализованных коцепях*. Теорема 15.7.1 справедлива, конечно, в обоих случаях, так как в ней ограничение 15.7.1 не использовалось. По сути же различие нормализованных и ненормализованных коцепей вводится исключительно для удобства, так как мы покажем, что группы когомологий любой размерности для ненормализованных коцепей изоморфны соответствующим группам для нормализованных.

**Теорема 15.7.2.** *Группы когомологий  $H^n(A, \Omega)$  любой размерности  $n$  для ненормализованных коцепей изоморфны соответствующим группам для нормализованных коцепей.*

*Доказательство.* Обозначим группы нормализованных коцепей, кограницы и коциклы размерности  $n$  соответственно через  $C^n, B^n, Z^n$ , а для ненормализованного случая — через  $C'^n, B'^n, Z'^n$ .

Для  $n=0$  и  $n=1$  легко проверить, что  $B^0=B'^0=0$ ,  $Z^0=Z'^0$  и  $B^1=B'^1$ ,  $Z^1=Z'^1$ , откуда группы  $H^0(A, \Omega)$  и  $H^1(A, \Omega)$  в обоих случаях одни и те же. При этом только надо проверить, что при  $f(\xi) \in Z'^1$   $\xi f(\eta) - f(\xi\eta) + f(\xi)\eta = 0$ , откуда, полагая  $\xi=\eta=1$ , находим  $f(1)=0$ , т. е. функция  $f(\xi)$  нормализована, и поэтому  $Z'^1=Z^1$ .

Предположим теперь, что  $n > 1$ . Ясно, что  $B^n \subseteq B'^n$  и  $Z^n \subseteq Z'^n$ . Поэтому класс когомологий для  $C^n$ , т. е. смежный класс по  $B^n$  в группе  $C^n$  соответствует одному единственному классу когомологий для  $C'^n$ , именно классу по подгруппе  $B'^n$ , который его содержит. Это соответствие является, конечно, гомоморфизмом группы  $H^n(A, \Omega)$  в группу  $H'^n(A, \Omega)$ . Чтобы установить изоморфизм, мы должны показать, что это взаимно однозначные соответствия на всю группу  $H'^n(A, \Omega)$ . Для этого нам понадобятся две леммы. Будем говорить, что две коцепи *когомологичны*, если их разность есть кограница. Так, два коцикла когомологичны, если они принадлежат одному классу когомологий.

**Лемма 15.7.1.** *Любой ненормализованный коцикл когомологичен нормализованному коциклу.*

**Лемма 15.7.2.** *Если кограница некоторой коцепи нормализована, то она является кограницей некоторой нормализованной коцепи.*

**Доказательство леммы.** Будем говорить, что коцепь  $f(x_1, \dots, x_n)$   $l$ -нормализована,  $i = 0, \dots, n$ , когда она обращается в нуль, как только один из первых  $l$  аргументов равен единице.  $0$ -нормализованная коцепь — это ненормализованная коцепь из  $C^n$ , а  $n$ -нормализованная цепь — это нормализованная коцепь из  $C^n$ . Для коцепи  $f(x_1, \dots, x_n)$  определим рекуррентно следующие коцепи:

$$f = f_0, \quad f_{i+1} = f_i - \delta g_{i+1}, \quad i = 0, \dots, n-1, \quad (15.7.4)$$

где

$$g_{i+1}(x_1, \dots, x_{n-1}) = (-1)^i f_i(x_1, \dots, x_i, 1, x_{i+1}, \dots, x_{n-1}). \quad (15.7.5)$$

Заметим, что коцепи  $f = f_0$  и  $f_n$  отличаются на кограницу и что в силу равенства  $\delta f_i = \delta f_{i+1}$  коцепи  $f = f_0, f_1, \dots, f_n$  обладают одной и той же кограницей  $\delta f$ .

**Лемма 15.7.3.** *Если кограница  $\delta f$  нормализована, то коцепь  $f_l$   $l$ -нормализована.*

Этим будут доказаны обе предыдущие леммы. Действительно, отсюда следует лемма 15.7.1, так как для ненормализованного коцикла  $f$  имеем  $\delta f = 0$ . Следовательно,  $\delta f$ , как  $(n+1)$ -мерная коцепь, нормализована тривиально, откуда, согласно лемме, коцепь  $f_n$ , когомологичная коцепи  $f_0 = f$ , является нормализованным коциклом. Отсюда же следует лемма 15.7.2. Действительно, если  $g = \delta f \in C^{n+1}$  — нормализованная кограница, то  $g = \delta f_0 = \dots = \delta f_n$  и, согласно лемме, коцепь  $f_n$  нормализована.

Докажем лемму 15.7.3 индукцией по  $i$ . Для  $i = 0$  утверждение очевидно. Пусть лемма верна для  $i$ . Докажем, что она верна для  $i+1$ , т. е. что

$$f_{i+1}(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_n) = 0. \quad (15.7.6)$$

Из определения (15.7.4) функции  $f_{i+1}$  имеем

$$\begin{aligned} f_{i+1}(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_n) &= \\ &= f_i(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_n) - \\ &- x_1 g_{i+1}(x_2, \dots, x_i, 1, x_{i+2}, \dots, x_n) + \\ &+ \sum_{j=1}^{i-1} (-1)^{j-1} g_{i+1}(x_1, \dots, x_j x_{j+1}, \dots, x_i, 1, x_{i+2}, \dots, x_n) + \end{aligned}$$

$$\begin{aligned}
 & + (-1)^{i-1} g_{i+1}(x_1, \dots, x_{i-1}, x_i \cdot 1, x_{i+2}, \dots, x_n) + \\
 & + (-1)^i g_{i+1}(x_1, \dots, x_i, 1 \cdot x_{i+2}, \dots, x_n) + \\
 & + \sum_{j=i+2}^{n-1} (-1)^{j-1} g_{i+1}(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_j x_{j+1}, \dots, x_n) + \\
 & + (-1)^n g_{i+1}(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_{n-1}) x_n. \quad (15.7.7)
 \end{aligned}$$

Так как по индукции коцель  $f_i$   $i$ -нормализована, коцель  $g_{i+1}$  вида (15.7.5) также  $i$ -нормализована. Это означает, что в сумме (15.7.7) второе слагаемое с множителем  $x_1$  слева и сумма по  $j$  от 1 до  $i-1$  равны нулю. Следующие два слагаемых взаимно уничтожаются. Заменив в оставшихся слагаемых коцели  $g_{i+1}$  их значениями (15.7.5), получаем

$$\begin{aligned}
 f_{i+1}(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_n) & = \\
 & = f_i(x_1, \dots, x_i, 1, x_{i+2}, \dots, x_n) + \\
 & + \sum_{j=i+2}^{n-1} (-1)^{i+j} f_i(x_1, \dots, x_i, 1, 1, x_{i+2}, \dots, x_j x_{j+1}, \dots, x_n) + \\
 & + (-1)^{n+i} f_i(x_1, \dots, x_i, 1, 1, x_{i+2}, \dots, x_{n-1}) x_n. \quad (15.7.8)
 \end{aligned}$$

Но по условию коцель  $\delta f_i = \delta f$  нормализована, откуда

$$(-1)^{i+1} \delta f(x_1, \dots, x_i, 1, 1, x_{i+2}, \dots, x_n) = 0. \quad (15.7.9)$$

По предположению индукции, коцель  $f_i$   $i$ -нормализована, поэтому правая часть равенства (15.7.8) состоит из всех не равных нулю слагаемых выражения (15.7.9), разложенного в сумму по определению оператора  $\delta$ . Таким образом,

$$f_{i+1}(x_1, x_2, \dots, x_i, 1, x_{i+2}, \dots, x_n) = 0. \quad (15.7.10)$$

Этим по индукции доказана лемма 15.7.3, из которой, как мы видели, следуют леммы 15.7.1 и 15.7.2, а из них — теорема.

## 15.8. Применение когомологии к теории расширений

Пусть  $A$  — инвариантная абелева подгруппа некоторой группы  $G$  и  $\Omega = G/A$  — фактор-группа  $G$  по  $A$ . Если смежный класс  $Au_\xi = \xi$  — элемент из  $\Omega$ , то при  $a \in A$  произведение  $u_\xi^{-1}au_\xi$  зависит только от  $a$  и  $\xi$  и не зависит от выбора представителя  $u_\xi$  смежного класса  $\xi$ . Поэтому равенство  $u_\xi^{-1}au_\xi = a\xi$  имеет вполне определенный смысл. Таким образом,  $\Omega$  является группой правых операторов группы  $A$ , причем будем полагать, что элементы группы  $\Omega$

слева действуют тривиально. Предположим, что группа  $A$  — аддитивная группа с фиксированной группой операторов  $\Omega$ , и положим для системы факторов  $f(u, v) = (u, v)$ , тогда условия (15.2.2) перепишутся в виде

$$f(uv, w) + f(u, v)w = f(u, vw) + f(v, w). \quad (15.8.1)$$

Переставим слагаемые следующим образом:

$$f(v, w) - f(uv, w) + f(u, vw) - f(u, v)w = 0. \quad (15.8.2)$$

Тогда видно, что система факторов представляет собой коцикл размерности два. Из соотношения (15.2.3) получаем следующее условие эквивалентности двух систем факторов  $f(u, v)$  и  $f_1(u, v)$ :

$$f_1(u, v) = f(u, v) + f(v) - f(uv) + f(u)v, \quad (15.8.3)$$

т. е. коцепи  $f_1$  и  $f$  отличаются на кограницу  $f(v) - f(uv) + f(u)v$ . Напомним, что группа операторов  $\Omega$  действует слева тождественно. Итак, группа расширений является второй группой когомологий  $H^2(A, \Omega)$ . Сформулируем этот результат в виде теоремы.

**Теорема 15.8.1.** *Группа расширений абелевой группы  $A$  при помощи группы  $\Omega$  есть вторая группа когомологий  $H^2(A, \Omega)$ , где*

- 1) группа  $\Omega$  действует на  $A$  слева тривиально;
- 2) справа группа  $\Omega$  действует на  $A$  как группа автоморфизмов;
- 3) системы факторов  $f(u, v)$  являются коциклами из  $Z^2$ ;
- 4) эквивалентные системы факторов отличаются на кограницы из  $B^2$ .

Выбор единицы в качестве представителя смежного класса  $A$  группы  $G$  по подгруппе  $A$  приводит к нормализации коцикла  $f(u, v) : f(1, 1) = 0$ . Полагая  $u = v = 1$  в соотношении (15.8.1), получаем

$$f(1, w) + f(1, 1)w = f(1, w) + f(1, w), \quad (15.8.4)$$

откуда

$$f(1, w) = 0. \quad (15.8.5)$$

Аналогично, полагая  $v = w = 1$ , получаем

$$f(1, 1) - f(u, 1) + f(u, 1) - f(u, 1) = 0, \quad (15.8.6)$$

откуда

$$f(u, 1) = 0; \quad (15.8.7)$$

последнее означает, что мы имеем дело с нормализованными коциклами.

Докажем одну общую теорему о когомологии, включающую теорему 15.2.1 как частный случай.

Пусть  $\Omega$  — конечная группа порядка  $m$ . Тогда для каждого  $n > 0$  можно определить аддитивный гомоморфизм  $\sigma$ , отображающий  $C^n$  в  $C^{n-1}$  по формуле

$$(\sigma f)(x_2, \dots, x_n) = \sum_{x \in \Omega} x^{-1}f(x, x_2, \dots, x_n). \quad (15.8.8)$$

Ясно, что здесь  $f \in C^n$  и  $\sigma f \in C^{n-1}$ . Положим  $g = \sigma f$  и распишем выражение  $(\delta g)(x_1, \dots, x_n)$ :

$$\begin{aligned} \delta g(x_1, \dots, x_n) = & x_1 \sum x^{-1}f(x, x_2, \dots, x_n) - \\ & - \sum x^{-1}f(x, x_1x_2, \dots, x_n) + \\ & + \dots \dots \dots \dots + \\ & + (-1)^{j-1} \sum x^{-1}f(x, x_1, \dots, x_{j-1}x_j, \dots, x_n) + \\ & + \dots \dots \dots \dots \dots \dots + \\ & + (-1)^{n-1} \sum x^{-1}f(x, x_1, \dots, x_{n-1}x_n) + \\ & + (-1)^n [\sum x^{-1}f(x, x_1, \dots, x_{n-1})] x_n; \end{aligned} \quad (15.8.9)$$

здесь везде суммирование проводится по всем  $x \in \Omega$ .

Рассмотрим  $(\delta f)(x, x_1, \dots, x_n)$ :

$$\begin{aligned} (\delta f)(x, x_1, \dots, x_n) = & xf(x_1, \dots, x_n) - \\ & - f(x \cdot x_1, x_2, \dots, x_n) + \\ & + f(x, x_1 \cdot x_2, \dots, x_n) + \\ & + \dots \dots \dots \dots + \\ & + (-1)^n f(x, x_1, \dots, x_{n-1}x_n) + \\ & + (-1)^{n+1} f(x, x_1, \dots, x_{n-1}) x_n. \end{aligned} \quad (15.8.10)$$

Теперь, используя формулу (15.8.10), вычисляем

$$\begin{aligned} \sigma(\delta f)(x_1, \dots, x_n) = & \sum_{x \in \Omega} x^{-1}(\delta f)(x, x_1, \dots, x_n) = \\ = & mf(x_1, \dots, x_n) - \\ & - \sum x^{-1}f(xx_1, x_2, \dots, x_n) + \\ & + \sum x^{-1}f(x, x_1 \cdot x_2, \dots, x_n) + \\ & + \dots \dots \dots \dots + \\ & + (-1)^n \sum x^{-1}f(x, x_1, \dots, x_{n-1}x_n) + \\ & + (-1)^{n+1} \sum x^{-1}f(x, x_1, \dots, x_{n-1}) x_n. \end{aligned} \quad (15.8.11)$$

В сумме  $S = \sum x^{-1}f(xx_1, x_2, \dots, x_n)$  положим  $y = xx_1$ . Тогда  $S = x_1 \sum y^{-1}f(y, x_2, \dots, x_n) = x_1 \sigma f(x_2, \dots, x_n)$ ,

так как при фиксированном  $x_1 \in \Omega$  элемент  $y$  пробегает всю группу  $\Omega$ . Поэтому равенство (15.8.11) эквивалентно следующему:

$$\sigma(\delta f) = mf - \delta(\sigma f). \quad (15.8.12)$$

Таким образом, справедлива

**Теорема 15.8.2.** *Если  $f \in C^n$ , то  $\sigma(\delta f) + \delta(\sigma f) = mf$ .*

**Следствие 15.8.1.** *Если  $f \in Z^n$ , то  $mf \in B^n$ .*

Действительно,  $f \in Z^n$  равносильно тому, что  $\delta f = 0$ , поэтому  $mf$  — кограница для  $\sigma f$ . Отсюда делаем следующий вывод. *Если порядок группы  $\Omega$  равен  $m$ , то порядок любого элемента группы когомологий  $H^n = Z^n/B^n$  делит  $m$ .* Теперь теорема 15.2.1 получается как следствие при  $n = 2$ .

Известен дальнейший результат о системах факторов, принадлежащий Гашюцу [1], а в более общей форме — Экману [1]. Он относится к когомологии группы  $\Omega$  и подгруппы  $B$ . Предположим, что  $B$  — подгруппа конечного индекса  $m$  в группе  $\Omega$ . Тогда

$$\Omega = B \cdot 1 + Bs_2 + \dots + Bs_m, s_1 = 1. \quad (15.8.13)$$

Если  $a_1, a_2, \dots, a_n$  — элементы из  $\Omega$ , то будем писать  $s_i a_1 = s_{i1}$ , а черта над элементом, как обычно, будет означать, что берется представитель соответствующего ему смежного класса. Кроме этого, введем обозначения

$$\overline{s_{i1} a_2} = s_{i2}, \dots, \overline{s_{i, n-1} a_n} = s_{in}.$$

Определим *перемещение*  $T(f(a_1, \dots, a_n))$  элемента  $f(a_1, a_2, \dots, a_n) \in C^n$  следующей формулой:

$$T(f(a_1, \dots, a_n)) = \sum_{i=1}^m s_i^{-1} f(s_i a_1 s_{i1}^{-1}, s_{i1} a_2 s_{i2}^{-1}, \dots, s_{i, n-1} a_n s_{in}^{-1}) s_{in}. \quad (15.8.14)$$

Заметим, что во всех случаях  $s_{i, j-1} a_j s_{ij}^{-1} \in B$ , откуда для элемента  $f \in C^n(A, \Omega)$  перемещение  $Tf$  содержится в подгруппе  $\Omega C^n(A, B) \Omega$ .

**Теорема 15.8.3.** (Теорема Гашюца.) *Если  $f(a_1, \dots, a_n) \in Z^n$  и  $B$  — подгруппа группы  $\Omega$  индекса  $m$ , то*

$$Tf(a_1, \dots, a_n) \equiv mf(a_1, \dots, a_n) (\text{mod } B^n).$$

**Следствие 15.8.2.** *Класс когомологий перемещения не зависит от выбора представителей смежных классов  $s_i$  в разложении (15.8.13).*

*Доказательство теоремы.* Рассмотрим сумму

$$\begin{aligned}
 & \sum_{i=1}^m (\delta f)(s_i^{-1}, s_i a_1 s_{i1}^{-1}, \dots, s_{i,n-1} a_n s_{in}^{-1}) s_{in} - \\
 & - \sum_{i=1}^m (\delta f)(a_1, s_{i1}^{-1}, s_{i1} a_2 s_{i2}^{-1}, \dots, s_{i,n-1} a_n s_{in}^{-1}) s_{in} + \\
 & + \dots \dots \dots \dots \dots \dots \dots \dots + \\
 & + (-1)^{j-1} \sum_{i=1}^m (\delta f)(a_1, \dots, a_{j-1}, s_{ij}^{-1}, s_{i,j-1} a_j s_{ij}^{-1}, \dots) s_{in} + \\
 & + (-1)^j \sum_{i=1}^m (\delta f)(a_1, \dots, a_{j-1}, a_j, s_{ij}^{-1}, s_{ij} a_{j+1} s_{i,j+1}^{-1}, \dots) s_{in} + \\
 & + \dots \dots \dots \dots \dots \dots \dots \dots + \\
 & + (-1)^n \sum_{i=1}^m (\delta f)(a_1, \dots, a_n, s_{in}^{-1}) s_{in} = 0. \tag{15.8.15}
 \end{aligned}$$

В этой сумме каждое слагаемое равно нулю, так как  $f \in Z^n$ , поэтому  $\delta f = 0$ . Распишем каждую слагаемую здесь кограницу и просуммируем в каждой из  $n+1$  строк все члены кограниц по  $i$  от 1 до  $m$ . Тогда первые члены первой строки дадут сумму

$$\sum s_i^{-1} f(s_i a_1 s_{i1}^{-1}, \dots, s_{i,n-1} a_n s_{in}^{-1}) s_{in} = Tf(a_1, \dots, a_n). \tag{15.8.16}$$

Последние члены последней строки образуют сумму

$$\begin{aligned}
 (-1)^n (-1)^{n+1} \sum f(a_1, \dots, a_n) s_{in}^{-1} \cdot s_{in} = - \\
 = -mf(a_1, \dots, a_n). \tag{15.8.17}
 \end{aligned}$$

Так как  $s_{i,j-1}^{-1} \cdot s_{i,j-1} a_j s_{ij}^{-1} = a_j \cdot s_{ij}^{-1}$ ,  $(j+1)$ -ые члены  $j$ -й и  $(j+1)$ -й строк взаимно уничтожаются при  $j = 1, \dots, n$ . Возьмем теперь первые  $j$  членов  $(j+1)$ -й строки и члены  $j+2, \dots, n+2$   $j$ -й строки:

$$\begin{aligned}
 & (-1)^j a_1 \sum_{i=1}^m f(a_2, \dots, a_j, s_{ij}^{-1}, s_{ij} a_{i,j+1} s_{i,j+1}^{-1}, \dots) s_{in} + \\
 & + (-1)^{j+1} \sum_{i=1}^m f(a_1 a_2, \dots, a_j, s_{ij}^{-1}, s_{ij} a_{i,j+1} s_{i,j+1}^{-1}, \dots) s_{in} + \\
 & + \dots \dots \dots \dots \dots \dots \dots \dots + \\
 & + (-1)^{2j} \sum_{i=1}^m f(a_1, \dots, a_{j-1} a_j, s_{ij}^{-1}, s_{ij} a_{i,j+1} s_{i,j+1}^{-1}, \dots) s_{in} + \\
 & + (-1)^{2j+1} \sum_{i=1}^m f(a_1, \dots, a_{j-1}, s_{i,j-1}^{-1}, s_{i,j-1} a_{ij} s_{ij}^{-1}, \dots) s_{in} + \\
 & + \dots \dots \dots \dots \dots \dots \dots \dots + \\
 & + (-1)^{n+j+1} \sum_{i=1}^m f(a_1, \dots, a_{j-1}, s_{i,j-1}^{-1}, s_{i,j-1} a_{ij} s_{ij}^{-1}, \dots) s_{i,n-1} a_n. \tag{15.8.18}
 \end{aligned}$$

Если для аргументов  $u_1, \dots, u_{n-1}$ , мы определим функцию  $F_j(u_1, \dots, u_{n-1}) \in C^{n-1}$  по формуле

$$F_j(u_1, \dots, u_{n-1}) = \sum_{i=1}^m f(u_1, \dots, u_{j-1}, \sigma_i^{-1}, \sigma_i u_j \sigma_i^{-1}, \dots, \sigma_{i, n-1} u_{n-1} \sigma_{in}^{-1}) \sigma_{in}, \quad (15.8.19)$$

где  $\sigma_i = s_i$  и рекуррентно  $\sigma_{it} = \overline{\sigma_{i, t-1} u_t}$ , то слагаемые суммы (15.8.18) являются кограницами  $(-1)^j (\delta F_j)(a_1, \dots, a_n)$ , так как при суммировании по  $i$  элементы  $s_{ij}$  или  $s_{i, j-1}$  могут служить в качестве  $\sigma_i$ . Если  $j$  пробегает значения от 1 до  $n$ , то кограницы  $(-1)^j (\delta F_j)(a_1, \dots, a_n)$  охватывают все слагаемые суммы (15.8.15), кроме уничтожающихся и входящих в суммы (15.8.16) и (15.8.17). Этим теорема доказана.

Теоретико-групповой формой теоремы Гашюца является

**Теорема 15.8.4.** (Теорема Гашюца.) Пусть  $F = [(u, v)]$ ,  $u, v \in H$ ,  $(u, v) \in A$  — система факторов  $H\chi$ -расширения абелевой группы  $A$  при помощи конечной группы  $H$ . Пусть  $B$  — подгруппа группы  $H$  индекса  $m$  и

$$H = B \cdot 1 + Bs_2 + \dots + Bs_m, \quad s_1 = 1.$$

Тогда

$$(u, v)^m \sim \prod_{i=1}^m (s_i u s_i \overline{u}^{-1}, \overline{s_i u v s_i \overline{u} \overline{v}}^{-1})^{\overline{s_i u v}}.$$

Здесь аргументы  $s_i u s_i \overline{u}^{-1}$  и  $\overline{s_i u v s_i \overline{u} \overline{v}}^{-1}$ , конечно, элементы из подгруппы  $B$ .

**Следствие 15.8.3.** Если  $(x, y) = 1$  для  $x, y \in B$ , то  $(u, v)^m \sim 1$ .

Существует еще много следствий этой теоремы, но особенно полезно следствие, связывающее  $H\chi$ -расширения группы  $A$  и  $S(p)\chi$ -расширения группы  $A$ , где  $S(p)$  — силовская  $p$ -подгруппа группы  $H$ . Пусть порядок  $H$  равен  $n = p^e m$ , а порядок подгруппы  $S(p)$  равен  $p^e$ . Пусть  $E = E(H)$  — группа  $H\chi$ -расширений группы  $A$ , определенная в § 15.2. Каждый ее элемент — это класс эквивалентных систем факторов  $F_i [(u, v)_i]$ . По теореме 15.2.1 порядок любого элемента из  $E$  делит  $n$ . Поэтому  $E$  — периодическая абелева группа, являющаяся прямым произведением своих силовских подгрупп  $E(p)$ .

**Теорема 15.8.5.** Силовская  $p$ -подгруппа  $E(p)$  группы  $E = E(H)$   $H\chi$ -расширений абелевой группы  $A$  при помощи конечной группы  $H$  изоморфна группе  $E_p S(p)\chi$ -расширений, получающихся в результате ограничений систем факторов  $F = [(u, v)]$   $H\chi$ -расширений группы  $A$  на аргументы  $(x, y)$ , где  $x, y \in S(p)$ , а  $S(p)$  — силовская  $p$ -подгруппа группы  $H$ .

*Доказательство.* Определим  $p$ -эквивалентность  $(u, v) \sim_p (u, v)_1$  систем факторов  $F = [(u, v)]$  для  $H$ - $\chi$ -расширений группы  $A$ . Две системы факторов  $p$ -эквивалентны, если при ограничении аргументов  $x, y \in S(p)$  для возникающих  $S(p)$ - $\chi$ -расширений имеет место

$$(x, y) \sim (x, y)_1.$$

Нетрудно заметить, что это истинная эквивалентность. Пусть  $E_1$  — подгруппа группы  $E$ , состоящая из тех систем факторов  $F = [(u, v)]$ , для которых  $(x, y) \sim 1$  при  $x, y \in S(p)$ . Тогда элементы группы  $E$  соответствуют  $p$ -эквивалентным системам факторов в том и только в том случае, когда они принадлежат одному и тому же смежному классу по  $E_1$ . Следовательно, фактор-группа  $E/E_1$  изоморфна группе  $E_p$  для  $S(p)$ - $\chi$ -расширений, получаемых при рассмотрении систем факторов  $F[(u, v)]$  для значений аргументов  $x, y$  только из группы  $S(p)$ . Так как  $S(p)$  — подгруппа группы  $B$ , то, согласно следствию из теоремы Гашюца, порядок любого элемента из  $E_1$  делит индекс  $m$  подгруппы  $S(p)$ ; следовательно, по теореме 15.2.1 мы получаем, что порядок любого элемента группы  $E_p$  делит  $p^e$ . Так как  $(p^e, m) = 1$ , отсюда вытекает, что группа  $E_p$  и силовская  $p$ -подгруппа  $E(p)$  группы  $E$  изоморфны фактор-группе  $E/E_1$  и, следовательно, изоморфны друг другу. Этим теорема доказана.

**Теорема 15.8.6.**  *$H$ - $\chi$ -расширение группы  $A$  расщепляется тогда и только тогда, когда для каждого простого числа  $p$ , делящего порядок группы  $H$ , расщепляется расширение для силовской  $p$ -подгруппы  $S(p)$  группы  $H$ .*

*Доказательство.* Очевидно, что из расщепляемости расширения группы  $A$  при помощи  $H$  следует расщепляемость расширения  $A$  при помощи  $S(p)$ . Докажем обратное. Пусть  $F[(u, v)]$  — система факторов, определяющая  $H$ - $\chi$ -расширение. По условию  $(u, v) \sim (u, v)_1$ , где  $(x, y)_1 = 1$  для  $x, y \in S(p)$ . В силу следствия  $(u, v)^m \sim (u, v)_1^m \sim 1$ , где  $n = p^em$ . Но это должно иметь место для любого  $p$ , которое делит  $n$ . Различные числа  $m$ , для которых  $(u, v)^m \sim 1$ , взаимно просты, и поэтому  $(u, v) \sim 1$ , т. е. расширение группы  $A$  при помощи  $H$  расщепляется.

## Г л а в а 16

# ПРЕДСТАВЛЕНИЯ ГРУПП

### 16.1. Общие замечания

Будем называть *представлением* группы  $G$  любой гомоморфизм  $\alpha$  группы  $G$  в некоторую группу  $W$ . Особую ценность имеют представления группы  $G$  в такие группы  $W$ , в которых удобно производить вычисления. Так, представления группы  $G$  подстановками, рассмотренные в главе 5, являются гомоморфизмами группы  $G$  в симметрическую группу  $S_n$ .

Вместо симметрической группы мы можем рассматривать эндоморфизмы векторного пространства  $V$  над полем  $F$ . Эти эндоморфизмы образуют группу, которая в случае векторного пространства  $V$  конечной размерности  $n$  над полем  $F$  называется *полной линейной группой*  $GL_n(F)$ . Она может быть задана также, как группа невырожденных квадратных матриц степени  $n$  над полем  $F$ . Здесь мы рассмотрим представления группы  $G$  линейными преобразованиями. При таком представлении можно рассматривать элементы из группы  $G$  как операторы векторного пространства  $V$ . Тогда подпространства пространства  $V$ , отображаемые в себя линейными преобразованиями, соответствующими элементам группы  $G$ , являются инвариантными подпространствами или, если рассматривать  $V$  как аддитивную группу с операторами из  $F$  и  $G$ , допустимыми подгруппами  $N$ .

Множество всех эндоморфизмов векторного пространства  $V$  образует кольцо. Поэтому от линейного представления группы  $G$  над  $V$  можно перейти, если ввести операции сложения и умножения элементов группы  $G$  на скаляры из поля  $F$ , к линейному представлению группового кольца  $R_G$  группы  $G$  над полем  $F$ , а в любой допустимой относительно  $R_G$  подгруппе  $N$  группы  $V$  реализуется представление как кольца  $R_G$ , так и группы  $G$ . Поэтому неудивительно, что существует тесная связь между разложением группового кольца  $R_G$  и разложением линейных представлений. Исторически теория представлений групп и структурная теория колец развивались отдельно, и только в сравнительно недавнее время была осознана тесная связь между этими двумя теориями.

## 16.2. Матричные представления. Характеры<sup>1)</sup>

**Определение.** Матричным представлением степени  $n$  группы  $G$  называется такая функция  $\rho$  на группе  $G$  со значениями в линейной группе  $GL_n(F)$  для некоторого поля  $F$ , что  $\rho(xy) = \rho(x)\rho(y)$  для всех  $x, y \in G$ .

Заметим, что, согласно этому определению,  $\rho(x)$  — невырожденная матрица, а отображение  $x \rightarrow \rho(x)$  — гомоморфизм группы  $G$  в группу  $GL_n(F)$ . Поэтому  $\rho(1) = I_n$  — единичная матрица  $n \times n$ , и  $\rho(x^{-1}) = [\rho(x)]^{-1}$ . Ядро  $K$  гомоморфизма  $x \rightarrow \rho(x)$  является инвариантной подгруппой группы  $G$ , и матрицы  $\rho(x)$  дают точное представление группы  $G/K$ . Представление точно только в случае, когда ядро  $K$  — единичная подгруппа.

**Определение.** Характер  $\chi$  представления  $\rho$  — это следующая функция на группе  $G$ :

$$\chi(x) = \text{след } \rho(x).$$

Характеры элементов группы являются числами из поля  $F$ . Если представление имеет степень 1, то  $\chi = \rho$ .

Будем говорить, что два представления  $\rho$  и  $\rho^*$  эквивалентны, если существует такая невырожденная матрица  $S \in GL_n(F)$ , что  $\rho^*(x) = S^{-1}\rho(x)S$  для любого  $x \in G$ . Если  $S$  — любая невырожденная матрица из группы  $GL_n(F)$  и  $\rho(x)$  — некоторое представление группы  $G$ , то  $S^{-1}\rho(x)S$  — также представление  $\rho_x^*$  группы  $G$ . Действительно, если рассматривать  $\rho(x)$ ,  $x \in G$ , как группу линейных преобразований векторного пространства  $V$  над полем  $F$  с базисом  $u_1, u_2, \dots, u_n$  и если

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = S \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

то  $S^{-1}\rho(x)S = \rho^*(x)$ ,  $x \in G$ , — группа тех же линейных преобразований пространства  $V$ , но в базисе  $v_1, \dots, v_n$ .

**Лемма 16.2.1.** Характер является функцией класса сопряженных элементов, т. е. характеристики сопряженных элементов равны.

1) Свойства матриц, определителей и полной линейной группы, которые здесь используются, можно найти в книге Биркгофа и Маклейна [1], гл. 6, § 9 (см. также Курош А. Г., Курс высшей алгебры, изд. 5, 1956; Мальцев А. И., Основы линейной алгебры, изд. 2, М.—Л., 1956. — Прим. перев.).

**Лемма 16.2.2.** Эквивалентные представления имеют равные характеристики.

Действительно, если  $A$  — матрица  $n \times n$ , то, по определению, ее характеристический многочлен равен  $f(\lambda) = |A - \lambda I| = (-1)^n [\lambda^n - a_1\lambda^{n-1} + \dots + (-1)^n a_n]$ , где коэффициент  $a_1$  равен следу матрицы  $A$ ,  $a_1 = \text{след}(A)$  и  $a_n = |A|$  — определитель матрицы  $A$ . Если теперь  $T$  — невырожденная матрица, то  $|T^{-1}AT - \lambda I| = |T^{-1}(A - \lambda I)T| = |T^{-1}| \cdot |A - \lambda I| \cdot |T| = |A - \lambda I|$ . Таким образом, матрицы  $A$  и  $T^{-1}AT$  имеют один и тот же характеристический многочлен и тем более один и тот же след. Поэтому матрицы  $\rho(y^{-1}xy) = \rho(y)^{-1}\rho(x)\rho(y)$  и  $\rho(x)$  имеют равные следы, т. е.  $\chi(y^{-1}xy) = \chi(x)$ . Значит, действительно, характер является функцией класса сопряженных элементов. Аналогично матрицы  $\rho^*(x) = S^{-1}\rho(x)S$  и  $\rho(x)$  имеют равные следы, и поэтому эквивалентные представления обладают равными характеристиками.

Напомним, что векторное пространство  $V$  (или „линейное пространство“) над полем  $F$  определяется следующими законами:

в нем задано **бинарное сложение**: для  $\alpha, \beta \in V$ ,  $\alpha + \beta \in V$ ;

в нем задано **умножение на скаляр**:  $c\alpha \in V$ , где  $c \in F$ ,  $\alpha \in V$ .

Эти операции подчинены следующим условиям:

V1)  $V$  — абелева группа по сложению,

V2)  $c(\alpha + \beta) = c\alpha + c\beta$ ,  $(c + c')\alpha = c\alpha + c'\alpha$ ,

V3)  $(cc')\alpha = c(c'\alpha)$ ,  $1\alpha = \alpha$ .

Здесь  $\alpha, \beta \in V$ ,  $c, c' \in F$ ,  $1$  — единица поля  $F$ .

Векторы  $u_1, \dots, u_r$  пространства  $V$  называются **линейно независимыми**, если из равенства

$$a_1u_1 + \dots + a_ru_r = 0, \quad a_i \in F,$$

следует, что  $a_1 = \dots = a_r = 0$ . Если, кроме того, каждый вектор  $u \in V$  представим в виде

$$u = b_1u_1 + b_2u_2 + \dots + b_nu_n, \quad b_i \in F,$$

то  $u_1, u_2, \dots, u_n$  образуют **базис** пространства  $V$ . Если пространство  $V$  имеет базис, то все его базисы состоят из одного и того же числа векторов; это число называется **размерностью** векторного пространства.

Определим  **$F$ - $G$ -модуль**  $M$  как векторное пространство  $V$  над полем  $F$  с элементами группы  $G$  в качестве операторов, причем

- 1)  $(u+v)g = ug + vg$ ,  $u, v \in V$ ,  $g \in G$ ,
- 2)  $u(g_1g_2) = (ug_1)g_2$ ,  $u \in V$ ,  $g_1, g_2 \in G$ ,
- 3)  $u \cdot 1 = u$ ,  $u \in V$ ,  $1$  — единица группы  $G$ ,
- 4)  $(au)g = a(ug)$ ,  $a \in F$ ,  $u \in V$ ,  $g \in G$ .

Будем также называть  $M$  **модулем представления группы  $G$** .

*Операторным гомоморфизмом* одного  $F$ - $G$ -модуля  $M_1$  в другой  $F$ - $G$ -модуль  $M_2$  называется такое отображение  $M_1 \rightarrow M_2$ , что

- 1) если  $u_1 \rightarrow v_1$  и  $u_2 \rightarrow v_2$ , то  $u_1 + u_2 \rightarrow v_1 + v_2$ ,
- 2) если  $u \rightarrow v$  и  $b \in F$ , то  $bu \rightarrow bv$ ,
- 3) если  $u \rightarrow v$  и  $g \in G$ , то  $ug \rightarrow vg$ .

*Операторный изоморфизм* между модулями  $M_1$  и  $M_2$  — это взаимно однозначный операторный гомоморфизм  $M_1$  на  $M_2$ .

Пусть  $u_1, \dots, u_n$  — базис модуля  $M$  над полем  $F$ ; если для  $x \in G$  положить  $v \rightarrow vx$ ,  $v \in V$ , причем  $u_i \rightarrow u_i x = \sum_{j=1}^n a_{ij} u_j$ , то мы получаем представление  $\rho(x) = (a_{ij})$ ,  $i, j = 1, \dots, n$ , группы  $G$  относительно модуля  $M$ . Обратно, если  $\rho$  — представление группы  $G$  относительно векторного пространства  $V$  с базисом  $v_1, \dots, v_n$  и если  $\rho(x) = (a_{ij}) = [a_{ij}(x)]$ , то полагаем

$$u_i x = \sum_{j=1}^n a_{ij}(x) u_j, \quad i = 1, \dots, n,$$

для любого элемента  $x$  из  $G$ . Тогда, так как  $\rho(1) = I_n$  и  $\rho(xy) = \rho(x)\rho(y)$ , векторное пространство  $V$  становится  $F$ - $G$ -модулем  $M$ . Таким образом,  $F$ - $G$ -модуль размерности  $n$  определяет представление группы  $G$  степени  $n$ , и наоборот.

**Теорема 16.1.1.** Два  $F$ - $G$ -модуля  $M_1$  и  $M_2$  определяют эквивалентные представления группы  $G$  тогда и только тогда, когда они операторно изоморфны.

*Доказательство.* Пусть даны два эквивалентных представления группы  $G$ :

$$\rho(x) \text{ и } S^{-1}\rho(x)S, \quad x \in G.$$

Если  $\rho(x) = [a_{ij}(x)]$ ,  $x \in G$ , то это означает, что в векторном пространстве  $V$  с базисом  $v_1, \dots, v_n$  определено действие операторов из группы  $G$  и  $u_i \rightarrow u_i x = \sum_j a_{ij}(x) v_j$ . Как мы уже отмечали, то же самое линейное преобразование соответствует представлению  $\rho^*(x) = S^{-1}\rho(x)S$ ,  $x \in G$ , относительно базиса  $v_1, \dots, v_n$ , где

$$\begin{pmatrix} u_1 \\ u_2 \\ \vdots \\ u_n \end{pmatrix} = S \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Если  $S = (s_{ij})$ , то эквивалентные представления  $\rho(x)$  и  $\rho^*(x)$  операторно изоморфны относительно отображения  $u_i \rightarrow \sum_j s_{ij} v_j$ ,  $i = 1, \dots, n$ . Обратно, пусть два  $F$ - $G$ -модуля  $M_1$  и  $M_2$  операторно

изоморфны. Будучи изоморфными как векторные пространства, модули  $M_1$  и  $M_2$  имеют равные размерности. Пусть  $u_1, \dots, u_n$  — базис модуля  $M_1$ , который при операторном изоморфизме отображается в базис  $v_1, \dots, v_n$  модуля  $M_2$ . При  $u_i \rightarrow v_i$  имеем  $u_i x \rightarrow v_i x$ . При таком выборе базисов в модулях  $M_1$  и  $M_2$  реализуются одинаковые представления, так как если

$$u_i x = \sum_{j=1}^n a_{ij}(x) u_j, \quad i = 1, \dots, n,$$

то

$$v_i x = \sum_{j=1}^n a_{ij}(x) v_j, \quad i = 1, \dots, n.$$

Таким образом, эквивалентные представления  $\rho(x)$  и  $\rho^*(x)$  соответствуют операторному изоморфизму модулей представления.

### 16.3. Теорема о полной приводимости

Предположим, что модуль представления  $M$  имеет подмодуль  $M_1$ , также являющийся модулем представления. Тогда выберем базис  $u_1, \dots, u_r$  подмодуля  $M_1$  и дополним его элементами  $u_{r+1}, \dots, u_n$  до базиса модуля  $M$ . Говорят, что соответствующее представление  $\rho$  *приводимо*; в базисе  $u_1, \dots, u_n$  оно имеет вид

$$\rho(x) = \begin{pmatrix} \sigma(x) & 0 \\ \theta(x) & \tau(x) \end{pmatrix},$$

где  $\sigma$  и  $\tau$  — представления группы  $G$  степеней  $r$  и  $n-r$  соответственно. Представление  $\sigma$  соответствует  $F$ - $G$ -модулю  $M_1$  с базисом  $u_1, \dots, u_r$ . Что касается  $\tau$ , то это — представление в базисе  $M_1 + u_{r+1}, \dots, M_1 + u_n$  фактор-модуля  $M/M_1$ . Вообще если

$$0 = M_0 \subset M_1 \subset M_2 \subset \dots \subset M_k = M$$

— цепь подмодулей и мы выбрали базис модуля  $M$ , соответствующий этой цепи, то соответствующее представление  $\rho$  принимает вид

$$\rho(x) = \left[ \begin{array}{c|c} \rho_1(x) & 0 \\ \hline & \rho_2(x) \\ \hline & * \\ & \rho_k(x) \end{array} \right],$$

где  $\rho_i(x)$  — представление, соответствующее определенному базису фактор-модуля  $M_i/M_{i-1}$ , а именно базису  $M_{i-1} + u_j$ , где  $u_j$  проходит базисные векторы, принадлежащие  $M_i$ , но не принадлежащие  $M_{i-1}$ . Для характеров, очевидно, справедливо равенство

$$\chi(x) = \chi_1(x) + \chi_2(x) + \dots + \chi_k(x).$$

Если мы выберем *максимальную* цепь, т. е. цепь, не допускающую дальнейших уплотнений, то фактор-модули  $M_i/M_{i-1}$  не имеют собственных подмодулей представления, и представления  $\rho_i$ , которые в них реализуются, называются *неприводимыми*. Очевидным следствием отсюда является

**Лемма 16.3.1.** *Любой характер является суммой неприводимых характеров.*

**Лемма 16.3.2.** *Неприводимые представления  $\rho_i$  определяются однозначно с точностью до порядка следования и операторного изоморфизма.*

Лемма 16.3.2 следует из теоремы Жордана — Гельдера.

Если модуль представления  $M$  обладает подмодулем представления  $M_1$ , то может случиться, что существует дополнительный подмодуль представления  $M_2$ , т. е. такой, что модуль  $M$  — прямая сумма  $M = M_1 \oplus M_2$ . В этом случае модуль  $M_2$ , очевидно, операторно изоморден модулю  $M/M_1$ , а представление  $\rho(x)$  имеет вид

$$\rho(x) = \begin{pmatrix} \rho_1(x) & 0 \\ 0 & \rho_2(x) \end{pmatrix}.$$

Обратно, если представление  $\rho(x)$  может быть представлено в такой форме, когда по главной диагонали стоят квадратные блоки, то модуль  $M$  является прямой суммой подмодулей  $M_1$  и  $M_2$  представления  $\rho(x)$ . В этом случае мы говорим, что представление *вполне приводимо*<sup>1)</sup>. Не всякое приводимое представление вполне приводимо. Например, представление

$$\rho(b^i) = \begin{pmatrix} 1, & 0 \\ i, & 1 \end{pmatrix}$$

бесконечной циклической группы, порожденной элементом  $b$ , приводимо, но если бы оно было вполне приводимо, то оно сопоставляло бы каждому элементу единичную матрицу, так как здесь

<sup>1)</sup> В советской литературе такие представления называются „разложимыми“, а „вполне приводимыми“ называются представления, которые разлагаются в прямую сумму неприводимых представлений. — Прим. перев.

$\rho_1(b^i) = \rho_2(b^i) = E$ . Но матрица  $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$  не сопряжена с единичной. Поэтому полная приводимость здесь невозможна.

Тем не менее существует важный класс представлений, для которых из приводимости следует полная приводимость.

Теорема 16.3.1. (Теорема о полной приводимости.) *Приводимое представление конечной группы  $G$  над полем  $F$ , характеристика которого не делит порядок группы  $G$ , вполне приводимо.*

*Доказательство.* Пусть  $M$  — модуль представления группы  $G$  над полем  $F$  и  $M_1$  — подмодуль представления. Дополним базис  $u_1, \dots, u_r$  подмодуля  $M_1$  до базиса модуля  $M$  элементами  $u_{r+1}, \dots, u_n$ , составляющими базис подпространства  $N$ , которое, вообще говоря, не является подмодулем представления. Тогда для  $x \in G$  имеем

$$\rho(x) = \begin{pmatrix} \sigma(x) & 0 \\ \theta(x) & \tau(x) \end{pmatrix}.$$

Теперь  $M = M_1 + N$ , откуда для элемента  $u \in M$  получаем однозначное представление

$$u = u_1 + v, \quad u_1 \in M_1, \quad v \in N.$$

Отображение  $\eta: u \rightarrow v$  идемпотентно и линейно. Если  $g$  — порядок группы  $G$ , то положим

$$u' = \frac{1}{g} \sum_{x \in G} ux\eta x^{-1} = u\zeta.$$

Весь  $u \rightarrow u' = u\zeta$  — линейное отображение. Для определения отображения  $\zeta$  необходимо производить деление на число  $g$ , а это действительно возможно, так как, согласно нашему предположению, группа  $G$  имеет конечный порядок  $g$ , не делящийся на характеристику поля  $F$ .

Если  $y \in G$ , положим  $z = y^{-1}x$  для  $x \in G$ . Тогда

$$(u\zeta)y = \frac{1}{g} \sum_x ux\eta x^{-1}y = \frac{1}{g} \sum_z (uy)z\eta z^{-1} = (uy)\zeta,$$

так как  $z$  одновременно с  $x$  пробегает все элементы группы  $G$ . Поэтому  $M_2 = M\zeta$  — модуль представления. Покажем, что  $M = M_1 \oplus M_2$ . Для этого мы должны показать, что любой элемент  $u \in M$  представим в виде  $u = u_1 + u_2$ ,  $u_1 \in M_1$ ,  $u_2 \in M_2$  и что это представление единственны, т. е. что из равенства  $0 = u_1 + u_2$  следует, что  $u_1 = u_2 = 0$ . Для произвольного элемента  $u \in M$  имеем

$$u = (u - u\zeta) + u\zeta,$$

где  $u\zeta = u_2 \in M_2$ , здесь  $u - u\zeta = \frac{1}{g} \sum_x (ux - ux\eta) x^{-1}$ , так как  $uxx^{-1} = u$ . Но  $ux - ux\eta = (ux)_1 \in M_1$ , откуда  $u - u\zeta = u_1 \in M_1$ . Итак,  $u = u_1 + u_2$ , где  $u_1 \in M_1$ ,  $u_2 \in M_2$ . Если теперь  $w \in M_1$ , то  $wx \in M_1$ ,  $wx\eta = 0$ , откуда  $w\zeta = 0$ . Таким образом, для любого элемента  $u \in M$  имеем  $(u - u\zeta)\zeta = 0$ , т. е.  $u\zeta^2 = u\zeta$ . Следовательно, если  $u_1 + u_2 = 0$ , то  $u_1\zeta + u_2\zeta = 0$ , откуда  $0 + u_2\zeta = u_2 = 0$ , а значит, и  $u_1 = 0$ . Поэтому представление вполне приводимо.

*Второе доказательство — с помощью матриц.* Пусть мы имеем представление

$$\rho(x) = \left( \begin{array}{c|c} \sigma(x) & 0 \\ \hline \theta(x) & \tau(x) \end{array} \right),$$

где  $\sigma(x)$  и  $\tau(x)$  — представления степеней  $r$  и  $n - r$  соответственно. Постараемся найти такую матрицу

$$S = \left( \begin{array}{c|c} I_r & 0 \\ \hline \mu & I_{n-r} \end{array} \right),$$

где  $\mu$  не зависит от  $x$ , что

$$\left( \begin{array}{c|c} \sigma(x) & 0 \\ \hline \theta(x) & \tau(x) \end{array} \right) \left( \begin{array}{c|c} I_r & 0 \\ \hline \mu & I_{n-r} \end{array} \right) = \left( \begin{array}{c|c} I_r & 0 \\ \hline \mu & I_{n-r} \end{array} \right) \left( \begin{array}{c|c} \sigma(x) & 0 \\ \hline 0 & \tau(x) \end{array} \right)$$

для всех элементов  $x \in G$ . Ясно, что если удастся найти матрицу  $S$ , то она будет невырождена и даст нам эквивалентное представление

$$\rho^*(x) = S^{-1} \rho(x) S = \left( \begin{array}{c|c} \sigma(x) & 0 \\ \hline 0 & \tau(x) \end{array} \right), \quad x \in G,$$

которое будет вполне приводимо.

Задача сводится к нахождению прямоугольной  $(n - r) \times r$  матрицы  $\mu$ , не зависящей от  $x$  и такой, что

$$\mu\sigma(x) - \tau(x)\mu = \theta(x)$$

для всех  $x \in G$ .

Из  $\rho(yx) = \rho(y)\rho(x)$  имеем

$$\theta(yx) = \theta(y)\sigma(x) + \tau(y)\theta(x),$$

откуда

$$\theta(x) = \tau(y^{-1})\theta(yx) - \tau(y^{-1})\theta(y)\sigma(x)$$

и

$$\theta(x) = \frac{1}{g} \sum_y (\tau(x)\tau(x^{-1}y^{-1})\theta(yx) - \tau(y^{-1})\theta(y)\sigma(x)).$$

Полагая теперь

$$-\mu = \frac{1}{g} \sum_y \tau(y^{-1})\theta(y) = \frac{1}{g} \sum_y \tau(x^{-1}y^{-1})\theta(yx),$$

находим, что  $\theta(x) = -\tau(x)\mu + \mu\sigma(x)$ . Таким образом, найдена искомая матрица  $\mu$ , а следовательно, и трансформирующая матрица  $S$ , которая приводит к вполне приводимому представлению  $\rho^*(x)$ .

Повторным применением этой теоремы получаем следующий основной результат.

**Теорема 16.3.2.** *Любое представление конечной группы  $G$  над полем  $F$ , характеристика которого не делит порядок группы  $G$ , разлагается в прямую сумму неприводимых представлений.*

**Следствие 16.3.1.** *Представления конечной группы  $G$  над полем  $F$ , характеристика которого взаимно проста с порядком группы  $G$ , эквивалентны тогда и только тогда, когда они разлагаются в прямую сумму одних и тех же неприводимых представлений, каждое из которых участвует в обеих суммах одинаковое число раз.*

Для вполне приводимого представления  $\rho$  мы можем записать

$$\rho = \rho_1 \oplus \rho_2 \oplus \dots \oplus \rho_k,$$

где  $\rho_i$  — неприводимые представления. Порядок слагаемых здесь несущественен, так как мы можем переставить элементы соответствующего базиса модуля представления  $M$  так, чтобы слагаемые  $\rho_i$  переставились произвольным образом. Ясно, что представлениям  $\rho_i$  соответствуют композиционные факторы модуля  $M$ , рассматриваемого как аддитивная группа с операторами из поля  $F$  и группы  $G$ . По теореме Жордана — Гельдера эти композиционные факторы определяются однозначно с точностью до порядка следования и операторного изоморфизма. В силу теоремы 16.1.1 операторный изоморфизм неприводимого представления означает эквивалентность. Таким образом, говоря в формулировке следствия „одни и те же неприводимые представления“, мы не различаем эквивалентные представления.

## 16.4. Полупростые групповые кольца<sup>1)</sup> и обыкновенные представления

Для произвольной группы  $G$  и поля  $F$  можно построить групповое кольцо  $R_G$  следующим образом:

- 1)  $R_G$  — векторное пространство над полем  $F$  с элементами  $g_i \in G$  в качестве базиса;
- 2) перемножаются элементы из  $R_G$  по правилу

$$\sum_i a_i g_i \cdot \sum_j b_j g_j = \sum_{i,j} a_i b_j g_{ij},$$

где  $g_{ij} = g_i g_j \in G$ .

Нетрудно показать, что  $R_G$  — ассоциативное кольцо с единицей  $1 \cdot 1 = 1$ , являющейся произведением единицы поля  $F$  и нейтрального элемента группы  $G$ . Ясно, что  $R_G$  можно рассматривать как модуль представления группы  $G$ , если элементы из  $G$  действуют на элементы из  $R_G$  путем умножения справа. Если порядок группы  $G$  равен  $n$ , то, взяв элементы  $g_1, \dots, g_n$  группы  $G$  в качестве базиса модуля представления  $R_G$ , получаем представление

$$\rho(x) = (x_{ij}), \quad i, j = 1, \dots, n, \quad x \in G,$$

где  $x_{ij} = 1$ , если  $g_i x = g_j$ , и  $x_{ij} = 0$  в остальных случаях. Мы узнаем известное нам уже правое регулярное представление группы  $G$ , которое в качестве группы подстановок определялось подстановками

$$\pi(x) = \begin{pmatrix} g_1 & \dots & g_n \\ g_1 x & \dots & g_n x \end{pmatrix}, \quad x \in G,$$

а здесь записано в матричном виде.

**Лемма 16.4.1.** При правом регулярном представлении  $\rho(x)$  группы  $G$  порядка  $n$  имеем  $\chi(1) = n$ ,  $\chi(g) = 0$ ,  $g \neq 1$ .

Действительно,  $\rho(x) = (x_{ij})$ , где  $x_{ij} = 1$ , если  $g_i x = g_j$ , и  $x_{ij} = 0$  в остальных случаях; поэтому  $\chi(x) = \sum_i x_{ii}$ . Если  $x = 1$ , то  $g_i 1 = g_j = g_i$  и  $x_{ii} = 1$ ,  $i = 1, 2, \dots, n$ , откуда  $\chi(1) = n$ . Если же  $x = g \neq 1$ , то  $x_{ii} = 0$ , так как равенство  $g_i x = g_i$  не имеет места ни для какого  $g_i$ , если  $x \neq 1$ .

Почти все результаты, которые будут получены ниже, относятся к представлениям конечной группы  $G$  над полем  $F$ , характеристика которого не делит порядок группы  $G$ . Такие представления мы будем называть *обыкновенными представлениями*. Представления конечной группы  $G$  над полем  $F$ , характеристика которого

<sup>1)</sup> Кольцом автор часто называет также и алгебру над полем. — Прим. перев.

делит порядок группы  $G$ , называются *модулярными представлениями*. Свойства модулярных представлений отличны от свойств обыкновенных представлений, и, конечно, можно ожидать, что представления бесконечных групп во многом отличаются от представлений конечных групп.

Кольцо  $R$  называется *регулярным*, если для любого элемента  $u \in R$  существует такой элемент  $x \in R$ , что  $ux = u$ . Регулярное кольцо конечной размерности над полем  $F$  называется *полупростым*. Элемент  $e \neq 0$  такой, что  $e^2 = e$ , называют *идемпотентом*.

**Теорема 16.4.1.** *Групповое кольцо  $R_G$  конечной группы  $G$  над полем  $F$  является полупростым тогда и только тогда, когда характеристика поля  $F$  не делит порядок группы  $G$ .*

**Доказательство.** Пусть  $G$  — группа конечного порядка  $g$ . Если характеристика поля  $F$  делит  $g$  и  $x_1, \dots, x_g$  — элементы группы  $G$ , то рассмотрим в кольце  $R_G$  элемент  $u = x_1 + \dots + x_g$ . Для него  $x_i u = ux_i = u$ . Следовательно, для элемента  $x = a_1 x_1 + \dots + a_g x_g$  мы имеем  $ux = (a_1 + \dots + a_g)u$ , откуда  $ux = (a_1 + \dots + a_g)gu = 0 \neq u$ . Следовательно, кольцо  $R_G$  не полу-простое.

Предположим теперь, что  $g$  не делится на характеристику поля  $F$ . Докажем, что кольцо  $R_G$  полу-простое, а также ряд других свойств кольца  $R_G$ . Пусть  $\mathfrak{a}_1$  — произвольный правый идеал кольца  $R_G$ . Тогда  $\mathfrak{a}_1$  — подмодуль представления модуля  $R_G$ , и, обратно, подмодули представления являются правыми идеалами. По теореме о полной приводимости

$$R_G = \mathfrak{a}_1 \oplus \mathfrak{a}_2,$$

где  $\mathfrak{a}_2$  — другой правый идеал. Тогда  $1 = a_1 + a_2$ ,  $a_1 \in \mathfrak{a}_1$ ,  $a_2 \in \mathfrak{a}_2$ , и это представление единственno. Но тогда равенство  $a_1 = a_1^2 + a_2 a_1$  также справедливо. С другой стороны,  $a_1 = a_1 + 0$ , откуда вследствие однозначности представления элемента  $a_1$  в виде суммы элементов из  $\mathfrak{a}_1$  и  $\mathfrak{a}_2$  получаем  $a_1^2 = a_1$ ,  $a_2 a_1 = 0$ . Таким образом,  $a_1 = e$  — идемпотент, и, следовательно,  $a_2 = 1 - e$  также идемпотент. Таким образом, для  $x \in R_G$  мы имеем  $x = ex + (1 - e)x$ , где  $ex \in \mathfrak{a}_1$ . Обратно, если  $y \in \mathfrak{a}_1$ , то  $y = ey + (1 - e)y = y + 0$  в силу однозначности представления. Следовательно, для  $y \in \mathfrak{a}_1$  справедливо равенство  $ey = y$ . Таким образом,  $\mathfrak{a}_1$  — главный правый идеал  $eR_G$ , порожденный идемпотентом  $e$ , и потому любой правый идеал кольца  $R_G$  является главным правым идеалом, порожденным некоторым идемпотентом. В частности, для любого элемента  $u$  существует такой идемпотент  $e$ , что  $uR_G = eR_G$ . Следовательно, для некоторого  $x$  имеем  $ux = e$ , а для некоторого  $y$  имеем  $ey = u$ ,  $eu = e^2y = ey = u$ . Поэтому  $u = eu = uxi$ , откуда следует регулярность кольца  $R_G$ .

**Теорема 16.4.2.** Регулярное кольцо  $R$  конечной размерности над полем  $F$  обладает единицей, а любой правый (левый) идеал является главным идеалом, порожденным некоторым идемпотентом. Любой двусторонний идеал является главным идеалом, порожденным идемпотентом из центра кольца  $R$ .

**Доказательство.** Пусть  $R$  — регулярное кольцо конечной размерности над полем  $F$ . Если  $u$  — произвольный элемент, то в силу регулярности существует такой элемент  $x$ , что  $ux = u$ . Тогда для элемента  $e = ux$  имеем равенства  $e^2 = uxux = ux = e$ , для  $f = xu$  — равенства  $f^2 = xuxu = xu = f$ . Кроме того,  $u = uxu = eu = uf$ , откуда  $eR = uR$ ,  $Ru = Rf$ . Таким образом, главные правые или левые идеалы порождаются идемпотентами. Рассмотрим теперь произвольный левый идеал  $\alpha$ . Если  $\alpha \neq 0$ , то в этом идеале содержится некоторый идемпотент  $e_1 \neq 0$ , причем  $Re_1 \subseteq \alpha$ . Предположим, что  $\alpha \neq Re_1$ . Тогда существует такой элемент  $x \in \alpha$ , что  $x \notin Re_1$ . Он равен

$$x = xe_1 + (x - xe_1),$$

где  $x_1 = xe_1 \in Re_1$ , и элемент

$$x_2 = x - xe_1$$

обладает свойством

$$x_2e_1 = 0.$$

Пусть  $f$  — такой идемпотент, что  $Rx_2 = Rf$ . Тогда  $f = wx_2$ ,  $fe_1 = wx_2e_1 = 0$ . Положим  $e_2 = e_1 + f - e_1f$ . Здесь  $e_1e_2 = e_1$ ,  $fe_2 = f$ . Отсюда

$$e_2^2 = (e_1 + f - e_1f)e_2 = e_1 + f - e_1f = e_2,$$

т. е.  $e_2$  — идемпотент, принадлежащий идеалу  $\alpha$ . Идеал  $Re_2$  содержит элементы  $e_1$  и  $f$ , поэтому он содержит идеал  $Re_1$  и элемент  $x \notin Re_1$ . Следовательно, размерность  $Re_2$  больше размерности  $Re_1$ . Продолжим процесс построения идемпотентов  $e_3, e_4, \dots$ , содержащихся в  $\alpha$  и таких, что размерность идеала  $Re_i$  больше размерности предыдущего идеала, до тех пор, пока не достигнем такого идемпотента  $e$ , что  $\alpha = Re$ . Этим доказано, что любой левый идеал является главным левым идеалом, порожденным некоторым идемпотентом. Аналогичные рассуждения показывают, что любой правый идеал является главным правым идеалом, порожденным некоторым идемпотентом. Если  $x \in eR$ , то для некоторого  $w$   $x = ew$  и  $ex = e^2w = ew = x$ , т. е.  $e$  — это левая единица для элементов из  $eR$ . Аналогично для  $x \in Rf$  верно соотношение  $xf = x$ . Но само кольцо  $R$  одновременно является

и левым, и правым идеалом. Поэтому существуют такие идемпотенты  $e$  и  $f$ , что  $R = eR = Rf$ . Тогда  $ef = f = e$  и  $ex = xe = x$ , откуда  $e = 1$  служит единицей для  $R$ .

Произведения произвольных элементов на идемпотент  $e$  из центра кольца  $R$  будут, конечно, образовывать двусторонний идеал. Мы покажем, что, обратно, произвольный двусторонний идеал  $\alpha$  есть главный идеал идемпотента центра. Для порождающих идемпотентов мы имеем  $\alpha = eR = Rf$ . Следовательно,  $ef = f = e$  и  $\alpha = eR = Re$ . Теперь для произвольного  $x \in R$  мы имеем  $ex \in \alpha$ , откуда  $ex = exe$ . Аналогично  $xe \in \alpha$ , откуда  $xe = exe$ . Таким образом,  $ex = xe$ , и потому  $e$  принадлежит центру кольца  $R$ .

Назовем кольцо  $R$  *простым*, если оно полупростое и не содержит двусторонних идеалов, отличных от  $0$  и  $R$ . Прямую сумму правых идеалов мы будем обозначать  $\oplus$ , а прямую сумму двусторонних идеалов — значком  $\boxplus$ .

**Теорема 16.4.3.** *Полупростое кольцо  $R$  есть прямая сумма  $R = R_1 \boxplus R_2 \boxplus \dots \boxplus R_s$  простых колец. Простые кольца  $R_i$  определяются однозначно с точностью до порядка следования.*

**Доказательство.** Пусть  $R_1$  — минимальный двусторонний идеал кольца  $R$ . Тогда  $R_1$  — главный идеал, порожденный некоторым идемпотентом  $e_1$  из центра кольца  $R$ . Для  $x \in R$ , следовательно, имеет место разложение  $x = xe_1 + x(1 - e_1)$ . Поэтому  $R = R_1 \boxplus \bar{R}_1$ , где  $\bar{R}_1$  состоит из всех элементов вида  $x(1 - e_1)$ .  $e_1$  — единица идеала  $R_1$ ,  $\bar{e}_1 = 1 - e_1$  — единица  $\bar{R}_1$ . Для  $x, y \in R_1$  и  $z, w \in \bar{R}_1$  имеем  $(x + z) + (y + w) = (x + y) + (z + w)$  и  $(x + z)(y + w) = xy + zw$ , так как  $zy = ze_1(1 - e_1)y = 0$  и аналогично  $xw = 0$ . Таким образом, в прямой сумме  $R_1 \boxplus \bar{R}_1$  сложение и умножение производятся покомпонентно. Поэтому, в частности, из регулярности кольца  $R$  следует регулярность подкольца  $R_1$  и  $\bar{R}_1$ . Далее, пусть  $R_2$  — минимальный двусторонний идеал кольца  $\bar{R}_1$ . Тогда находим, что  $\bar{R}_1 = R_2 \boxplus \bar{R}_2$ . Продолжив этот процесс, мы получаем

$$R = R_1 \boxplus R_2 \boxplus \dots \boxplus R_s,$$

где  $1 = e_1 + e_2 + \dots + e_s$ , и элементы  $e_i$ ,  $i = 1, \dots, s$ , являются идемпотентами из центра кольца  $R$ , причем  $e_i e_j = 0$ , если  $i \neq j$ .

Элементы

$$\begin{aligned} x &= x_1 + x_2 + \dots + x_s, \\ y &= y_1 + y_2 + \dots + y_s, \end{aligned}$$

где  $x_i, y_j \in R_i$ , складываются и перемножаются следующим образом:

$$\begin{aligned} x + y &= (x_1 + y_1) + (x_2 + y_2) + \dots + (x_s + y_s), \\ xy &= x_1 y_1 + x_2 y_2 + \dots + x_s y_s. \end{aligned}$$

Поэтому, обратно, прямая сумма простых колец  $R$  над одним и тем же полем  $F$  регулярна и, следовательно, является полупростым кольцом. Если теперь  $\alpha$  — любой двусторонний идеал в  $R$ , то он является главным идеалом, порожденным идемпотентом  $e$  из центра кольца. Тогда

$$e = e_1e + e_2e + \dots + e_se,$$

где  $e_ie \neq 0$  для некоторого  $i$ . Но, если идеал  $\alpha$  минимальный, и при этом имело бы место неравенство  $e_ie \neq e_i$ , то главный идеал, порожденный элементом  $e_ie$ , строго содержался бы в  $R_i$ , а если бы имело место неравенство  $e_ie \neq e$ , то он бы строго содержался в  $\alpha$ . Следовательно,  $e_ie = e_i = e$ , т. е.  $\alpha = R_i$ . Этим доказана однозначность разложения кольца в прямую сумму.

**Теорема 16.4.4.** Любое обыкновенное неприводимое представление конечной группы  $G$  эквивалентно представлению, которое реализуется в некотором минимальном правом идеале кольца  $R_G$ . Два минимальных правых идеала кольца  $R_G$  дают эквивалентные представления тогда и только тогда, когда они принадлежат одному и тому же простому слагаемому кольца  $R_G$ .

**Доказательство.** Отметим, что произвольное представление  $\rho$  группы  $G$  индуцирует представление кольца  $R_G$ , так как для любого элемента  $h = \sum_{x \in G} a_x x$ ,  $a_x \in F$ ,  $x \in G$ , кольца  $R_G$  мы можем определить представление

$$\rho(h) = \sum a_x \rho(x).$$

Эквивалентные представления группы  $G$  дают эквивалентные представления кольца  $R_G$ , и обратно.

Регулярное представление группы  $G$  — это представление в  $F$ - $G$ -модуле  $R_G$ . Он разлагается в прямую сумму

$$R_G = e_1R_G \oplus e_2R_G \oplus \dots \oplus e_tR_G,$$

где  $1 = e_1 + e_2 + \dots + e_t$ , а  $e_i$  — ортогональные идемпотенты, т. е.  $e_i e_j = 0$ , если  $i \neq j$ ;  $e_i R_G$  — минимальные правые идеалы.

Пусть теперь  $\rho(x)$  — обыкновенное неприводимое представление группы  $G$ , а тем самым и кольца  $R_G$ . Пусть  $M$  — неприводимый  $F$ - $G$ -модуль представления  $\rho$ . Тогда  $M = M \cdot 1 = M(e_1 + \dots + e_t)$ . Следовательно, для некоторого  $e_i$ :  $Me_i \neq 0$ . Пусть  $m$  — такой вектор из  $M$ , что  $me_i \neq 0$ . Тогда  $me_i R_G \neq 0$  — модуль представления группы  $G$ , отличный от нуля и содержащийся в  $M$ . Так как модуль  $M$  неприводим, то  $M = me_i R_G$ . Соответствие

$$me_i \left( \sum_{x \in G} a_x x \right) \leftrightarrow e_i \sum_{x \in G} a_x x$$

взаимно однозначно, так как элементы  $e_i h$ , для которых  $te_i h = 0$ , образуют правый идеал, строго содержащийся в  $e_i R_G$  и, следовательно, равный нулю. Это соответствие является операторным изоморфизмом между модулем представления  $M$  и модулем, представления  $e_i R_G$ , и поэтому, согласно теореме 16.1.1, представление  $\rho(x)$  эквивалентно представлению, реализующемуся в минимальном правом идеале  $e_i R_G$ .

В каком случае два минимальных правых идеала определяют эквивалентные представления? Минимальный правый идеал должен содержаться в одном из минимальных двусторонних идеалов. Пусть

$$R_G = R_1 \boxplus R_2 \boxplus \dots \boxplus R_s$$

— разложение кольца  $R_G$  в сумму простых идеалов, т. е. минимальных двусторонних идеалов. При этом  $1 = e_1 + e_2 + \dots + e_s$ , где  $e_i$  — ортогональные идемпотенты из центра.

Предположим, что  $e_{i1} R_G$  и  $e_{i2} R_G$  — два минимальных правых идеала из одного и того же простого идеала  $R_i$ . Тогда все конечные суммы вида  $u_1 e_{i1} v_1 + \dots + u_m e_{i1} v_m$ , где  $u_k, v_k \in R_G$ , образуют двусторонний идеал, а так как элемент  $e_i(e_{i1})e_i = e_{i1} \neq 0$  принадлежит этому идеалу, то он совпадает с  $R_i$ . Следовательно, для подходящих элементов  $u_i$  и  $v_i$

$$u_1 e_{i1} v_1 + \dots + u_m e_{i1} v_m = e_{i2}.$$

Так как  $e_{i2}^2 = e_{i2}$ , то для некоторого  $j$  имеем

$$e_{i2} u_j e_{i1} v_j \neq 0.$$

Но тогда  $e_{i1} v_j R_G \neq 0$ , а так как это правый идеал, содержащийся в минимальном идеале  $e_{i1} R_G$ , то  $e_{i1} v_j R_G = e_{i1} R_G$ . Аналогично  $e_{i2} u_j e_{i1} v_j R_G = e_{i2} R_G$ . Следовательно, при  $w = e_{i2} u_j$  имеем  $w e_{i1} R_G = e_{i2} R_G$ . Значит, для  $h \in R_G$  имеем соответствие  $w e_{i1} h \leftrightarrow e_{i2} h$ , т. е. правые идеалы  $e_{i1} R_G$  и  $e_{i2} R_G$  операторно изоморфны, а поэтому соответствующие представления эквивалентны. Этим показано, что минимальные правые идеалы из одного и того же простого идеала дают то же самое представление.

Предположим теперь, что  $e_{i1} R_G$  и  $e_{j1} R_G$  — минимальные правые идеалы из простых идеалов  $R_i$  и  $R_j$ ,  $i \neq j$ . Если рассматривать представление в идеале  $e_{i1} R_G$ , то мы получаем следующие отображения соответственно для  $e_i$  и  $e_j$ :

$$\begin{aligned} e_i : e_{i1} h \rightarrow e_{i1} h e_i &= e_{i1} e_i h = e_{i1} h, \\ e_j : e_{i1} h \rightarrow e_{i1} h e_j &= e_{i1} e_j h = 0, \end{aligned}$$

откуда  $\rho(e_i) = 1$ , и  $\rho(e_j) = 0$ . Аналогично в идеале  $e_{j1} R_G$  элементу  $e_j$  соответствует нуль, а  $e_i$  соответствует единица. Следовательно, эти представления неэквивалентны.

Мы находим разложение кольца  $R_G$  в прямую сумму простых идеалов с помощью ортогональных идемпотентов из центра  $Z$  кольца  $R_G$ . Что можно сказать о центре кольца  $R_G$ ? На этот вопрос отвечает следующая теорема.

**Теорема 16.4.5.** Элементы вида  $C_i = x_{i1} + \dots + x_{ih}$ , где  $x_{i1}, \dots, x_{ih}$  образуют класс сопряженных элементов группы  $G$ , составляют базис центра кольца  $R_G$ .

**Доказательство.** Если  $C_i = x_{i1} + \dots + x_{ih}$ , где справа записана сумма элементов некоторого класса сопряженных элементов группы  $G$ , то  $y^{-1}C_iy = C_i$  для  $y \in G$ , так как трансформирование просто переставляет слагаемые суммы  $C_i$  между собой. Так как элемент  $C_i$  перестановочен с любым элементом  $y \in G$ , он перестановочен с любым элементом из кольца  $R_G$ , т. е. принадлежит его центру. Обратно, если элемент  $u$  принадлежит центру кольца  $R_G$  и  $u = \sum_{x \in G} a_x x$ , то для  $y \in G$  мы имеем  $y^{-1}uy = u = \sum_{x \in G} a_x y^{-1}xy$ . Поэтому в сумме для элемента  $u$  сопряженные элементы имеют равные коэффициенты, откуда следует, что  $u$  есть линейная комбинация элементов  $C_i$ .

## 16.5. Абсолютно неприводимые представления.

### Структура простых колец

Мы уже видели, что все неприводимые представления оказываются компонентами регулярного представления  $R(G)$  группы  $G$ . Поэтому нахождение всех таких представлений сводится к нахождению всех неприводимых составных частей представления  $R(G)$ , или, что то же самое, к отысканию минимальных правых идеалов группового кольца  $R_G$ .

Неприводимость представления — понятие относительное, оно зависит от основного поля. Так, если  $G$  — циклическая группа порядка 3 с элементами 1,  $x$ ,  $x^2$  над полем рациональных чисел, групповое кольцо  $R_G$  обладает разложением  $R_G = R_1 \boxplus R_2$ . При этом  $1 = e_1 + e_2$ , где

$$e_1 = \frac{1+x+x^2}{3}, \quad e_2 = \frac{2-x-x^2}{3}$$

— идемпотенты;  $e_1$  — базис для  $R_1$ , а  $e_2, e_2x$  — базис для  $R_2$ . Этому базису соответствует представление

$$\rho(x) = \left( \begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 0 & 1 \\ 0 & -1 & -1 \end{array} \right),$$

т. е. идеалам  $R_1$  и  $R_2$  соответствуют неприводимые представления степеней 1 и 2 соответственно. Но если мы расширим поле рациональных чисел, присоединив к нему кубический корень из единицы  $\varepsilon = (-1 + \sqrt{-3})/2$ , то неприводимое представление  $R_2$  степени 2 станет приводимым. В базисе

$$e_1 = \frac{1+x+x^2}{2},$$

$$\bar{e}_2 = \frac{1+\varepsilon x+\varepsilon^2 x^2}{3}, \quad \bar{e}_3 = \frac{1+\varepsilon^2 x+\varepsilon x^2}{3},$$

где  $\bar{e}_2 + \bar{e}_3 = e_2$ , имеем

$$\rho(x) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \varepsilon^2 & 0 \\ 0 & 0 & \varepsilon \end{pmatrix}, \quad \varepsilon^3 = 1.$$

Ясно, что дальнейшее расширение основного поля не приведет к дальнейшему выделению неприводимых составных частей представления  $\rho(x)$ .

Представление  $\rho$  степени  $n$  называется *абсолютно неприводимым*, если оно остается неприводимым при любом расширении поля  $F$ . Очевидно, если представление  $\rho$  приводимо над полем  $K \supset F$

$$\rho(x) = \left( \begin{array}{c|c} \sigma(x) & 0 \\ \hline 0 & \tau(x) \end{array} \right),$$

где все  $x \in G$ ,  $\sigma(x)$  — матрица порядка  $s$ , а  $\tau(x)$  — матрица порядка  $n-s$ , то  $\rho(h)$ ,  $h \in R_G$ , рассматриваемая как алгебра над  $K$ , имеет размерность не большую, чем  $s^2 + (n-s)^2 < n^2$ . Следовательно, если  $\rho(h)$ ,  $h \in R_G$ , как алгебра над  $F$ , имеет размерность, равную  $n^2$ , то представление  $\rho$  абсолютно неприводимо над  $F$ . Мы покажем, что при подходящем алгебраическом расширении основного поля  $F$  любое обыкновенное представление разложится в прямую сумму неприводимых представлений, причем неприводимое представление степени  $n$  реализуется в алгебре размерности  $n^2$  над соответствующим полем.

**Теорема 16.5.1.** Алгебра с делением  $D$  конечной размерности над полем  $F$  будет только тогда алгеброй с делением над всеми алгебраическими расширениями поля  $F$ , когда размерность  $D$  над  $F$  равна 1, т. е. если  $D=F$ .

**Доказательство.** Пусть  $u_1, \dots, u_n$  — базис алгебры  $D$  над полем  $F$ . Мы можем выбрать элемент  $u_1=1$  в качестве единицы кольца  $D$ . Если  $n > 1$ , рассмотрим последовательность  $1=u_1$ ,

$u_2, u_2^2, \dots, u_2^n$ . Эти элементы линейно зависимы над полем  $F$ , т. е.

$$u_2^r + a_1 u_2^{r-1} + \dots + a_r = 0, \quad a_i \in F,$$

где не все  $a_i$  равны нулю. Если присоединим к  $F$  корни  $\alpha_1, \dots, \alpha_r$  многочлена  $f(x) = x^r + a_1 x^{r-1} + \dots + a_r$ , то получим  $(u_2 - \alpha_1 u_1) \dots (u_2 - \alpha_r u_1) = 0$ . Следовательно, над этим алгебраическим расширением поля  $F$  разности  $u_2 - \alpha_i u_1$  являются делителями нуля. Поэтому  $D$  остается алгеброй с делением над всеми алгебраическими расширениями поля  $F$  только в случае  $n = 1$ , т. е. когда  $D = F$ .

**Теорема 16.5.2.** *Простое кольцо  $R$  есть полное матричное кольцо над алгеброй с делением  $D$ , содержащейся в  $R$ .*

**Доказательство.** Пусть  $e_{11}R$  — минимальный правый идеал кольца  $R$ ,  $e_{11}$  — идемпотент. Тогда  $1 - e_{11}$  — также идемпотент и  $R = e_{11}R \oplus (1 - e_{11})R$ . Если  $e_2R$  — минимальный правый идеал кольца  $(1 - e_{11})R$  и  $e_2$  — идемпотент, то  $(1 - e_{11})e_2 = e_2$ , откуда  $e_{11}e_2 = 0$ . Элемент  $e_{22} = e_2 - e_2e_{11}$  также идемпотент,  $e_{22}R = e_2R$  и  $e_{11}e_{22} = 0$ ,  $e_{22}e_{11} = 0$ . Тогда  $R = e_{11}R \oplus e_{22}R \oplus (1 - e_{11} - e_{22})R$ . Пусть мы уже нашли такие ортогональные идемпотенты  $e_{11}, \dots, e_{ii}$ , что  $e_{jj}R$ ,  $j = 1, \dots, i$ , — минимальные правые идеалы и  $R = e_{11}R \oplus e_{22}R \oplus \dots \oplus e_{ii}R \oplus (1 - e_{11} - \dots - e_{ii})R$ . Тогда определим  $e_{i+1}$  как такой идемпотент, что  $e_{i+1}R$  — минимальный правый идеал в кольце  $(1 - e_{11} - \dots - e_{ii})R$ . Тогда  $e_{i+1} = (1 - e_{11} - \dots - e_{ii})e_{i+1}$ , откуда  $e_{jj}e_{i+1} = e_{jj}(1 - e_{11} - \dots - e_{ii})e_{i+1} = 0$ ,  $j = 1, \dots, i$ . Если положить  $e_{i+1, i+1} = e_{i+1}(1 - e_{11} - \dots - e_{ii})$ , то мы получим идемпотент  $e_{i+1, i+1}$ , ортогональный к идемпотентам  $e_{11}, \dots, e_{ii}$  и такой, что  $e_{i+1, i+1}R = e_{i+1}R$ . Продолжая это построение, мы находим, что

$$R = e_{11}R \oplus e_{22}R \oplus \dots \oplus e_{nn}R,$$

где  $e_{ii}$  — ортогональные идемпотенты,  $e_{11} + e_{22} + \dots + e_{nn} = 1$ , а  $e_{ii}R$  — минимальные правые идеалы.

**Лемма 16.5.1.**  $e_{ii}Re_{jj} \neq 0$ , где  $i, j = 1, \dots, n$ .

**Доказательство.** Все конечные суммы  $\sum_k u_k e_{ii} v_k$  образуют двусторонний идеал, содержащий идемпотент  $e_{ii} \neq 0$ . Поэтому этот идеал совпадает со всем кольцом  $R$ . Значит, для подходящих элементов  $u_k, v_k$  имеем  $\sum_k u_k e_{ii} v_k = e_{jj}$ , или  $\sum_k u_k e_{ii} v_k e_{jj} = e_{jj}$ . Следовательно, для некоторого  $v$

$$e_{ii} v e_{jj} \neq 0.$$

**Лемма 16.5.2.**  $e_{ii}Re_{ii}$  — алгебра с делением  $D_i$ .

**Доказательство.** Ясно, что множество  $e_{ii}Re_{ii}$  замкнуто относительно операций сложения и умножения, т. е. является

подкольцом кольца  $R$ , единицей которого является идемпотент  $e_{ii}$ . Поэтому достаточно указать элементы, обратные к элементам, отличным от 0. Если  $e_{ii}xe_{ii} \neq 0$ , то  $e_{ii}xe_{ii}R$  — правый идеал, отличный от нуля, содержащийся в минимальном правом идеале  $e_{ii}R$  и поэтому совпадающий с ним. Следовательно, для некоторого элемента  $y$  имеем  $e_{ii}xe_{ii}y = e_{ii}$ , или  $e_{ii}xe_{ii} \cdot e_{ii}ye_{ii} = e_{ii}$ . Таким образом, элемент  $e_{ii}ye_{ii}$  является обратным к элементу  $e_{ii}xe_{ii}$  в кольце  $e_{ii}Re_{ii}$ , которое, следовательно, является кольцом с делением. Обозначим его через  $D_i$ .

Выберем для  $i = 2, \dots, n$  элементы  $e_{11}be_{ii} \neq 0$  и положим  $e_{11}be_{ii} = e_{1i}$ . Тогда

$$e_{11}e_{1i} = e_{1i}e_{ii} = e_{1i}.$$

Здесь  $e_{1i}R \subseteq e_{11}R$ , откуда  $e_{1i}R = e_{11}R$ . Поэтому для некоторого  $y$   $e_{1i}y = e_{11}$ ,  $e_{1i}(e_{ii}ye_{11}) = e_{11}$ . Пусть  $e_{1i} = e_{ii}ye_{11}$ . Тогда при  $i = 2, \dots, n$

$$e_{ii}e_{1i} = e_{1i}e_{ii} = e_{ii}, \quad e_{1i}e_{ii} = e_{ii}.$$

Отсюда  $e_{1i}e_{ii}e_{1i}e_{ii} = e_{ii}^2 = e_{ii}$ , поэтому  $e_{ii}e_{1i} \neq 0$ . Но  $(e_{ii}e_{1i})^2 = e_{ii}e_{1i}e_{1i}e_{ii} = e_{ii}$  — идемпотент в кольце  $e_{ii}Re_{ii}$ , откуда  $e_{ii}e_{1i} = e_{ii}$  — единица, являющаяся единственным ненулевым идемпотентом в кольце с делением. Положим теперь  $e_{ij}e_{1j} = e_{ij}$  при  $i \neq j$ . Тогда  $e_{ij}e_{jk} = e_{ii}e_{1j}e_{j1}e_{1k} = e_{ii}e_{11}e_{1k} = e_{ii}e_{1k} = e_{ik}$ . Аналогично  $e_{ij}e_{kt} = e_{ij}e_{jj}e_{kk}e_{kt} = 0$  при  $j \neq k$ . Таким образом, для  $n^2$  единиц  $e_{ij}$  мы установили следующее правило умножения:

$$e_{ij}e_{kt} = \delta_{jk}e_{it}, \quad \delta_{jj} = 1, \quad \delta_{jk} = 0, \quad j \neq k,$$

т. е. единицы  $e_{ij}$  перемножаются точно так же, как матрицы

$E_{ij} = (a_{rs})$ ,  $a_{ij} = 1$ ,  $a_{rs} = 0$ , если  $(r, s) \neq (i, j)$ ;  $i, j = 1, \dots, n$ .

Теперь для кольца с делением  $D_1 = e_{11}Re_{11}$  определяем кольцо  $D$ , состоящее из элементов

$$d = d_1 + e_{21}d_1e_{12} + \dots + e_{nn}d_1e_{1n},$$

где  $d_i \in D_1$ . Легко убедиться в том, что кольцо  $D$  изоморфно кольцу  $D_1$  и, значит, также является алгеброй с делением. При этом изоморфизме единице  $e_{11}$  кольца  $D_1$  соответствует  $e_{11} + e_{22} + \dots + e_{nn} = 1$  — единица кольца  $D$ , а также кольца  $R$ . Для  $d \in D$  имеем  $e_{ij}d = e_{i1}d_1e_{1j} = de_{ij}$ .

Наконец, для произвольного элемента  $x \in R$  получаем  $x = 1x1 = (e_{11} + \dots + e_{nn})x(e_{11} + \dots + e_{nn}) = \sum_{i,j} e_{ii}xe_{jj}$ , но  $x_{ij} = e_{ii}xe_{jj} = e_{ii}e_{1i}xe_{j1}e_{1j} = e_{ii}e_{1i}e_{1j}$

для некоторого элемента  $u_1 \in D_1$ , откуда для  $u \in D$  имеем  $x_{ij} = ue_{ij} = e_{ij}u$ . Этим завершается доказательство теоремы. Мы показали, что простое кольцо  $R$  может быть представлено в явном виде как кольцо матриц порядка  $n$  над алгеброй с делением  $D$ , единица которой совпадает с единицей кольца  $R$ .

**Теорема 16.5.3.** *Если  $R_G$  — полупростое групповое кольцо над полем  $F$ , то существует алгебраическое расширение  $F^*$  поля  $F$ , над которым кольцо  $R_G$  распадается в прямую сумму полных матричных колец над полем  $F^*$ . В качестве расширения  $F^*$  можно выбрать конечное алгебраическое расширение поля  $F$ .*

**Доказательство.** Кольцо  $R_G$  является полупростым над полем  $F$  тогда и только тогда, когда характеристика поля не делит порядок группы  $G$ . Это свойство будет сохраняться, если поле  $F$  заменить его алгебраическим расширением  $F^*$ . Если в разложении кольца  $R_G$  над полем  $F$  в прямую сумму простых колец  $R_1 \boxplus R_2 \boxplus \dots \boxplus R_s$  существует некоторое простое кольцо  $R_k$ , соответствующая алгебра с делением  $D$  которого не совпадает с полем  $F$ , то алгебра  $D$  при некотором алгебраическом расширении  $F^*$  поля  $F$  перестает быть алгеброй с делением. При этом расширении разложение кольца  $R_G$  претерпевает одно из следующих изменений: (1) увеличивается (но, конечно, не уменьшается) число идемпотентов центра кольца  $R$ , и, таким образом, некоторое простое кольцо дальше распадается в прямую сумму нескольких простых колец; или (2) в простом кольце  $R$  содержится тело  $D^*$  меньшей размерности, а кольцо  $R$  представляется как большее матричное кольцо над телом  $D^*$ . Оба эти изменения возможны. Первый случай мы наблюдали, когда находили представления группы порядка 3. Второй возникает в кольце  $R_Q$  группы кватернионов  $Q$  над полем рациональных чисел  $F$ . Кольцо  $R_Q$  над полем  $F$  — это прямая сумма четырех простых колец размерности 1 и одного — размерности 4. Последнее является алгеброй с делением (алгеброй кватернионов). Если присоединить комплексное число  $i$  к полю  $F$ , то алгебра с делением превращается в алгебру матриц порядка 2 над полем комплексных рациональных чисел.

В любом из этих случаев алгебраическое замыкание  $\bar{F}$  поля  $F$  является полем, над которым любая простая алгебра  $R_k$ , являющаяся слагаемым для  $R_G$ , есть матричное кольцо над полем  $\bar{F}$ . Матричные единицы  $e_{ij}^k$  простых колец  $R_k$  можно представить через элементы  $x$  группы  $G$ , а любое поле  $F^*$ , содержащее все возникающие при этом коэффициенты, таково, что  $R_k$  — полные матричные алгебры над полем  $F^*$ . Последнее, разумеется, является конечным расширением поля  $F$ .

**Теорема 16.5.4.** *Центр полной матричной алгебры  $R_k$  над полем  $F$  состоит из скалярных кратных единицы алгебры  $R_k$*

являющейся единичной матрицей. Базис центра прямой суммы матричных колец  $R = R_1 + \dots + R_r$  над полем  $F$  составляют  $r$  единиц колец  $R_1, \dots, R_r$ .

*Доказательство.* Пусть  $R_k$  — полная матричная алгебра над полем  $F$ . Предположим, что элемент

$$x = \sum_{i,j} a_{ij} e_{ij}, \quad a_{ij} \in F,$$

находится в центре алгебры  $R_k$ . Из условия  $e_{rs}x = xe_{rs}$  находим

$$\sum_j a_{sj} e_{rj} = \sum_i a_{ir} e_{is}.$$

Поэтому  $a_{sj} = 0$  при  $j \neq s$  и  $a_{ss} = a_{rr}$ , откуда  $x = a_{11}(e_{11} + \dots + e_{nn}) = a_{11} \cdot 1$ , и, наоборот, все элементы такого вида содержатся в центре алгебры  $R_k$ . Если

$$R = R_1 + \dots + R_r,$$

то центр алгебры  $R$  — прямая сумма центров алгебр  $R_k$ . Поэтому базис центра кольца  $R$  состоит из  $r$  единиц алгебр  $R_k$ .

Мы получили уже ряд результатов, связывающих представления группы  $G$  с полупростыми групповыми алгебрами  $R_G$ . Подведем итог.

**Теорема 16.5.5.** Любое неприводимое обыкновенное представление конечной группы  $G$  является компонентой правого регулярного представления  $R(G)$ . Число неэквивалентных абсолютно неприводимых представлений равно числу классов сопряженных элементов группы  $G$ . Если  $\rho_1, \dots, \rho_r$  — различные абсолютно неприводимые представления степеней  $n_1, \dots, n_r$  соответственно, то степень представления  $\rho_i$  равна  $n_i^2$  над полем  $F$  и  $\rho_i$  встречается  $n_i$  раз в представлении  $R(G)$ . Единственными матрицами, перестановочными с представлением  $\rho_i(x)$ ,  $x \in G$ , являются скалярные кратные единицы. Если  $g$  — порядок группы  $G$ , то  $g = n_1^2 + n_2^2 + \dots + n_r^2$ .

*Доказательство.* По теореме 16.4.4 любое неприводимое обыкновенное представление эквивалентно представлению в некотором минимальном правом идеале алгебры  $R_G$  и в этом смысле является компонентой представления  $R(G)$ . Число неэквивалентных неприводимых представлений равно числу простых идеалов в  $R_G$ . Над полем  $F$  или над его расширением  $F^*$  центр кольца  $R_G$  обладает базисом из  $r$  идемпотентов, а само  $R_G$  по теореме 16.5.4 — прямая сумма  $r$  полных матричных алгебр. Но в силу теоремы 16.4.5 базис центра кольца  $R_G$  состоит из сумм  $C_i$  элементов классов сопряженных элементов группы  $G$ . Поэтому  $r$  — число классов сопряженных элементов группы  $G$ . Над полем  $F^*$

минимальный правый идеал, содержащийся в подкольце  $R_i$ , имеет вид  $e_{11}R$ . Если же  $R_i$  — полная алгебра матриц порядка  $n_i$ , то этот идеал имеет базис  $e_{11}, e_{12}, \dots, e_{1n_i}$ . Соответствующее представление  $\rho_i$  имеет степень  $n_i$ . Представление алгебры  $R_G$ , индуцированное представлением  $\rho_i$ , является точным представлением простой алгебры  $R_i$ , а остальные простые алгебры отображаются в нуль, так как, согласно теореме 16.4.4,  $\rho_i(e_j) = 0$ , если  $e_j$  — единица подалгебры  $R_j$ ,  $j \neq i$ . Таким образом,  $\rho_i(R_G)$  — полная матричная алгебра размерности  $n_i^2$  над полем  $F^*$ , конечно, абсолютно неприводимая, так как дальнейшее разложение было бы возможно только в случае, если бы это представление было меньшей степени над полем  $F^*$ . Далее, единственными матрицами порядка  $n_i$ , перестановочными с каждой матрицей  $\rho_i(x)$ ,  $x \in G$ , являются скалярные кратные единичной матрицы. Наконец, так как каждое кольцо  $R_i$  имеет базис из  $n_i^2$  элементов, их прямая сумма обладает базисом, состоящим из  $n_1^2 + \dots + n_r^2$  элементов. Но кольцо  $R_G$  имеет также базис, состоящий из  $g$  элементов группы  $G$ . Следовательно,

$$g = n_1^2 + \dots + n_r^2.$$

$R_i$  является прямой суммой  $n_i$  минимальных правых идеалов  $e_{11}R, \dots, e_{n_i n_i}R$ , и поэтому представление  $\rho_i$  встречается в представлении  $R(G)$  точно  $n_i$  раз.

## 16.6. Соотношения между обыкновенными характерами

В предыдущем параграфе исследовались представления группы  $G$ , которые определялись строением алгебры  $R_G$  и тем фактом, что представление группы  $G$  индуцирует представление алгебры  $R_G$ . В этом параграфе мы рассмотрим соотношения между характерами  $\chi(x)$ ,  $x \in G$ . Они более тесно связаны с самой группой  $G$ , чем с алгеброй  $R_G$ . В этом параграфе будем рассматривать только представления над полем, характеристика которого взаимно проста с порядком группы.

**Теорема 16.6.1.** Пусть  $A$  и  $B$  — два  $F$ - $G$ -модуля. Если модуль  $A$  размерности  $m$  определяет представление  $\rho(x)$ ,  $x \in G$ , а модуль  $B$  размерности  $n$  определяет представление  $\sigma(x)$ , то аддитивная группа операторных гомоморфизмов модуля  $A$  в  $B$  изоморфна аддитивной группе всех матриц  $\alpha$  размерности  $m \times n$ , таких, что  $\rho(x)\alpha = \alpha\sigma(x)$ ,  $x \in G$ .

**Следствие 16.6.1.** Кольцо операторных эндоморфизмов модуля  $A$  в себя изоморфно алгебре матриц  $\alpha$  порядка  $m$ , таких, что  $\rho(x)\alpha = \alpha\sigma(x)$ .

**Доказательство.** Пусть  $u_1, \dots, u_m$  — базис модуля  $A$  и  $v_1, \dots, v_n$  — базис модуля  $B$ . Тогда каждое линейное отображение модуля  $A$  в модуль  $B$  определяется заданием образов элементов базиса. Пусть

$$\begin{aligned} u_1 &\rightarrow a_{11}v_1 + \dots + a_{1n}v_n, \\ &\dots \dots \dots \dots \dots \\ u_i &\rightarrow a_{i1}v_1 + \dots + a_{in}v_n, \\ &\dots \dots \dots \dots \dots \\ u_m &\rightarrow a_{m1}v_1 + \dots + a_{mn}v_n, \end{aligned}$$

и пусть  $\alpha = (a_{ij})$ ,  $i = 1, \dots, m$ ;  $j = 1, \dots, n$ . Эти линейные отображения образуют аддитивную группу, изоморфную аддитивной группе матриц  $\alpha$ . Если, кроме того, эти линейные отображения являются операторными гомоморфизмами, то из соответствия  $u \rightarrow v$  следует, что  $ux \rightarrow vx$  для всех  $x \in G$ . Это означает, что отображения  $u \rightarrow ux \xrightarrow{\alpha} (vx)$  и  $u \xrightarrow{\alpha} v \rightarrow vx$  совпадают, откуда

$$\rho(x)\alpha = \alpha\rho(x), \quad x \in G.$$

Если модуль  $A$  отображается в себя, то такие отображения называются *эндоморфизмами*. Если  $\alpha$  и  $\beta$  — два операторных эндоморфизма, то имеем

$$\rho(x)(\alpha\beta) = [\rho(x)\alpha]\beta = [\alpha\rho(x)]\beta = (\alpha\beta)\rho(x),$$

и, таким образом, алгебра матриц  $\alpha$  со свойством  $\rho(x)\alpha = \alpha\rho(x)$  изоморфна алгебре операторных эндоморфизмов модуля  $A$ .

Теорема 16.6.2 справедлива для любых  $\Omega$ -модулей, где  $\Omega$  — произвольное множество операторов, но нас интересуют главным образом  $F$ - $G$ -модули.

**Теорема 16.6.2. (Лемма Шура.)** *Если  $A$  и  $B$  — два неприводимых  $\Omega$ -модуля, то они либо операторно изоморфны, либо единственным операторным гомоморфизмом  $A$  в  $B$  является нулевой гомоморфизм. Если модуль  $A$  неприводим, то любой его операторный эндоморфизм, не равный тождественно нулю, является операторным изоморфизмом.*

**Доказательство.** Пусть  $u \in A$ ,  $v \in B$ ,  $\omega \in \Omega$ . Если тогда для некоторого  $u \in A$  операторный гомоморфизм отображает  $u$  в  $v \neq 0$ , то  $u\omega \rightarrow v\omega$  для всех  $\omega \in \Omega$ . При этом  $u\Omega$  — подмодуль модуля  $A$ , а так как модуль  $A$  неприводим,  $u\Omega = A$ . Таким образом,  $A = u\Omega \rightarrow v\Omega \neq 0$ , откуда  $A \rightarrow v\Omega = B$ . Это отображение должно быть взаимно однозначным, так как в противном случае ненулевые элементы модуля  $A$ , отображаемые в нуль, образуют  $\Omega$ -подмодуль модуля  $A$ , что противоречит его неприводимости. Следовательно, это отображение — изоморфизм. Поэтому, в частности, любой операторный эндоморфизм модуля  $A$  в себя есть операторный изоморфизм.

**Теорема 16.6.3.** Если  $\rho$  и  $\sigma$  — два неприводимых неэквивалентных представления конечной группы  $G$  степеней  $m$  и  $n$  соответственно и  $\xi$  — любая матрица размерности  $m \times n$ , то

$$\sum_{y \in G} \rho(y) \xi \sigma(y^{-1}) = 0.$$

*Доказательство.* Пусть  $\alpha = \sum_{y \in G} \rho(y) \xi \sigma(y^{-1})$ . Тогда для  $x \in G$ ,

$$xy = z, \quad y^{-1} = z^{-1}x$$

$$\begin{aligned} \rho(x)\alpha &= \sum_y \rho(x)\rho(y)\xi\sigma(y^{-1}) = \\ &= \sum_y \rho(xy)\xi\sigma(y^{-1}) = \\ &= \sum_z \rho(z)\xi\sigma(z^{-1})\sigma(x) = \\ &= \alpha\sigma(x). \end{aligned}$$

Поэтому в силу теорем 16.6.1 и 16.6.2, а также в силу неприводимости и неэквивалентности представлений  $\rho$  и  $\sigma$ ,  $\alpha = 0$ . Заметим, что эти теоремы справедливы для представлений группы  $G$  над произвольным полем.

Если  $f_1(y)$  и  $f_2(y)$  — две произвольные функции на группе  $G$  со значениями в поле  $F$  (предполагаем, что характеристика поля  $F$  не делит порядок группы  $G$ ), то *симметричным билинейным скалярным произведением* называется число

$$(f_1, f_2) = \frac{1}{g} \sum_{y \in G} f_1(y) f_2(y^{-1}).$$

Учитывая, что  $y^{-1}$  пробегает всю группу  $G$ , когда  $y$  пробегает всю группу  $G$ , легко проверить следующие свойства:

- 1)  $(f_1, f_2) = (f_2, f_1)$ ,
- 2)  $(f_1 + f_2, f_3) = (f_1, f_3) + (f_2, f_3)$ ,
- 3)  $(af_1, f_2) = a(f_1, f_2)$ ,  $a \in F$ .

Предположим теперь, что  $\rho(x)$  и  $\sigma(x)$  — неприводимые неэквивалентные представления. Если в теореме 16.6.3 положить  $\xi = e_{rs}$ , где  $e_{rs}$  — матрица размерности  $m \times n$  с единицей на месте  $(r, s)$  и нулями на всех остальных местах, то мы находим матрицу  $\alpha = (\alpha_{ij})$ , где  $\alpha_{ij} = \sum_{y \in G} \rho_{ir}(y) \sigma_{sj}(y^{-1})$ . При этом

$$\rho(x) = (\rho_{ij}(x)), \quad i, j = 1, \dots, m,$$

$$\sigma(x) = (\sigma_{ij}(x)), \quad i, j = 1, \dots, n.$$

Так как, согласно теоремам 16.6.1 и 16.6.2,  $\alpha = 0$ , справедливы равенства  $(\rho_{ir}, \sigma_{sj}) = 0$ . Мы можем показать даже больше.

**Теорема 16.6.4.** Если  $\rho$  и  $\sigma$  — неэквивалентные неприводимые представления конечной группы  $G$ , то симметрическое билинейное скалярное произведение  $(\rho_{ir}, \sigma_{sj}) = 0$  при любых индексах  $i, r, s, j$ . Если  $\rho$  — абсолютно неприводимое представление степени  $n$ , то  $(\rho_{ir}, \rho_{sj}) = 0$ , если  $i \neq j$  или  $r \neq s$ ; в оставшемся случае  $(\rho_{ij}, \rho_{ji}) = \frac{1}{n}$  при любых индексах  $i$  и  $j$ .

**Доказательство.** Первую часть теоремы мы уже доказали. Теперь рассмотрим абсолютно неприводимое представление  $\rho$  степени  $n$  группы  $G$ . Если  $\xi$  — произвольная матрица порядка  $n$ , то, как и прежде,

$$\alpha = \frac{1}{g} \sum_{y \in G} \rho(y) \xi \rho(y^{-1}),$$

где  $\alpha$  — такая матрица, что  $\rho(x)\alpha = \alpha\rho(x)$  для всех значений  $x \in G$ . Следовательно, по теореме 16.5.5 матрица  $\alpha$  представима, как скалярное кратное единичной матрицы,  $\alpha = \lambda I_n$ , где скаляр  $\lambda$  зависит от матрицы  $\xi$ . Если  $\xi = e_{rs}$ , то соответствующее значение  $\lambda$  обозначим через  $\lambda_{rs}$ . Тогда  $\lambda_{rs}\delta_{ij} = (\rho_{ir}, \rho_{sj})$ . Но  $(\rho_{ir}, \rho_{sj}) = (\rho_{sj}, \rho_{ir})$ , поэтому  $\lambda_{rs}\delta_{ij} = \lambda_{ji}\delta_{sr} = 0$ , если только  $i \neq j$  и  $r \neq s$ , в то время как  $(\rho_{ij}, \rho_{ji}) = \lambda_{ii} = (\rho_{ji}, \rho_{ij}) = \lambda_{jj}$ . Следовательно,  $\lambda_{11} = \lambda_{22} = \dots = \lambda_{nn} = \lambda$ . Таким образом,

$$\begin{aligned} n\lambda &= \sum_j \lambda_{jj} = \\ &= \frac{1}{g} \sum_{y, j} \rho_{ij}(y) \rho_{ji}(y^{-1}) = \\ &= \frac{1}{g} \sum_y \rho_{ii}(1) = 1, \end{aligned}$$

откуда  $\lambda = 1/n$ . Теорема доказана. Заметим, что из равенства  $n\lambda = 1$  следует, что степень  $n$  не делится на характеристику поля  $F$ .

Эти результаты переносятся на характеристы.

**Теорема 16.6.5.** Если  $\chi, \psi$  — различные неприводимые характеристы, то  $(\chi, \psi) = 0$ . Если  $\chi$  — абсолютно неприводимый характер, то  $(\chi, \chi) = 1$ .

**Доказательство.** Если  $\chi$  и  $\psi$  — неприводимые характеристы представлений  $\rho$  и  $\sigma$ , то  $\chi(y) = \sum_i \rho_{ii}(y)$ ,  $\psi = \sum_j \sigma_{jj}(y)$  для  $y \in G$ . Так как скалярное произведение билинейно, то

$$(\chi, \psi) = \sum_{i, j} (\rho_{ii}, \sigma_{jj}) = 0,$$

поскольку каждое слагаемое равно нулю. Пусть теперь  $\chi$  — абсолютно неприводимый характер представления  $\rho$  степени  $n$ . Тогда

$$\langle \chi, \chi \rangle = \sum_{i,j} (\rho_{ii}, \rho_{jj}) = \sum_{i,i} (\rho_{ii}, \rho_{ii}) = \sum_i \frac{1}{n} = 1,$$

что и требовалось доказать.

**Следствие 16.6.2.** Для единичного представления  $\sum_{x \in G} \chi(x) = g$ .

Для любого другого неприводимого представления  $\sum_{x \in G} \chi(x) = 0$ .

Действительно,  $\chi(x) = 1$  для любого  $x$  при единичном представлении, откуда  $\sum_{x \in G} \chi(x) = g$ . Но если  $\chi$  — характер любого другого неприводимого представления, то обозначим через  $\psi$  характер единичного представления. Тогда  $\langle \chi, \psi \rangle = 0$ , откуда  $\frac{1}{g} \sum_{x \in G} \chi(x) = 0$ .

**Теорема 16.6.6.** Если  $\chi$  и  $\psi$  — характеристы и  $\chi = \sum a_i \chi_i$ ,  $\psi = \sum b_i \chi_i$ , где  $\chi_i$ ,  $i = 1, \dots, r$ , — абсолютно неприводимые характеристы, то  $\langle \chi, \psi \rangle = \sum a_i b_i$ . Чтобы характер  $\varphi$  был абсолютно неприводимым над полем  $F$ , характеристика которого равна нулю, необходимо и достаточно, чтобы  $\langle \varphi, \varphi \rangle = 1$ .

**Доказательство.** Эта теорема получается как следствие из теоремы 16.6.5, если применить свойство билинейности скалярного произведения. Если  $\varphi = \sum c_i \chi_i$ , то коэффициенты  $c_i$  — неотрицательные целые числа, а если  $\langle \varphi, \varphi \rangle = \sum c_i^2 = 1$ , то в поле характеристики нуль один из коэффициентов  $c_i$  равен 1, а все остальные — нулю.

**Теорема 16.6.7.** Все абсолютно неприводимые представления абелевой группы  $G$  одномерны.

**Доказательство.** Так как группа  $G$  абелева, каждый элемент представляет собой класс сопряженных элементов, и поэтому, если  $g$  — порядок группы  $G$ , то существует  $g$  абсолютно неприводимых представлений степеней  $n_1, n_2, \dots, n_g$ , где  $g = n_1^2 + n_2^2 + \dots + n_g^2$ , откуда  $n_1 = n_2 = \dots = n_g = 1$ . При этом для любого представления  $\rho$  степени 1 мы имеем  $\chi(x) = \rho(x)$ , т. е. абсолютно неприводимые представления задаются характерами и являются по сути характерами абелевой группы, рассмотренной в гл. 13.

**Теорема 16.6.8.** Пусть  $x$  — элемент порядка  $t$  из группы  $G$ , и пусть  $\rho(x)$  — ее представление степени  $n$ . Тогда, присоединяя, если нужно, корни степени  $t$  из единицы к полю  $F$ , получаем, что матрица  $\rho(x)$  подобна диагональной матрице,

элементами которой являются корни степени  $m$  из единицы. Если  $F$  — поле комплексных чисел, то  $\chi(x^{-1}) = \overline{\chi(x)}$ , где черта означает комплексное сопряжение.

**Доказательство.** Матрицы  $1, \rho(x), \dots, \rho(x^{m-1})$  представляют циклическую группу  $C$  порядка  $m$ . Но степень абсолютно неприводимых представлений  $\sigma(x)$  группы  $C$  равна единице. Пусть  $\sigma(x) = (b)$ , тогда  $b^m = 1$ , так как  $1 = x^m$ , т. е.  $b$  есть корень степени  $m$  из единицы. Легко проверить, что в алгебре  $R_C$  элементы вида  $(1/m)(1 + \omega x + \omega^2 x^2 + \dots + \omega^{m-1} x^{m-1})$ , где  $\omega$  проходит все корни степени  $m$  из единицы, являются идемпотентами порождающими неприводимые представления. Следовательно, при присоединении корней степени  $m$  из единицы к полю  $F$  (характеристика которого, конечно, не делит  $m$ ) представление  $\rho(x)$  группы  $C$  вполне приводимо, и матрица  $\rho(x)$  подобна диагональной матрице с элементами  $b_1, \dots, b_n$  на главной диагонали, где  $b_i$  — корень степени  $m$  из единицы. Следовательно,  $\chi(x) = b_1 + \dots + b_n$ . Тогда  $\rho(x^{-1})$  подобна диагональной матрице с элементами  $b_1^{-1}, \dots, b_n^{-1}$  на главной диагонали и  $\chi(x^{-1}) = b_1^{-1} + \dots + b_n^{-1}$ . Если же  $F$  — поле комплексных чисел, то обратным элементом к любому корню из единицы является комплексно сопряженное число  $b_i^{-1} = \bar{b}_i$ , и поэтому  $\chi(x^{-1}) = \overline{\chi(x)}$ .

Пусть  $\rho$  — произвольное представление группы  $G$ . Для каждого элемента  $x \in G$  определяем представление  $\hat{\rho}(x) = \rho(x^{-1})^T$ , где  $T$  означает транспонирование матрицы. Тогда

$$\begin{aligned}\hat{\rho}(xy) &= \rho(y^{-1}x^{-1})^T = [\rho(y^{-1})\rho(x^{-1})]^T = \\ &= \rho(x^{-1})^T\rho(y^{-1})^T = \hat{\rho}(x)\hat{\rho}(y).\end{aligned}$$

Представление  $\hat{\rho}$  называется *контраградиентным* по отношению к представлению  $\rho$ .

Предположим, что  $L$  — модуль представления  $\rho$  с базисом  $u_1, \dots, u_n$  над полем  $F$ . Пусть  $\hat{L}$  — другое пространство над полем  $F$  с базисом  $v_1, \dots, v_n$ . Определяем скалярное произведение  $u \cdot v$

элементов  $u = a_1u_1 + \dots + a_nu_n \in L$  и  $v = b_1v_1 + \dots + b_nv_n \in \hat{L}$ :

$$u \cdot v = a_1b_1 + a_2b_2 + \dots + a_nb_n \in F.$$

Это скалярное произведение является билинейной функцией на множестве  $(L, \hat{L})$ , определяемой равенствами  $u_i v_j = \delta_{ij}$ .

Мы превратим  $v_1, v_2, \dots, v_n$  в базис для представления  $\rho$ , положив

$$v_i x = \sum_j \hat{\rho}_{ij}(x) v_j = \sum_j \rho_{ji}(x^{-1}) v_j.$$

Тогда

$$\begin{aligned} u_i x \cdot v_j x &= \sum_{k,s} \rho_{ik}(x) \rho_{sj}(x^{-1}) (u_k \cdot v_s) = \\ &= \sum_k \rho_{ik}(x) \rho_{kj}(x^{-1}) = \delta_{ij}, \end{aligned}$$

так как  $\rho(x)\rho(x^{-1}) = I_n$ . Таким образом,  $ux \cdot vx = u \cdot v$  для всех элементов  $u \in L$ ,  $v \in L$  и  $x \in G$ , т. е. скалярное произведение сохраняется, если на оба сомножителя подействовать одним и тем же элементом группы  $G$ . Для каждого подпространства  $M'$  пространства  $L$  определим подпространство  $M$  пространства  $L$ , состоящее из всех таких элементов  $u \in L$ , что  $u \cdot v = 0$  для всех  $v \in M'$ . Тогда  $\dim M' + \dim M = n$  и установленное соответствие является дуальным соотношением между подпространствами пространств  $L$  и  $L$ . Если  $M'$  — подмодуль представления в  $L$  и  $v \in M'$ , то для  $x \in G$  также  $vx^{-1} \in M'$ . Поэтому  $vx^{-1} \cdot u = 0$  и  $v \cdot ux = 0$  для всех  $v \in M'$ ,  $u \in M$ , откуда  $ux \in M$ , т. е.  $M$  — также подмодуль представления. Поэтому, в частности, модуль  $L$  неприводим тогда и только тогда, когда неприводим модуль  $L$ . Если  $\rho$  — абсолютно неприводимое представление степени  $n$  над полем  $F$  (реализуется в пространстве размерности  $n^2$ ), степень представления  $\hat{\rho}$  над полем  $F$  также равна  $n$  (реализуется в пространстве размерности  $n^2$ ), т. е.  $\hat{\rho}$  — абсолютно неприводимое представление.

Из определения следует, что  $\hat{\hat{\rho}} = \rho$ . Если представления  $\rho$  и  $\sigma$  эквивалентны, то

$$S^{-1} \rho(x^{-1}) S = \sigma(x^{-1}).$$

для некоторой матрицы  $S$  и всех  $x \in G$ . Транспонируем левую и правую части:

$$S^T \rho(x^{-1})^T S^{T^{-1}} = \sigma(x^{-1})^T,$$

т. е. представления  $\hat{\rho}$  и  $\hat{\sigma}$  эквивалентны.

Пусть  $r$  — число классов сопряженных элементов группы  $G$ , а  $\rho_1, \dots, \rho_r$  — абсолютно неприводимые представления группы  $G$  над полем  $F$ , где  $\rho_1$  — единичное представление (соответствующее идемпотенту  $(1/g) \sum_{x \in G} x$ ):  $\rho_1(x) = 1$ ,  $x \in G$ . Тогда  $\rho_1 = \rho_1, \dots, \rho_r$  — те же самые представления, взятые в другом порядке. Аналогично пусть  $C_1, \dots, C_r$  — классы сопряженных элементов группы  $G$ , где  $C_1 = 1$  — класс, состоящий только из единицы. Элементы, обратные элементам класса  $C_i$ , образуют другой класс  $C'_i$ . Поэтому

$C'_1 = C_1, \dots, C'_r$  — те же самые классы, но взятые в другом порядке.

Если  $\chi(x)$  — характер представления  $\rho(x)$ , то обозначим характер представления  $\bar{\rho}(x)$  через  $\bar{\chi}(x)$ . Здесь  $\chi(x) = \text{след } \rho(x)$ ; тогда

$$\bar{\chi}(x) = \text{след } \rho(x^{-1})^T = \text{след } \rho(x^{-1}) = \chi(x^{-1}).$$

Как отмечалось в теореме 16.6.8, в поле комплексных чисел  $\chi(x^{-1}) = \overline{\chi(x)}$ , где черта означает комплексное сопряжение. Таким образом, наше обозначение согласуется с обозначением комплексной сопряженности над полем комплексных чисел. Заметим, что над этим полем равенство  $\bar{\rho} = \rho$  справедливо только в случае, когда все характеры  $\chi(x)$  представления  $\rho$  — действительные числа.

Обозначим через  $\chi_i^a$  абсолютно неприводимый характер некоторого элемента из класса  $C_i$  при представлении  $\rho_a$ , через  $h_i$  — число элементов класса  $C_i$ , т. е. индекс нормализатора некоторого элемента  $x \in C_i$ . Если порядок этого нормализатора равен  $g_i$ , то  $g_i h_i = g$ .

**Теорема 16.6.9.** Для абсолютно неприводимых характеров группы  $G$  справедливы соотношения ортогональности:

$$\sum_{i=1}^r \frac{\chi_i^a \bar{\chi}_i^b}{g_i} = \delta_{ab},$$

$$\sum_{a=1}^r \bar{\chi}_i^a \chi_j^a = \delta_{ij} g_j.$$

*Доказательство.* Согласно теореме 16.6.5,

$$\frac{1}{g} \sum_{x \in G} \chi^a(x) \bar{\chi}^b(x^{-1}) = \delta_{ab}.$$

Но  $\chi(x) = \chi(y)$ , если элементы  $x$  и  $y$  принадлежат одному классу  $C_i$  (тогда и элементы  $x^{-1}$  и  $y^{-1}$  принадлежат одному классу  $C_i$ ).  $\chi^b(x^{-1}) = \bar{\chi}^b(x)$ , следовательно, при  $x \in C_i$  наша исходная сумма содержит  $h_i$  членов, равных  $\chi_i^a \bar{\chi}_i^b$ . Поэтому

$$\sum_{i=1}^r \frac{h_i}{g} \chi_i^a \bar{\chi}_i^b = \delta_{ab},$$

или

$$\sum_{i=1}^r \frac{\chi_i^a \bar{\chi}_i^b}{g_i} = \delta_{ab}.$$

А это значит, что для матрицы  $M = (m_{ai})$ ,  $a, i = 1, \dots, r$ , где  $m_{ai} = \chi_i^a$ , матрица

$$M' = (r_{ib}), \quad i, b = 1, \dots, r,$$

где

$$r_{ib} = \frac{1}{g_i} \bar{\chi}_i^b,$$

такова, что  $MM' = I_r$ , т. е.  $M'$  — обратная матрица для матрицы  $M$ . Но тогда  $M'M = I_r$ , откуда

$$\sum_{a=1}^r \frac{1}{g_i} \chi_i^a \bar{\chi}_j^a = \delta_{ij},$$

а это и есть вторая формула, которую требовалось доказать.

Изучение структуры групповой алгебры дает возможность установить дальнейшие соотношения для характеров. Пусть

$$R_G = R_1 \boxplus \dots \boxplus R_a \boxplus \dots \boxplus R_r$$

— разложение алгебры  $R_G$  в прямую сумму простых алгебр, и пусть  $e_{ij}^a$ ,  $i, j = 1, \dots, n$ , — матричные единицы алгебры  $R_a$  и  $e_a = e_{11}^a + e_{22}^a + \dots + e_{nn}^a$  — единица алгебры  $R_a$ . Неприводимое представление  $\rho_a = \rho^a$ , соответствующее  $R_a$ , эквивалентно представлению в минимальном правом идеале алгебры  $R_a$ . Пусть этим правым идеалом будет идеал  $e_{11}^a R$  с базисом  $e_{11}^a, e_{12}^a, \dots, e_{1n}^a$ .

Тогда

$$e_{1i}^a x = \sum_j \rho_{ij}^a(x) e_{1j}^a, \quad i = 1, \dots, n.$$

Пусть теперь  $x = x_1 + \dots + x_a + \dots + x_r$ , где  $x_a \in R_a$ , причем

$$x_a = e_a x e_a = e_a x = x e_a.$$

Если

$$x_a = \sum_{i,j} x_{ij}^a e_{ij}^a,$$

мы имеем  $e_{1i}^a x = e_{1i}^a e_a x = e_{1i}^a x_a$  и

$$e_{1i}^a x e_{ij}^a = x_{ij}^a e_{1j}^a.$$

Но по определению представления

$$e_{1i}^a x e_{jj}^a = \rho_{ij}^a(x) e_{1j}^a.$$

Следовательно,  $x_{ij}^a = \rho_{ij}^a(x)$  во всех случаях, и поэтому

$$x_a = \sum_{i,j} \rho_{ij}^a(x) e_{ij}^a.$$

Будем писать  $C_k = \sum_{x \in C_k} x$ , употребляя одну и ту же букву для обозначения класса и суммы его элементов, рассматриваемой как элемент алгебры  $R_G$ . Такое обозначение не приведет к недоразумению. Тогда  $C_1, C_2, \dots, C_r$  образуют базис центра  $Z_G$  алгебры  $R_G$ . Пусть

$$C_k = C_k^1 + \dots + C_k^a + \dots + C_k^r,$$

где  $C_k^a \in R_a$ . Тогда, так как  $C_k^a$  — элемент центра алгебры  $R_a$ , он является скалярным кратным единицы  $e_a$ , т. е.  $C_k^a = u_k^a e_a$ . Но

$$\text{след } \rho^a(C_k^a) = \sum_{x \in C_k^a} \text{след } \rho^a(x),$$

откуда  $n_a u_k^a = h_k \chi_k^a$ , где  $n_a$  — степень представления  $\rho_a$ . Поэтому

$$u_k^a = \frac{h_k \chi_k^a}{n_a},$$

откуда

$$C_k^a = \frac{h_k \chi_k^a}{n_a} e_a.$$

Таблица умножения для базиса  $C_1, \dots, C_r$  центра  $Z(R_G)$  следующая:

$$C_j C_i = C_i C_j = \sum_k c_{ijk} C_k,$$

где над полем  $F$  характеристики нуль  $c_{ijk}$  — неотрицательные целые числа, так как произведение  $C_i C_j = C_j C_i$  не содержит отрицательных членов.

Так как  $R_G$  разлагается в прямую сумму простых алгебр  $R_a$ , компоненты  $C_i^a$  удовлетворяют тем же самым соотношениям, что и  $C_i$ . Поэтому справедлива

Теорема 16.6.10.

$$C_i^a C_j^a = C_j^a C_i^a = \sum_k c_{ijk} C_k^a, \quad a = 1, \dots, r,$$

и

$$\frac{h_i \chi_i^a}{n_a} \frac{h_j \chi_j^a}{n_a} = \sum_k c_{ijk} \frac{h_k \chi_k^a}{n_a}, \quad a = 1, \dots, r.$$

При доказательстве теоремы 16.6.4 мы установили, что  $n\lambda = 1$ , где  $n = n_a$  — степень абсолютно неприводимого представления. Поэтому деление на  $n_a$  в равенствах теоремы 16.6.10 допустимо.

Определим *тензорное произведение*  $L \times M$  двух пространств  $L$  и  $M$  над полем  $F$  следующим образом. Если  $u_1, \dots, u_m$  — базис пространства  $L$ , а  $v_1, \dots, v_n$  — базис про-

пространства  $M$ , то  $L \times M$  — линейное пространство над полем  $F$  с базисом  $u_i v_j$ ,  $i = 1, \dots, m$ ;  $j = 1, \dots, n$ . Если

$$\begin{aligned} u &= a_1 u_1 + \dots + a_m u_m \in L, \\ v &= b_1 v_1 + \dots + b_n v_n \in M, \end{aligned}$$

то произведение  $uv = \sum_{i,j} a_i b_j u_i v_j$  определено как элемент пространства  $L \times M$ . Можно проверить, что замена базиса пространства  $L$  или  $M$  соответствует замене базиса произведения  $L \times M$ . Если  $\rho$  есть  $F$ - $G$ -модуль представления  $\rho$  группы  $G$ , а  $\sigma$  есть  $F$ - $G$ -модуль представления  $\sigma$  группы  $G$ , то можно определить *кронекеровское произведение*  $\rho \times \sigma$  представлений  $\rho$  и  $\sigma$  как следующее представление группы  $G$  в модуле  $L \times M$ :

$$(uv)x = (ux)(vx), \quad u \in L, \quad v \in M, \quad x \in G.$$

Если представление  $\rho_1$  эквивалентно  $\rho$ , а  $\sigma_1$  эквивалентно  $\sigma$ , то представление  $\rho_1 \times \sigma_1$  эквивалентно представлению  $\rho \times \sigma$ , так как замена базисов пространств  $L$  и  $M$  ведет к замене базиса пространства  $L \times M$ .

**Теорема 16.6.11.** *Если  $\rho$  и  $\sigma$  — представления группы  $G$  с характерами  $\chi$  и  $\psi$  соответственно и если  $\varphi$  — характер представления  $\rho \times \sigma$ , то  $\varphi(x) = \chi(x)\psi(x)$  при любом  $x \in G$ .*

**Доказательство.** Если  $u_i x = \sum_j \rho_{ij}(x) u_j$ ,  $i = 1, \dots, m$ ,  $v_i x = \sum_j \sigma_{ij}(x) v_j$ ,  $i = 1, \dots, n$ , то

$$\chi(x) = \sum_i \rho_{ii}(x), \quad \psi(x) = \sum_i \sigma_{ii}(x).$$

Но

$$(u_i v_j) x = \sum_{k,t} [\rho_{ik}(x) u_k] [\sigma_{jt}(x) v_t],$$

откуда

$$\varphi(x) = \sum_{i,j} \rho_{ii}(x) \sigma_{jj}(x) = \left[ \sum_i \rho_{ii}(x) \right] \left[ \sum_j \sigma_{jj}(x) \right] = \chi(x)\psi(x).$$

Из определений тензорного и кронекеровского произведений видно, что они коммутативны и ассоциативны. Поэтому, если  $\rho_a$  и  $\rho_b$  — абсолютно неприводимые представления группы  $G$ , то

$$\rho_a \times \rho_b = \rho_b \times \rho_a = \sum_c g_{abc} \rho_c,$$

где  $g_{abc}$  — неотрицательные целые числа, а сумма означает разложение представления  $\rho_a \times \rho_b$  в прямую сумму неприводимых представлений  $\rho_c$ , каждое из которых имеет кратность  $g_{abc}$ . Аналогичная формула справедлива для характеров. Мы сформулируем этот факт в виде следующей теоремы.

**Теорема 16.6.12.** Для абсолютно неприводимых характеров группы  $G$  имеет место соотношение

$$\chi_i^a \chi_i^b = \sum_c g_{abc} \chi_i^c,$$

где  $g_{abc}$  — неотрицательные целые числа, образующие таблицу умножения некоторой коммутативной и ассоциативной алгебры.

Подытожим то, что мы узнали об отношениях характеров. Пусть  $C_1 = 1, C_2, \dots, C_r$  — классы сопряженных элементов группы  $G$ ;  $\rho_1 = 1$  (единичное представление),  $\rho_2, \dots, \rho_r$  — абсолютно неприводимые представления и  $\chi_i^a$  — характер элемента из класса  $C_i$  в представлении  $\rho_a$ :

	$C_1$	$\dots$	$C_i$	$\dots$	$C_r$
$\rho_1$	$\chi_1^1$	$\dots$	$\chi_i^1$	$\dots$	$\chi_r^1$
	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\rho_a$	$\chi_1^a$	$\dots$	$\chi_i^a$	$\dots$	$\chi_r^a$
	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\rho_r$	$\chi_1^r$	$\dots$	$\chi_i^r$	$\dots$	$\chi_r^r$

При этом пусть  $h_i$  — порядок класса  $C_i$  и  $g_i h_i = g$ . Установлены следующие соотношения для характеров:

- 1) из разных строк  $\sum_{i=1}^r \frac{\chi_i^a \chi_i^b}{g_i} = \delta_{ab}$ ,
- 2) из разных столбцов  $\sum_{a=1}^r \chi_i^a \chi_j^a = \delta_{ij} g_i$ ,
- 3) внутри одной строки  $\frac{h_i \chi_i^a}{n_a} \frac{h_j \chi_j^a}{n_a} = \sum_k c_{ijk} \frac{h_k \chi_k^a}{n_a}$ ,
- 4) внутри одного столбца  $\chi_i^a \chi_i^b = \sum_c g_{abc} \chi_i^c$ .

Здесь  $c_{ijk}$  и  $g_{abc}$  — неотрицательные целые числа, являющиеся элементами таблицы умножения коммутативных и ассоциативных алгебр.

Всякое представление группы  $G$  группой подстановок  $\pi(G)$  можно рассматривать также как матричное представление. Действительно, если

$$\pi(x) = \begin{pmatrix} u_1 & \dots & u_n \\ u_{i_1} & \dots & u_{i_n} \end{pmatrix}$$

при  $x \in G$ , то мы можем рассматривать это как представление  $\rho$  относительно базиса  $u_1, \dots, u_n$ , причем

$$u_j x = u_{i_j}.$$

Тогда  $\chi(x)$  — это число символов  $u_i$ , оставляемых на месте подстановкой  $\pi(x)$ .

**Теорема 16.6.13.** *Если  $\pi(G)$  — представление подстановками группы  $G$  порядка  $g$ , то  $\sum_{x \in G} \chi(x) = kg$ , где  $k$  — число областей транзитивности. При этом если рассматривать это представление как матричное, то оно содержит точно  $k$  единичных представлений.*

**Доказательство.** Пусть  $n_1, n_2, \dots, n_k$  — числа элементов в каждой из  $k$  областей транзитивности. Тогда индекс подгруппы  $H_j$ , оставляющей на месте символ  $a_j$  из  $j$ -й области транзитивности, равен  $n_j$ , а порядок этой группы —  $g/n_j$ . Следовательно, символ  $a_j$  остается на месте  $g/n_j$  раз под действием всех элементов группы  $G$ . Поэтому хоть один символ  $j$ -й области транзитивности остается на месте  $n_j \cdot g/n_j = g$  раз, а, значит, число случаев, когда не сдвигается хоть один из символов  $k$  областей транзитивности, равно  $kg$ , т. е.  $\sum_{x \in G} \chi(x) = kg$ . Если  $\chi = \sum_a m_a \chi^a$  — сумма абсолютно неприводимых характеров, то  $\sum_{x \in G} \chi(x) = m_1 g$  согласно следствию из теоремы 16.6.5. Следовательно, наше представление содержит единичное представление  $m_1 = k$  раз.

**Теорема 16.6.14.** *Если  $\chi$  — характер транзитивной группы подстановок  $G$ , то  $\sum_{x \in G} \chi^2(x) = tg$ , где  $t$  — число областей транзитивности подгруппы  $H$ , оставляющей на месте один символ;  $t$  равно также числу двойных смежных классов  $HxH$  группы  $G$  по  $H$ .*

**Доказательство.** Пусть  $G$  — транзитивная группа подстановок символов 1, 2, ...,  $n$  и  $H_i$  — подгруппа, оставляющая на месте символ  $i$  ( $i = 1, \dots, n$ ). Можно считать, что  $H = H_1$ , так как все подгруппы  $H_i$  сопряжены. Пусть  $h$  — порядок группы  $H$ . Тогда в силу предыдущей теоремы

$$\sum_{x \in H_i} \chi(x) = th.$$

Просуммируем это равенство по  $i$ :

$$\sum_i \sum_{x \in H_i} \chi(x) = tn h = tg.$$

Слева для каждой подгруппы  $H_i$ , содержащей элемент  $x$ , слагаемое  $\chi(x)$  встречается один раз. Но элемент  $x$  оставляет на месте  $\chi(x)$  букв и поэтому содержится в  $\chi(x)$  различных подгруппах  $H_i$  (это число равно нулю, если элемент  $x$  переставляет все буквы). Значит,

$$tg = \sum_i \sum_{x \in H_i} \chi(x) = \sum_{x \in G} \chi^2(x).$$

Легко видеть, что число  $t$  равно числу двойных смежных классов  $HxH$  группы  $G$ . Действительно, пусть  $G = H + Hx_2 + \dots + Hx_n$ , где  $H$  — подгруппа, оставляющая на месте 1, и  $x_i = (1, i, \dots)$ ,  $i = 2, \dots, n$ . Если  $Hx_iH = Hx_jH$ , то  $x_i = h_1x_jh_2$ ,  $h_1, h_2 \in H$ . Здесь элемент  $h_2$  отображает  $j$  в  $i$ , откуда символы  $i$  и  $j$  содержатся в одной области транзитивности группы  $H$ . Обратно, если  $i$  и  $j$  — символы из одной области транзитивности группы  $H$ , то некоторый элемент  $h_2 \in H$  отображает  $j$  в  $i$ , а элемент  $x_jh_2$  переводит 1 в  $i$ , откуда  $x_jh_2 \in Hx_i$ , т. е.  $x_i = h_1x_jh_2$  и  $Hx_iH = Hx_jH$ . Итак, любой двойной класс по  $H$  — это один из классов  $Hx_iH$ . Следовательно, в группе  $G$  существует точно столько двойных классов  $HxH$ , сколько областей транзитивности в группе  $H$ .

**Теорема 16.6.15.** *Каждое дважды транзитивное представление группы  $G$  подстановками над полем комплексных чисел есть сумма тождественного и некоторого абсолютно неприводимого представлений.*

*Доказательство.* Для дважды транзитивного представления имеем

$$\sum_{x \in G} \chi^2(x) = 2g,$$

так как подгруппа  $H$ , оставляющая на месте символ 1, обладает точно двумя областями транзитивности: 1 и остальные символы. Так как число  $\chi(x)$  действительное, то

$$\sum_{x \in G} \chi(x)\overline{\chi(x)} = 2g.$$

Если  $\chi = \sum_a c_a \chi^a$  — сумма абсолютно неприводимых характеров, то

$$\sum_{x \in G} \chi(x)\overline{\chi(x)} = \sum_x \left[ \sum_a c_a \chi^a(x) \right] \left[ \sum_a c_a \overline{\chi^a(x)} \right] = g \sum_a c_a^2$$

в силу соотношений ортогональности. Поэтому  $\sum_a c_a^2 = 2$ , откуда  $c_1 = 1$  (как уже известно) и еще только одно  $c_a = 1$ .

## 16.7. Импримитивные представления

Пусть модуль представления  $M$  группы  $G$  распадается в прямую сумму подпространств  $M_1, M_2, \dots, M_n$ , на которых это представление *транзитивно*, но *импримитивно*. Это означает следующее:

1) для любых подпространств  $M_i$  и  $M_j$  существует такой элемент  $x \in G$ , что  $M_i x = M_j$ ;

2) для каждого подпространства  $M_i$  и каждого элемента  $x \in G$  существует такое подпространство  $M_j$ , что  $M_i x = M_j$ . Первое требование — это свойство транзитивности, а второе — свойство импримитивности.

Зафиксируем подпространство  $M_1$ . Множество всех таких  $x$ , что  $M_1 x = M_1$ , непусто, так как, конечно, содержит элемент  $x = 1$ , и, как легко видеть, оно образует подгруппу  $H$  группы  $G$ . Тогда для любого элемента  $h \in H$

$$M_1 h = M_1,$$

поэтому  $M_1$  — модуль представления группы  $H$ . Если  $b_i \in G$  — такой элемент, что

$$M_1 b_i = M_i,$$

то элементы  $x$ , такие, что  $M_1 x = M_i$ , образуют смежный класс  $Hb_i$ . Таким образом, мы имеем

$$G = H + Hb_2 + Hb_3 + \dots + Hb_n,$$

где

$$M_1(hb_i) = M_i, \quad i = 1, \dots, n.$$

Этим мы установили связь между подпространствами  $M_i$  и смежными классами по подгруппе  $H$ . Если элемент  $x$  такой, что

$$M_i x = M_i,$$

то

$$M_1 b_i x = M_1 b_i,$$

т. е.

$$M_1 b_i x b_i^{-1} = M_1,$$

откуда  $b_i x b_i^{-1} \in H$ , или  $x$  — элемент подгруппы  $b_i^{-1} H b_i$ . Наконец, если

$$M_i x = M_j,$$

то

$$x \in b_i^{-1} H b_j.$$

Пусть  $\rho_1$  — представление группы  $H$  относительно базиса  $v_1, \dots, v_m$  подпространства  $M_1$ . Тогда элементы  $v_1 b_i, \dots, v_m b_i$

образуют базис подпространства  $M_i$ . В таком случае для произвольного элемента  $x \in G$  имеем

$$M_1x = M_{j_1}, \dots, M_i x = M_{j_i}, \dots, M_n x = M_{j_n}.$$

Здесь  $M_{j_1}, \dots, M_{j_n}$  — перестановка подмодулей  $M_1, \dots, M_n$ , так как, подействовав на них элементом  $x^{-1}$ , мы должны получить опять  $M_1, \dots, M_n$ . Если  $M_i x = M_j$  ( $j = j_i$ ), то  $x \in b_i^{-1}Hb_j$  или  $b_i x b_j^{-1} = h_{ij} \in H$ . Следовательно, в базисе  $v_k b_i$ ,  $k = 1, \dots, m$ , подпространства  $M_i$

$$v_k b_i \cdot x = (v_k \cdot h_{ij}) b_j, \quad k = 1, \dots, m.$$

Другими словами, эта часть представления полностью определена представлением элементов  $h_{ij}$  в подмодуле  $M_1$ :

$$v_k(b_i x b_j^{-1}) = v_k h_{ij}.$$

Отсюда

$$\rho(x) = (\rho_1(b_i x b_j^{-1})), \quad i, j = 1, \dots, n,$$

при условии, что  $\rho_1(y) = 0$  при  $y \notin H$ . Здесь матрица  $\rho(x)$  состоит из  $n^2$  матриц порядка  $m$  и имеет порядок  $mn$ . Таким образом, любое представление, транзитивное и импримитивное на подпространствах  $M_1, \dots, M_n$ , определяется представлением  $\rho_1$  подгруппы  $H$  индекса  $n$  в группе  $G$ . Обратное также верно. Пусть  $\rho_1$  — произвольное представление подгруппы  $H$ , где

$$G = H + Hb_2 + \dots + Hb_n.$$

Тогда определяем представление

$$\rho(x) = (\rho_1(b_i x b_j^{-1})), \quad i, j = 1, \dots, n,$$

причем  $\rho_1(y) = 0$ , если  $y \notin H$ . Применяя побочное умножение матриц, получаем

$$\begin{aligned} \rho(x)\rho(y) &= (\rho_1(b_i x b_j^{-1}))(\rho_1(b_k y b_t^{-1})) = \\ &= (\rho_1(b_i x b_j^{-1}))(\rho_1(b_j y b_t^{-1})) = \\ &= (\rho_1(b_i x y b_t^{-1})) = \rho(xy), \end{aligned}$$

а также, очевидно,

$$\rho(1) = (\rho_1(b_1 b_i^{-1})) = (\rho_1(1)) = I.$$

Таким образом,  $\rho(x)$  — представление группы  $G$ .

**ТЕОРЕМА 16.7.1.** *Если  $\rho_1$  — представление степени  $m$  подгруппы  $H$  группы  $G$  и  $G = H + Hb_2 + \dots + Hb_n$ , то*

$$\rho(x) = (\rho_1(b_i x b_j^{-1})), \quad i, j = 1, \dots, n,$$

при условии, что  $\rho_1(y) = 0$  для  $y \notin H$ , является представлением степени  $m$  группы  $G$  на модуле  $M$ , который содержит подмодули  $M_1, M_2, \dots, M_n$ , отвечающие соответственно смежным классам  $H, Hb_2, \dots, Hb_n$ ;  $\rho$  — транзитивное и импримитивное представление на  $M_1, \dots, M_n$ . Обратно, всякое представление, транзитивное и импримитивное на подмодулях некоторого модуля, является представлением такого типа.

**Доказательство.** Если  $u_1, \dots, u_m, \dots, u_{mn}$  — базис модуля представления  $\rho$ , то  $u_1, \dots, u_m$  — базис представления  $\rho_1$  группы  $H$  и  $u_{m(i-1)+j} = u_j b_i$ ,  $i = 1, \dots, n$ . Отсюда следует, что модуль  $M$  с базисом  $u_1, \dots, u_{mn}$  обладает подмодулями  $M_1, \dots, M_n$ , на которых представление  $\rho$  транзитивно и импримитивно. Будем говорить, что представление  $\rho$  группы  $G$  индуцировано представлением  $\rho_1$  группы  $H$ .

**Следствие 16.7.1.** Представление  $\rho$  группы  $G$ , индуцированное представлением  $\rho_1$  подгруппы  $H$ , не зависит от выбора представителей смежных классов группы  $G$  по подгруппе  $H$ .

Это следует из того, что замена этих представителей не изменяет подпространств  $M_1, \dots, M_n$ , а только изменяет их базисы.

**Теорема 16.7.2.** Пусть  $\chi$  — характер представления  $\rho$  группы  $G$ , индуцированного представлением  $\rho_1$  подгруппы  $H$ , характер которого равен  $\chi_1$ . Пусть  $x$  — элемент класса  $C_j$  со-пряженных элементов группы  $G$ , состоящего из  $h_j$  элементов. Пусть, наконец,  $g = g_i h_i$ , где  $g$  — порядок группы  $G$ , и  $h$  — порядок группы  $H$ . Тогда

$$\chi(x) = \frac{g_j}{h} \sum_{z \in C_j \cap H} \chi_1(z).$$

**Доказательство.**  $\chi(x) = \sum_{i=1}^{h_j} \chi_1(b_i x b_i^{-1})$ , причем  $\chi_1(w) = 0$ , если  $w \notin H$ . Тогда

$$\chi(x) = \frac{1}{h} \sum_{y \in G} \chi_1(y x y^{-1}),$$

так как для всех элементов  $y$  из класса  $Hb_i$  значения  $\chi_1(y x y^{-1})$  равны  $\chi_1(b_i x b_i^{-1})$ . Когда  $y$  пробегает группу  $G$ , элемент  $y x y^{-1}$  пробегает класс  $C_j$  и принимает значение  $z \in C_j$  точно  $g_j$  раз. Таким образом,

$$\sum_{y \in G} \chi_1(y x y^{-1}) = g_j \sum_{z \in C_j \cap H} \chi_1(z),$$

что и требовалось доказать.

**Теорема 16.7.3.** (Теорема взаимности.) Пусть  $\rho$  и  $\rho_1$  — соответственно абсолютно неприводимые представления группы  $G$

и подгруппы  $H$  над полем характеристики нуль. Тогда представление  $\rho_1$  столько раз содержится в представлении подгруппы  $H$ , индуцированном представлением<sup>1)</sup>  $\rho$ , сколько раз представление  $\rho$  содержится в представлении  $\rho^*$  группы  $G$ , индуцированном представлением  $\rho_1$ .

*Доказательство.* Пусть  $\chi = \chi^d$  — характер представления  $\rho$  и  $\chi_1 = \chi_1^c$  — характер представления  $\rho_1$ ;  $\chi^*$  — характер  $\rho^*$ ,  $\chi^* = \sum_b m_b \chi^b$ , где  $\chi^b$  — неприводимые характеры группы  $G$ . Пусть для характера представления подгруппы  $H$ , индуцированного представлением  $\rho$ ,  $\chi = \chi^a = \sum_d n_d \chi_1^d$ , где  $\chi_1^d$  — неприводимый характер группы  $H$ . Здесь представление  $\rho$  содержит в представлении  $\rho^*$   $m_a$  раз, а кратность, с которой  $\rho_1$  входит в ограничение  $\rho$  на  $H$ , равна  $n_c$ . В силу предыдущей теоремы

$$\frac{1}{g_j} \chi_j^* = \frac{1}{g_j} \sum_b m_b \chi_j^b = \frac{1}{h} \sum_{z \in C_j \cap H} \chi_1^c(z).$$

Здесь мы придерживаемся соглашения, что сумма по пустому множеству индексов равна нулю. Умножим это равенство на  $\bar{\chi}_j^a$  и просуммируем по  $j$ . Тогда получим

$$\sum_{j, b} m_b \frac{\bar{\chi}_j^a \chi_j^b}{g_j} = \frac{1}{h} \sum_j \bar{\chi}_j^a \sum_{z \in C_j \cap H} \chi_1^c(z),$$

откуда, используя соотношения ортогональности в группе  $G$  и в подгруппе  $H$ , получаем

$$\begin{aligned} m_a &= \frac{1}{h} \sum_{d, j} n_d \bar{\chi}_1^d \sum_{z \in C_j \cap H} \chi_1^c(z) = \frac{1}{h} \sum_{d, z \in H} n_d \bar{\chi}_1^d(z) \chi_1^c(z) = \\ &= \frac{1}{h} h n_c = n_c, \end{aligned}$$

и теорема доказана.

### 16.8. Некоторые применения теории характеров

В этом параграфе мы будем иметь дело только с полем  $F$  комплексных чисел, хотя читателю будет ясно, что ряд установленных результатов сохраняется и для произвольного поля, характеристика которого не делит порядок рассматриваемой группы  $G$ .

<sup>1)</sup> Представлением подгруппы, индуцированным представлением группы, называется представление группы, если его рассматривать только на этой подгруппе. — *Прим. перев.*

Нам понадобятся некоторые факты из теории алгебраических чисел<sup>1)</sup>. Число  $\theta$  называется *алгебраическим*, если оно является корнем уравнения

$$x^n + a_1x^{n-1} + \dots + a_n = 0,$$

где  $a_1, \dots, a_n$  — рациональные числа. Число  $\theta$  называется *целым алгебраическим*, если оно является корнем полинома, коэффициенты которого  $a_1, \dots, a_n$  — целые рациональные числа.

**Теорема 16.8.1.** *Если рациональное число — целое алгебраическое, то оно — целое рациональное.*

**Доказательство.** Пусть  $\theta = r/s$  — несократимое рациональное число, удовлетворяющее уравнению

$$x^n + a_1x^{n-1} + \dots + a_n = 0,$$

где  $a_1, \dots, a_n$  — целые числа. Тогда

$$r^n = -s(a_1r^{n-1} + a_2sr^{n-2} + \dots + a_ns^{n-1}).$$

Поэтому любое простое число, которое делит  $s$ , должно делить также  $r^n$ , а значит, и  $r$ . Этого не может случиться, если  $r/s$  — несократимая дробь и  $s \neq 1$ . Следовательно,  $s = 1$ , т. е.  $\theta = r$  — целое рациональное число.

**Теорема 16.8.2.** *Алгебраические числа образуют поле. Сумма и произведение двух целых алгебраических чисел есть целое алгебраическое число.*

**Доказательство.** Пусть  $\theta, \varphi$  — алгебраические числа, удовлетворяющие уравнениям  $x^n + a_1x^{n-1} + \dots + a_n = 0$  и  $x^m + b_1x^{m-1} + \dots + b_m = 0$  соответственно. Пусть

$$v_{ij} = \theta^i \varphi^j, \quad i = 0, 1, \dots, n-1; \quad j = 0, \dots, m-1.$$

Тогда

$$\theta v_{ij} = v_{i+1, j} \quad \text{для } i = 0, \dots, n-2$$

и

$$\theta v_{n-1, j} = -a_1 v_{n-1, j} - \dots - a_n v_{0, j}.$$

Аналогично

$$\varphi v_{ij} = v_{i, j+1} \quad \text{для } j = 0, \dots, m-2$$

и

$$\varphi v_{i, m-1} = -b_1 v_{i, m-1} - \dots - b_m v_{i, 0}.$$

<sup>1)</sup> Эти факты содержатся у Биркгофа и Маклейна [1], стр. 410—422 (см. также Гекке Э., Лекции по теории алгебраических чисел, ГИТТЛ, 1940. — Прим. перев.).

**Лемма 16.8.1.** Если  $y_1, \dots, y_N$  — числа, не все равные нулю, и  $z$  — такое число, что

$$zy_i = \sum_j a_{ij}y_j, \quad i = 1, \dots, N,$$

где  $a_{ij}$  — рациональные числа, то  $z$  — алгебраическое число. Если числа  $a_{ij}$  целые, то  $z$  — целое алгебраическое число.

**Доказательство.** Условия теоремы представляют собой систему линейных уравнений

$$\begin{cases} (a_{11} - z)y_1 + a_{12}y_2 + \dots + a_{1N}y_N = 0, \\ a_{21}y_1 + (a_{22} - z)y_2 + \dots + a_{2N}y_N = 0, \\ \dots \dots \dots \dots \dots \dots \\ a_{N1}y_1 + a_{N2}y_2 + \dots + (a_{NN} - z)y_N = 0 \end{cases}$$

относительно  $y_1, \dots, y_N$ , имеющую вполне определенное ненулевое решение  $y_1, \dots, y_N$ . Следовательно, определитель этой системы равен нулю:

$$\begin{vmatrix} a_{11} - z & a_{12} & \dots & a_{1N} \\ a_{21} & a_{22} - z & \dots & a_{2N} \\ \dots & \dots & \dots & \dots \\ a_{N1} & a_{N2} & \dots & a_{NN} - z \end{vmatrix} = 0,$$

т. е.

$$(-1)^N z^N + p_1 z^{N-1} + \dots + p_N = 0,$$

где  $p_i$  — целочисленные полиномы от  $a_i$ . Поэтому, при рациональных значениях  $a_{ij}$ ,  $z$  — алгебраическое число, а при целых  $a_{ij}$   $z$  — целое алгебраическое число.

Используем эту лемму для доказательства теоремы. Тривиальные случаи, когда  $\theta$  или  $\varphi$  — нуль, мы исключаем. В качестве чисел  $y_1, \dots, y_N$  возьмем числа  $v_{ij}$ , которые не все равны нулю, так как  $v_{00} = 1$ . В качестве  $z$  возьмем  $\theta + \varphi$  или  $\theta\varphi$ . Коэффициенты  $a_{ij}$  по лемме являются целочисленными полиномами от  $a_1, \dots, a_n$  и  $b_1, \dots, b_m$ . Поэтому  $z = \theta + \varphi$  и  $z = \theta\varphi$  — алгебраические числа, а если  $a_1, \dots, a_n$  и  $b_1, \dots, b_m$  — целые, то  $\theta + \varphi$  и  $\theta\varphi$  — целые алгебраические числа. Таким образом, сумма и произведение алгебраических чисел являются алгебраическими числами, сумма и произведение целых алгебраических чисел — снова целые алгебраические числа. Наконец, если  $\theta \neq 0$  — алгебраическое число, удовлетворяющее уравнению  $z^n + a_1 z^{n-1} + \dots + a_n = 0$ , то мы можем считать, что  $a_n \neq 0$ , так как в противном случае мы могли бы этого добиться, разделив многочлен на подходящую степень  $z$ . Тогда

$$z^n + \frac{a_{n-1}}{a_n} z^{n-1} + \dots + \frac{1}{a_n} = 0$$

— уравнение, корнем которого является число  $\frac{1}{\theta}$ . Кроме этого, очевидно, что число  $-\theta$  удовлетворяет уравнению  $z^n - a_1 z^{n-1} + \dots + (-1)^n a_n = 0$ . Итак, алгебраические числа образуют поле, а целые алгебраические — область целостности<sup>1)</sup>.

**Теорема 16.8.3.** Любой характер  $\chi(x)$  является целым алгебраическим числом. Числа  $h_i \chi_i^a / n_a$  из теоремы 16.6.10 — также целые алгебраические.

**Доказательство.** Корень  $m$ -й степени из единицы удовлетворяет уравнению  $x^m - 1 = 0$  и поэтому является целым алгебраическим числом. По теореме 16.6.8 любой характер  $\chi(x)$  есть сумма корней из единицы. Поэтому  $\chi(x)$  — целое алгебраическое число. Так как коэффициенты  $c_{ijk}$  в теореме 16.6.10 — целые числа, мы можем применить лемму 16.8.1, взяв числа

$$\frac{h_i \chi_i^a}{n_a} = \eta_i^a, \quad i = 1, \dots, r,$$

в качестве  $y_1, \dots, y_N$  и любое из них — в качестве  $z$ . Отсюда заключаем, что  $\eta_i^a$  — целые алгебраические числа.

**Теорема 16.8.4.** Степени  $n_a$  абсолютно неприводимых представлений конечной группы являются делителями порядка  $g$  группы  $G$ .

**Доказательство.** Одно из соотношений ортогональности дает

$$\sum_{i=1}^r \frac{\chi_i^a \bar{\chi}_i^a}{g_i} = 1.$$

Положив  $g_i h_i = g$ , получаем

$$\sum_{i=1}^r \frac{\chi_i^a h_i \bar{\chi}_i^a}{g} = 1,$$

или

$$\sum_{i=1}^r \frac{h_i \chi_i^a}{n_a} \bar{\chi}_i^a = \frac{g}{n_a}.$$

Слева записана сумма произведений целых алгебраических чисел. Следовательно,  $g/n_a$  — также целое алгебраическое число, а так как это рациональное число, то оно должно быть целым рациональным числом. Таким образом,  $n_a$  делит  $g$ .

Для дальнейшего применения теории алгебраических чисел нам необходимы некоторые сведения о симметрических функциях.

1) То есть коммутативное кольцо без делителей нуля. — Прим. ред.

Раскрыв скобки в произведении

$$(z - x_1) \dots (z - x_n) = z^n - E_1 z^{n-1} + \dots + (-1)^n E_n,$$

получаем

$$\begin{aligned} E_1 &= \sum x_i, \\ E_2 &= \sum x_i x_j, \\ &\dots \\ E_r &= \sum x_{i_1} x_{i_2} \dots x_{i_r}, \\ &\dots \\ E_n &= x_1 x_2 \dots x_n. \end{aligned}$$

Ясно, что  $E_1, \dots, E_n$  остаются неизменными при любых перестановках букв  $x_1, \dots, x_n$ .  $E_i$  называются *элементарными симметрическими функциями* от переменных  $x_1, \dots, x_n$ . Полином  $P(x_1, \dots, x_n)$  над полем  $F$  называется *симметрической функцией*, если он не изменяется при всех подстановках из симметрической группы подстановок элементов  $x_1, \dots, x_n$ .

**Теорема 16.8.5.** Любая симметрическая функция  $P(x_1, \dots, x_n)$  может быть записана в виде полинома  $Q(E_1, \dots, E_n)$  от элементарных симметрических функций  $E_1, \dots, E_n$ , коэффициентами которого являются целочисленные полиномы от коэффициентов полинома  $P$ .

**Доказательство.** Если  $P$  — симметрический полином, то для каждого  $l = 0, 1, \dots$  сумма членов  $l$ -й степени — также симметрическая функция. Теорема очевидна для полинома  $P$  степени 1, так как все симметрические функции в этом случае имеют вид  $cE_1$ ,  $c \in F$ . Кроме того,  $P$  есть сумма симметрических полиномов, каждый из которых определяется одним из своих членов вида  $c(x_1 \dots x_r)^a (x_{r+1} \dots x_{r+s})^b \dots (x_{u+1} \dots x_{u+v})^t$ , где показатели степени подчинены неравенствам  $a > b > \dots > t$ . Поэтому теорему достаточно доказать для симметрических форм вида

$$K = \sum (x_1 \dots x_r)^a (x_{r+1} \dots x_{r+s})^b \dots (x_{u+1} \dots x_{u+v})^t,$$

где  $a > b > \dots > t$ . Будем применять индукцию, во-первых, по степени полинома  $K$ , во-вторых, по  $a$  и, в-третьих, по числу  $r$ . Если аргументы  $x_1, x_2, \dots, x_n$  встречаются в каждом члене, мы выносим симметрическую функцию  $E_n$  за скобки. В скобках остается симметрический полином более низкой степени. Поэтому мы можем считать, что  $u+v < n$ . Если  $a=1$ , то  $K=E_r$ . В противном случае рассмотрим произведение

$$\begin{aligned} \sum x_1 \dots x_r \cdot \sum (x_1 \dots x_r)^{a-1} (x_{r+1} \dots x_{r+s})^b \dots \\ \dots (x_{u+1} \dots x_{u+v})^t = E_r \cdot K^*, \end{aligned}$$

где  $E_r \cdot K^* = K +$  дополнительные члены. Но как  $K^*$ , так и сумма дополнительных членов — симметрические полиномы. Этим теорема доказана.

Полином наименьшей степени с рациональными коэффициентами, корнем которого является алгебраическое число  $\theta$ , называется *минимальным полиномом* для числа  $\theta$ . Минимальный полином

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n$$

делит любой полином  $h(x)$  с рациональными коэффициентами, корнем которого является число  $\theta$ . Если теперь

$$f(x) = (x - \theta_1)(x - \theta_2) \dots (x - \theta_n),$$

где  $\theta = \theta_1$ , то числа  $\theta_2, \dots, \theta_n$  называются *сопряженными* с  $\theta$ : Числа, сопряженные с  $\theta$ , также обращают в нуль любой многочлен, корнем которого является число  $\theta$ . Следовательно, если  $\theta$  — целое алгебраическое число, то они также являются целыми алгебраическими; поэтому коэффициенты минимального полинома для целого алгебраического  $\theta$ , являясь элементарными симметрическими функциями от  $\theta_1, \dots, \theta_n$ , — также целые алгебраические, а значит, и целые рациональные числа.

При изучении представлений мы обычно имеем дело с корнями из единицы. Примитивными корнями степени  $m$  из единицы являются числа  $\omega = \exp(2\pi i/m)$  и  $\omega^j$  при  $(j, m) = 1$ . Они удовлетворяют уравнению  $x^m - 1 = 0$ , но не удовлетворяют никакому уравнению  $x^r - 1 = 0$  при  $0 < r < m$ . Остальные корни степени  $m$  из единицы являются корнями уравнения  $x^d - 1 = 0$ , где  $d$  пробегает все делители числа  $m$ . Разделив многочлен  $x^m - 1$  на его сомножители, общие со всеми многочленами  $x^d - 1$ ,  $d < m$ , мы получаем полином  $f(x)$  с рациональными коэффициентами, корнями которого являются примитивные корни степени  $m$  из единицы, и только они. Следовательно,

$$f(x) = \prod_j (x - \omega^j), \quad (j, m) = 1,$$

и  $f(x)$  — многочлен с целыми рациональными коэффициентами степени  $\varphi(m)$ , где  $\varphi$  — функция Эйлера. Многочлен  $f(x)$  неприводим, но это доказывается с помощью более глубоких результатов об алгебраических числах, которые нам не понадобятся. Здесь нам нужен только тот факт, что симметрические функции примитивных корней степени  $m$  являются целыми рациональными числами.

**Теорема 16.8.6.** Пусть  $\rho_a$  — абсолютно неприводимое представление степени  $n$  группы  $G$ , обладающей таким классом сопряженных элементов  $C_i$ , что  $(h_i, n) = 1$ . Тогда или (1)

$\chi^a = 0$ , или (2)  $\chi_i^a = n\omega$ , где  $\omega$  — корень из единицы, причем образ  $C_i$  содержится в центре  $\rho_a$ .

*Доказательство.* Для данного элемента  $x \in C_i$  мы можем преобразовать представление  $\rho_a$  так, что матрица  $\rho_a(x)$  примет диагональный вид. Если все  $n$  характеристических корней матрицы  $\rho_a(x)$  равны, скажем, некоторому корню  $\omega$  степени  $m$  из единицы, то

$$\rho_a(x) = \omega I_n, \quad \chi(x) = n\omega,$$

и  $x$  — элемент центра  $\rho_a$ . Это случай (2) в формулировке теоремы. Теперь мы должны доказать, что при выполнении условий теоремы в случае, когда не все характеристические корни элемента  $x$  равны между собой,  $\chi(x) = 0$ . В этом случае  $x$  имеет порядок  $m$ ,  $\chi_i^a = \chi(x) = \omega^{e_1} + \dots + \omega^{e_n}$  и  $|\chi_i^a| < n$ , так как числа  $\omega^{e_i}$  не все имеют одинаковые аргументы. Здесь

$$\frac{h_i \chi_i^a}{n}$$

— целое алгебраическое число; так как  $(h_i, n) = 1$ , существуют такие целые числа  $r$  и  $s$ , что  $rh_i + sn = 1$ . Следовательно,

$$r \left( \frac{h_i \chi_i^a}{n} \right) + s \cdot \chi_i^a = \frac{\chi_i^a}{n}$$

— целое алгебраическое число. При этом

$$\left| \frac{\chi_i^a}{n} \right| < 1$$

и

$$\xi = \frac{\chi_i^a}{n} = \frac{\omega^{e_1} + \dots + \omega^{e_n}}{n}.$$

Заменяя  $\omega$  сопряженными числами  $\omega^j$ , получаем полином

$$\prod_{(j, m)=1} [z - q(\omega^j)],$$

коэффициенты которого — симметрические функции от сопряженных корней и, следовательно, рациональные числа. Так, сопряженные с  $\xi$  числа находятся среди чисел вида

$$\frac{\omega^{je_1} + \dots + \omega^{je_n}}{n},$$

и поэтому для любого числа  $\xi^{(i)}$ , сопряженного с  $\xi$ ,  $|\xi^{(i)}| \leq 1$ , и любое такое сопряженное число является целым алгебраическим.  $|\xi| = |\xi^{(1)}| < 1$ , и поэтому  $|\xi^{(1)} \dots \xi^{(s)}| < 1$ , где  $\xi^{(1)}, \dots, \xi^{(s)}$  — все

числа, сопряженные с  $\xi$ . Это произведение должно быть целым рациональным числом, значит оно равно нулю. Таким образом,  $\xi^{(1)} \dots \xi^{(s)} = 0$ . Следовательно, по меньшей мере один из сомножителей равен нулю. Но с нулем сопряжен только нуль. Поэтому  $\xi = \xi^{(1)} = 0$ , т. е.

$$\xi = \frac{\chi_i^a}{n} = 0,$$

откуда  $\chi_i^a = 0$ , что и требовалось доказать.

**Теорема 16.8.7<sup>1)</sup>.** (1) *Если число  $h_i$  элементов в классе  $C_i$  группы  $G$  равно степени простого числа, то  $G$  — не простая группа. Точнее, существует гомоморфный образ группы  $G$ , в котором образы элементов класса  $C_i$  содержатся в центре.* (2) *Группы порядка  $p^aq^b$ , где  $p$  и  $q$  — простые числа, разрешимы.*

**Доказательство.** (1) Пусть  $n_1 = 1, n_2, \dots, n_r$  — степени абсолютно неприводимых представлений группы  $G$ . Пусть  $h_i = p^s$  — число элементов в классе  $C_i$ . Для регулярного представления группы  $G$   $\chi(x) = 0$  для  $x \in C_i$ , так как  $x \neq 1$ . Пусть

$$\chi(x) = \sum_{a=1}^r n_a \chi_i^a.$$

— разложение регулярного представления. Здесь  $n_1 \chi_i^1 = 1$ . Что касается остальных слагаемых при условии  $p \nmid n_a$ , то по теореме 16.8.6 или  $\chi_i^a = 0$ , или образ класса  $C_i$  содержится в центре гомоморфного образа  $\rho_a(G)$ . Но если бы  $\chi_i^a = 0$ , когда  $p \nmid n_a$ , мы бы имели

$$0 = 1 + \sum_{a=2}^r n_a \chi_i^a = 1 + p\alpha,$$

где  $\alpha$  — целое алгебраическое число. Это значило бы, что  $-(1/p)$  — целое алгебраическое число, что невозможно. Следовательно, для некоторого  $\rho_a$  образ класса  $C_i$  содержится в центре образа  $\rho_a(G)$ .

(2) Пусть  $G$  — группа порядка  $p^aq^b$ . Для доказательства применим индукцию по порядку групп.  $p$ -группы, как известно, разрешимы. Элемент из центра силовой  $q$ -подгруппы или содержится в центре группы  $G$ , или же число его сопряженных элементов равно степени числа  $p$ . В обоих случаях группа  $G$  обладает собственной инвариантной подгруппой  $H$ . Тогда, по предположению индукции, группы  $H$  и  $G/H$  разрешимы, откуда, в силу предположения индукции, следует разрешимость группы  $G$ .

<sup>1)</sup> В. Бернсайд [2], стр. 322—323.

**Теорема 16.8.8.** (Теорема Фробениуса.) *Если  $G$  — транзитивная группа подстановок степени  $n$ , каждая подстановка которой, отличная от единицы, оставляет на месте не более одного символа, то те подстановки из группы  $G$ , которые переставляют все символы, образуют вместе с единичной подстановкой инвариантную подгруппу порядка  $n$ .*

**Доказательство.** Пусть  $G$  — указанная в условии теоремы группа подстановок символов  $1, 2, \dots, n$ , и пусть  $H_i$  — подгруппа, оставляющая на месте символ  $i$ . Тогда по условию  $H_i \cap H_j = 1$  при  $i \neq j$ . Если порядок подгруппы  $H = H_1$  равен  $h$ , то порядки всех подгрупп  $H_i$  равны  $h$ , а общее число элементов  $x \neq 1$  во всех подгруппах  $H_i$  равно  $(h - 1)n$ .  $[G : H] = n$ , так что порядок группы  $G$  равен  $nh$ . Остается еще точно  $n$  подстановок, а именно единичная и  $n - 1$  подстановок, переставляющих все символы.

Пусть  $\psi$  — абсолютно неприводимый характер группы  $H$ , а  $\psi'$  — индуцированный характер группы  $G$ . Группу  $G$  можно рассматривать как представление самой себя, и в этом смысле она имеет характер  $\theta_1 = \psi'_1$ , где  $\psi_1$  — единичный характер подгруппы  $H$ . По теореме 16.6.13,  $\theta_1$  есть сумма единичного характера группы  $G$  и некоторого другого характера, скажем,  $\theta$ . Обозначим через  $r_G$  характер регулярного представления группы  $G$ . Положим  $\omega = r_G - h\theta$ . Наша теорема будет доказана, если мы докажем, что  $\omega$  — характер группы  $G$ . Действительно, в следующей таблице для характеров пусть  $x \neq 1$  — произвольный элемент любой из подгрупп  $H_i$  а  $y$  — произвольная подстановка, переставляющая все буквы:

	1	$x$	$y$
$\psi'$	$mn$ ,	$\psi(x)$ ,	0
$\theta$	$n - 1$ ,	0,	-1
$r_G$	$nh$ ,	0,	0
$\omega$	$h$ ,	0,	$h$

Здесь, как уже известно,  $\psi'$ ,  $\theta$ ,  $r_G$  — характеристы. Если  $\omega$  — характериста, то, так как  $\omega(1) = h$ ,  $\omega$  — характериста представления степени  $h$ . Так как  $\omega(y) = h$ ,  $\omega(x) = 0$ , то любой элемент  $y$ , отличный от  $x$ , представляется единицей. Следовательно,  $\omega$  — представление группы  $G$  с ядром, состоящим только из единицы и всех элементов  $y$ , переставляющих все символы. Поэтому единица и все элементы  $y$  образуют инвариантную подгруппу группы  $G$ .

Докажем теперь, что  $\omega$  — характериста. Пусть  $s$  — число классов сопряженных элементов группы  $H$  и  $\psi^a$ ,  $a = 1, \dots, s$ , —

абсолютно неприводимые характеристы степеней  $m_a$ . Тогда

$$r_H = \sum_{a=1}^s m_a \psi_a.$$

Но  $r_G = (r_H)'$  и  $h = \sum_a m_a^2$ . Следовательно,

$$\omega = \sum_a m_a [(\psi^a) - m_a \theta].$$

Поэтому достаточно доказать, что  $\psi' - m\theta$  — характер группы  $G$  при любых значениях  $\psi = \psi^a$ ,  $m = m_a$ .

Вычислим скалярное произведение

$$(\psi' - m\theta, \psi' - m\theta) = (\psi', \psi') - 2m(\psi', \theta) + m^2(\theta, \theta).$$

Учитывая, что  $g = nh$ , из таблицы для характеристик получаем

$$(\psi', \psi') = \frac{m^2 n}{h} + \frac{1}{nh} \sum_x \psi(x) \overline{\psi(x)} = \frac{m^2 n}{h} + \frac{1}{h} \sum_{\substack{x \in H \\ x \neq 1}} \psi(x) \overline{\psi(x)}.$$

Но

$$\sum_{x \in H} \psi(x) \overline{\psi(x)} = h,$$

откуда

$$(\psi', \psi') = [m^2 n + (h - m^2)]/h.$$

Аналогично из той же таблицы находим, что  $(\psi', \theta) = m(n-1)/h$  и

$$(\theta, \theta) = [(n-1)^2 + (n-1)]/nh = (n-1)/h.$$

Отсюда

$$(\psi' - m\theta, \psi' - m\theta) = 1.$$

Но  $\psi' - m\theta$  есть, во всяком случае, линейная комбинация характеристик с целыми коэффициентами  $\psi' - m\theta = \sum c_a \chi^a$ , откуда

$$(\psi' - m\theta, \psi' - m\theta) = \sum c_a^2.$$

Следовательно,  $\sum c_a^2 = 1$ . Поэтому существует точно один коэффициент  $c_a = \pm 1$ , а все остальные равны нулю. Таким образом,  $\psi' - m\theta = \pm \psi^a$ . Но  $(\psi' - m\theta)(1) = m > 0$ , откуда  $\psi' - m\theta = \psi^a$  — характер группы  $G$ . Поэтому  $\omega$  — характер группы  $G$ , и теорема доказана.

## 16.9. Унитарные и ортогональные представления

Произвольной матрице  $A$  порядка  $n$

$$A = (a_{ij}), \quad i, j = 1, \dots, n, \tag{16.9.1}$$

соответствует билинейная форма  $B(y, x)$ :

$$B(y, x) = \sum_{i,j} a_{ij} y_i x_j, \quad i, j = 1, \dots, n, \tag{16.9.2}$$

причем это соответствие, конечно, обратимо. Нас интересует, каким образом изменяется матрица  $A$  при линейном преобразовании аргументов  $x_j$  и  $y_i$ . Пусть

$$\begin{aligned}x_j &= \sum_k c_{jk} x'_k, \quad j, k = 1, \dots, n, \\y_i &= \sum_s d_{is} y'_s, \quad i, s = 1, \dots, n.\end{aligned}\tag{16.9.3}$$

Тогда

$$B(y, x) = B'(y', x') = \sum_{i, j, k, s} d_{is} a_{ij} c_{jk} y'_s x'_k.\tag{16.9.4}$$

Отсюда видно, что билинейной форме  $B'(y', x')$  соответствует матрица

$$A' = D^T A C, \quad D = (d_{is}), \quad C = (c_{jk}).\tag{16.9.5}$$

Далее нас будут интересовать не самые общие билинейные формы, а только определенного частного вида. В этом параграфе будем брать коэффициенты из поля комплексных чисел. Если

$$a_{ij} = \bar{a}_{ij}, \quad i, j = 1, \dots, n,\tag{16.9.6}$$

где  $\bar{a}_{ij}$  — число, комплексно сопряженное с  $a_{ij}$ , то мы называем матрицу  $A$  *эрмитовой*. Ей соответствует билинейная *эрмитова форма*  $H(\bar{x}, x)$ :

$$H(\bar{x}, x) = \sum_{i, j} a_{ij} \bar{x}_i x_j, \quad a_{ji} = \bar{a}_{ij}, \quad i, j = 1, \dots, n.\tag{16.9.7}$$

Заметим, что в *эрмитовой* форме или *эрмитовой* матрице коэффициенты  $a_{ii} = \bar{a}_{ii}$  — действительные числа. Действительная *эрмитова* матрица является симметрической матрицей и соответствует действительной квадратичной форме  $Q(x)$ :

$$Q(x) = \sum_{i, j} a_{ij} x_i x_j, \quad a_{ji} = a_{ij}, \quad i, j = 1, \dots, n.\tag{16.9.8}$$

Невырожденные линейные преобразования, относительно которых *эрмитова* (или *квадратичная*) форма инвариантна, очевидно, образуют группу. Разумеется, при этом сопряженные значения  $x_i$  подвергаются преобразованию, сопряженному к преобразованию аргументов  $x_i$ .

**Определение.** Матрица  $U$ , для которой

$$\bar{U}^T I U = I,\tag{16.9.9}$$

называется *унитарной матрицей*.

**ОПРЕДЕЛЕНИЕ.** Матрица  $V$ , удовлетворяющая условию

$$V^T IV = I, \quad (16.9.10)$$

называется ортогональной.

Очевидно, что унитарные и ортогональные матрицы невырождены и что они образуют группы. Унитарные матрицы образуют группу линейных преобразований, оставляющих инвариантной форму  $\bar{x}_1x_1 + \dots + \bar{x}_n x_n$ , а ортогональные матрицы образуют группу линейных преобразований, оставляющих инвариантной форму  $x_1^2 + \dots + x_n^2$ . Действительные унитарные матрицы ортогональны, однако существуют также ортогональные матрицы, не являющиеся действительными; например

$$V = \begin{pmatrix} i & \sqrt{2} \\ -\sqrt{2} & i \end{pmatrix}. \quad (16.9.11)$$

Но здесь, говоря об ортогональных матрицах, мы будем иметь в виду действительные матрицы.

Представление  $\rho(g)$  группы  $G$  называется *унитарным*, если все матрицы  $\rho(g)$ ,  $g \in G$ , унитарны, или *ортогональным*, если все матрицы  $\rho(g)$ ,  $g \in G$ , ортогональны.

**Теорема 16.9.1.** Любое представление конечной группы над полем комплексных (действительных) чисел эквивалентно унитарному (ортогональному) представлению.

*Доказательство.* Если в эрмитовой форме

$$H(\bar{x}, x) = \sum a_{ij} \bar{x}_i x_j, \quad a_{ji} = \bar{a}_{ij}, \quad (16.9.12)$$

переменные  $x_i$  принимают комплексные значения, то  $H$  принимает действительные значения, так как все слагаемые можно сгруппировать парами

$$a_{ji} \bar{x}_j x_i + a_{ij} \bar{x}_i x_j = \bar{a}_{ij} \bar{x}_j x_i + a_{ji} \bar{x}_i x_j, \quad (16.9.13)$$

являющимися суммами комплексного числа и комплексно сопряженного к нему. Диагональные члены  $a_{ii} \bar{x}_i x_i$  действительны. Будем говорить, что  $H(\bar{x}, x)$  — *положительно определенная* форма, если ее значения всегда положительны, кроме случая равенства всех аргументов нулю, когда значение формы равно нулю. Очевидно, что свойство быть положительно определенной формой сохраняется при невырожденном преобразовании переменных. Примером положительно определенной формы от  $n$  переменных является форма

$$I(\bar{x}, x) = \bar{x}_1 x_1 + \dots + \bar{x}_n x_n, \quad (16.9.14)$$

которой соответствует единичная матрица.  $I(\bar{x}, x)$  — положительно определенная форма, так как каждое слагаемое  $x_j x_j$  положительно, если только  $x_j \neq 0$ ,  $j = 1, \dots, n$ .

**ЛЕММА 16.9.1.** Положительно определенная эрмитова форма  $H(\bar{x}, x)$  от  $n$  переменных может быть приведена к виду  $\bar{x}_1x_1 + \dots + \bar{x}_nx_n$ .

Заметим, что для положительно определенной формы

$$H(\bar{x}, x) = \sum_{i,j} a_{ij} \bar{x}_i x_j, \quad a_{ji} = \bar{a}_{ij},$$

диагональные коэффициенты  $a_{rr}$  положительны. Действительно, в противном случае при  $a_{rr} \leq 0$ , полагая  $x_r = 1$ ,  $x_j = 0$ ,  $j \neq r$ , мы бы имели  $H(\bar{x}, x) = a_{rr} \leq 0$ , что противоречит свойству положительной определенности. Теперь в форме

$$H = \sum_{i,j} a_{ij} \bar{x}_i x_j, \quad a_{ji} = \bar{a}_{ij}, \quad i, j = 1, \dots, n, \quad (16.9.15)$$

преобразуем переменные следующим образом:

$$\begin{aligned} x'_1 &= \sqrt{a_{11}} \left( x_1 + \frac{a_{12}x_2}{a_{11}} + \dots + \frac{a_{1n}x_n}{a_{11}} \right), \\ x'_j &= x_j, \quad j = 2, \dots, n. \end{aligned} \quad (16.9.16)$$

Такое преобразование допустимо, так как  $a_{11}$  — действительное положительное число. Тогда легко подсчитать, что

$$H = \bar{x}'_1 x'_1 + \sum b_{ij} \bar{x}'_i x'_j, \quad i, j = 2, \dots, n, \quad (16.9.17)$$

где сумма — положительно определенная форма от переменных  $x'_2, \dots, x'_n$ , к которой снова можно применить аналогичное преобразование переменных. Продолжая этот процесс, мы в конце концов приведем форму  $H$  к виду

$$H = \bar{x}_1 x_1 + \dots + \bar{x}_n x_n. \quad (16.9.18)$$

Этим лемма доказана. Заметим, что если бы мы исходили из действительной квадратичной формы  $Q$ , то путем таких же замен переменных мы привели бы форму  $Q$  к виду

$$x_1^2 + \dots + x_n^2.$$

Пусть теперь  $\rho(g)$ ,  $g \in G$ , — комплексное представление степени  $n$  конечной группы  $G$ , и пусть  $g_1 = 1$ ,  $g_2, \dots, g_t$  — элементы группы  $G$ . Тогда

$$M = I + \overline{\rho(g_2)}^T I \rho(g_2) + \dots + \overline{\rho(g_t)}^T I \rho(g_t) \quad (16.9.19)$$

— матрица, соответствующая положительно определенной эрмитовой форме, так как каждое слагаемое в отдельности соответствует

положительно определенной форме. Поэтому для любого элемента  $g \in G$

$$\begin{aligned} \overline{\rho(g)^T M \rho(g)} &= \sum_{i=1}^t \overline{\rho(g)^T} \overline{\rho(g_i)^T} \rho(g_i) \rho(g) = \\ &= \sum_{i=1}^t \overline{\rho(g_i g)^T} \rho(g_i g) = \sum_{i=1}^t \overline{\rho(g_i)^T} \rho(g_i) = M. \end{aligned} \quad (16.9.20)$$

Следовательно,  $M$  соответствует положительно определенной эрмитовой форме  $H$ , инвариантной при преобразованиях  $\rho(g)$ ,  $g \in H$ . При преобразовании переменных

$$x_j = \sum_{k=1}^n c_{jk} x'_k, \quad j = 1, \dots, n, \quad (16.9.21)$$

форма  $H$  принимает вид  $\bar{x}'_1 x'_1 + \dots + \bar{x}'_n x'_n = I(\bar{x}', x')$  и соответственно

$$\rho'(g) = C^{-1} \rho(g) C, \quad C = (c_{jk}), \quad (16.9.22)$$

— представление, эквивалентное  $\rho(g)$  и являющееся унитарным, что и требовалось доказать.

Можно проделать то же самое в матричной форме. Имеем

$$\bar{C}^T M C = I, \quad M = \overline{C^{-1}}^T C^{-1}; \quad (16.9.23)$$

для любого элемента  $g \in G$

$$\overline{\rho(g)^T M \rho(g)} = M, \quad (16.9.24)$$

или

$$\overline{\rho(g)^T \bar{C}^{-1}^T C^{-1} \rho(g)} = \bar{C}^{-1}^T C^{-1}, \quad (16.9.25)$$

откуда

$$\overline{(C^{-1} \rho(g) C)^T C^{-1} \rho(g) C} = I. \quad (16.9.26)$$

Поэтому представление  $\rho'(g) = C^{-1} \rho(g) C$  унитарно.

## 16.10. Несколько примеров представлений групп

Начнем с интересного для физиков примера представления бесконечной матричной группы другой матричной группой. Унитарные и унимодулярные матрицы второго порядка имеют вид

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \quad (16.10.1)$$

где  $\alpha$  и  $\beta$  — произвольные комплексные числа, подчиненные только условию  $\alpha\bar{\alpha} + \beta\bar{\beta} = 1$ . Группа  $U_2$  всех таких матриц — это группа линейных преобразований:

$$\begin{aligned} u &= \alpha u' + \beta v', \\ v &= -\bar{\beta} u^1 + \bar{\alpha} v', \quad \alpha\bar{\alpha} + \beta\bar{\beta} = 1, \end{aligned} \quad (16.10.2)$$

оставляющих инвариантной форму  $\bar{u}u + \bar{v}v$ . С помощью комплексных переменных  $u$  и  $v$  можно определить три действительные переменные:

$$\begin{aligned} x_1 &= \bar{u}v + \bar{v}u, \\ x_2 &= \frac{1}{i} (\bar{u}v - \bar{v}u), \\ x_3 &= \bar{u}u - \bar{v}v. \end{aligned} \quad (16.10.3)$$

При этом

$$x_1^2 + x_2^2 + x_3^2 = (\bar{u}u + \bar{v}v)^2. \quad (16.10.4)$$

Линейное преобразование (16.10.2), примененное к (16.10.3), индуцирует действительное линейное преобразование переменных  $x_1, x_2, x_3$ , принадлежащее в силу равенства (16.10.4) действительной ортогональной группе  $O_3$ . Выпишем это линейное преобразование:

$$\begin{aligned} x_1 &= \frac{1}{2} (\alpha^2 + \bar{\alpha}^2 - \beta^2 - \bar{\beta}^2) x'_1 + \frac{i}{2} (-\alpha^2 + \bar{\alpha}^2 - \beta^2 + \bar{\beta}^2) x'_2 + \\ &\quad + (-\alpha\beta - \bar{\alpha}\bar{\beta}) x'_3, \\ x_2 &= \frac{i}{2} (\alpha^2 - \bar{\alpha}^2 - \beta^2 + \bar{\beta}^2) x'_1 + \frac{1}{2} (\alpha^2 + \bar{\alpha}^2 + \beta^2 + \bar{\beta}^2) x'_2 + \\ &\quad + i(\bar{\alpha}\beta - \alpha\bar{\beta}) x'_3, \\ x_3 &= (\bar{\alpha}\bar{\beta} + \beta\bar{\alpha}) x'_1 + i(\bar{\alpha}\beta - \beta\bar{\alpha}) x'_2 + \\ &\quad + (\alpha\bar{\alpha} - \beta\bar{\beta}) x'_3. \end{aligned} \quad (16.10.5)$$

Таким образом, мы получили представление  $\rho$ , выражаемое формулами (16.10.5), группы  $U_2$  матрицами трехмерной ортогональной группы  $O_3$ . Это представление не точно; два элемента отображаются в один: матрицы  $\begin{pmatrix} 1, 0 \\ 0, 1 \end{pmatrix}$  и  $\begin{pmatrix} -1, 0 \\ 0, -1 \end{pmatrix}$  группы  $U_2$  представляются единицей группы  $O_3$ . Образом группы  $U_2$  при этом представлении является группа собственных вращений (группа матриц с определителем  $+1$ ). При этом прообраз в  $U_2$  некоторой группы  $G$  собственных вращений известен как „удвоенная

группа"  $2G^1$ ). Группа  $2G$  является расширением подгруппы порядка 2 из центра с помощью фактор-группы, изоморфной группе  $G$ .

Паули [1] обнаружил, что если физической системе  $S$  сопоставлена некоторая подгруппа  $K$  группы  $O_3$ , то волновой функции электронного спина системы  $S$  соответствует удвоенная группа  $2K$ .

Наряду с (16.10.5) существует другая формула, устанавливающая явную связь между группой  $U_2$  и ее представлением матрицами из  $O_3$ . Пусть дано собственное вращение евклидова трехмерного пространства (т. е. элемент группы  $O_3$ ),

пусть  $OT$  — прямая пересечения координатной плоскости  $XOY$  и ее образа  $X'OX'$ . Тогда (см. рис. 7), если  $\varphi$  — угол  $X'OT$ ,  $\psi$  — угол  $XOT$  и  $\theta$  — угол  $ZOZ'$ , мы можем найти соответствующий элемент группы  $U_2$  в виде (16.10.1), полагая

$$\alpha = \cos \frac{\theta}{2} \exp i\left(\frac{\varphi + \psi}{2}\right), \quad (16.10.6)$$

$$\beta = i \sin \frac{\theta}{2} \exp i\left(\frac{\varphi - \psi}{2}\right).$$

Эти формулы верны также и в случае совпадения плоскостей  $XOY$  и  $X'OX'$  (т. е. для случая вращения вокруг оси  $Z$ ), если считать, что  $\theta = 0$ ,  $\varphi = 0$ , а  $\psi$  — угол вращения вокруг оси  $Z$ .

Группа собственных вращений правильного тетраэдра может быть точно представлена группой подстановок его четырех вершин. Для каждой вершины существует подгруппа, не двигающая эту вершину и вращающая три вершины противоположной грани. Это подгруппа порядка 3. Симметрия, фиксирующая две вершины и переставляющая другие две вершины, есть зеркальное отображение относительно плоскости и не является собственным вращением, так как она меняет ориентацию. Таким образом, группа собственных вращений тетраэдра состоит из 12 элементов и изоморфна знакопеременной группе  $A_4$ . Выпишем ее классы сопряженных элементов:

$$\begin{aligned} C_1 &= (1), \\ C_2 &= (12)(34), (13)(24), (14)(23), \\ C_3 &= (123), (142), (134), (243), \\ C_4 &= (132), (124), (143), (234). \end{aligned} \quad (16.10.7)$$

<sup>1)</sup> Автор называет эту подгруппу "double group" — удвоенная группа. — Прим. перев.

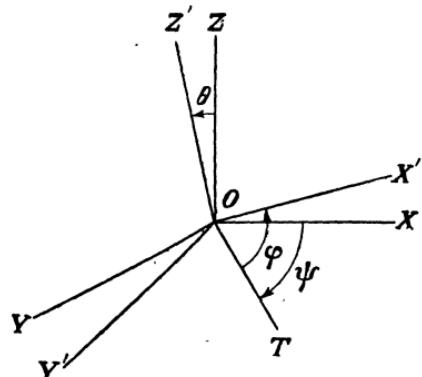


Рис. 7. Поворот в трехмерном пространстве.

Таблица умножения этих классов имеет вид

$$\begin{aligned}
 C_1C_i &= C_iC_1 = C_i, \quad i = 1, 2, 3, 4. \\
 C_2^2 &= 3C_1 + 2C_2, \\
 C_2C_3 &= C_3C_2 = 3C_3, \\
 C_2C_4 &= C_4C_2 = 3C_4, \\
 C_3^2 &= 4C_4, \\
 C_3C_4 &= C_4C_3 = 4C_1 + 4C_2, \\
 C_4^2 &= 4C_3.
 \end{aligned} \tag{16.10.8}$$

Будем искать теперь идемпотенты центра  $Z$  группового кольца, образующие ортогональный базис для  $Z$ . Это те и только те идемпотенты  $e$ , для которых  $eZ$  — минимальный идеал кольца  $Z$ . Поэтому процесс нахождения таких идемпотентов можно рассматривать как разложение кольца  $Z$  в прямую сумму (двусторонних) идеалов. В частности, любой собственный делитель нуля дает идеал центра  $Z$ , отличный от нуля. Таким образом, находя собственные делители нуля в двусторонних идеалах, мы тем самым находим еще меньшие двусторонние идеалы и, наконец, минимальные идеалы, а уже отсюда — ортогональные идемпотенты. Пусть  $f$  — идемпотент центра  $Z$ . Если  $fC_i = a_i f$  для любого класса  $C_i$ , то  $fZ$  — минимальный идеал в  $Z$ , а  $f$  — один из ортогональных идемпотентов. Если же для некоторого класса  $C$  произведение  $fC$  линейно не зависит от  $f$ , то пусть  $s$  — такое наименьшее целое число, что элементы  $fC^j$ ,  $j = 0, \dots, s - 1$ , линейно независимы, а  $fC^s$  зависит от них. Тогда  $f(C^s + a_1C^{s-1} + \dots + a_s) = 0$ . Присоединим к полю, из которого берутся коэффициенты, если необходимо, корень многочлена  $x^s + a_1x^{s-1} + \dots + a_s$ . Если  $u$  — такой корень, то  $f(C - u)$  — собственный делитель нуля идеала  $fZ$ , позволяющий указать еще меньший двусторонний идеал. Это общее построение и применяется при изучении группы вращений тетраэдра.

Для любой группы  $G$  порядка  $g$  сумма всех ее элементов, деленная на  $g$ , есть идемпотент  $e$ , которому соответствует минимальный идеал центра  $Z$ . Этот идемпотент соответствует единичному представлению группы  $G$ . В нашем примере  $e = e_1 = (C_1 + C_2 + C_3 + C_4)/12$ . Отметим, что из тождеств (16.10.8) следует равенство

$$C_2^2 - 2C_2 - 3C_1 = (C_2 - 3C_1)(C_2 + C_1) = 0. \tag{16.10.9}$$

Отсюда ясно, что  $C_2 - 3C_1$  и  $C_2 + C_1$  — собственные делители нуля. Далее находим, что  $(C_2 - 3C_1)Z$  — минимальный идеал и

что  $e_2 = (3C_1 - C_2)/4$  — идемпотент, порождающий этот минимальный идеал, причем  $e_1e_2 = e_2e_1 = 0$ . Образуем теперь идемпотент  $f = 1 - e_1 - e_2$ , который должен служить единицей для дополнения к  $e_1Z \oplus e_2Z$  в центре  $Z$ . Действительно, идеал  $fZ$  имеет размерность 2 и  $f = e_3 + e_4$ , где  $e_3$  и  $e_4$  — остальные ортогональные идемпотенты базиса центра  $Z$ . Теперь находим:

$$\begin{aligned} f &= (2C_1 + 2C_2 - C_3 - C_4)/12, \\ fC_1 &= f, \\ fC_2 &= 3f, \\ fC_3 &= (-4C_1 - 4C_2 + 8C_3 - 4C_4)/12, \\ fC_4 &= (-4C_1 - 4C_2 - 4C_3 + 8C_4)/12. \end{aligned} \quad (16.10.10)$$

При этом идеал  $fZ$  должен иметь размерность 2. Отметим, что

$$fC_4 + fC_3 + 4f = 0, \quad (16.10.11)$$

откуда видно, что  $fZ$  имеет размерность 2. Справедливо также следующее соотношение:

$$f(C_3^2 + 4C_3 + 16) = 0. \quad (16.10.12)$$

Если присоединить к полю рациональных чисел комплексный кубический корень из единицы  $\omega = (-1 + \sqrt[3]{3}i)/2$ , то равенство (16.10.12) примет вид

$$f(C_3 - 4\omega)(C_3 - 4\omega^2) = 0. \quad (16.10.13)$$

Поэтому главные идеалы, порожденные элементами  $f(C_3 - 4\omega)$  и  $f(C_3 - 4\omega^2)$ , содержатся в главном идеале  $fZ$ . В (16.10.14) первый из этих элементов отличается на скалярный множитель от идемпотента  $e_3$ , а второй — от  $e_4$ :

$$\begin{aligned} e_1 &= (C_1 + C_2 + C_3 + C_4)/12, \\ e_2 &= (3C_1 - C_2)/4, \\ e_3 &= (C_1 + C_2 + \omega C_3 + \omega^2 C_4)/12, \\ e_4 &= (C_1 + C_2 + \omega^2 C_3 + \omega C_4)/12, \\ e_1 + e_2 + e_3 + e_4 &= C_1 = 1. \end{aligned} \quad (16.10.14)$$

Пользуясь этими выражениями минимальных ортогональных идемпотентов через классы сопряженных элементов, можно легко получить таблицу для характеров, и обратно. Непосредственно перед теоремой 16.6.10 мы установили соотношение

$$C_k = h_k \sum_a \frac{\chi_k^a}{n_a} e_a. \quad (16.10.15)$$

Умножим это равенство на  $\bar{\chi}_k^b$  и просуммируем по  $k$ :

$$\sum_k \bar{\chi}_k^b C_k = \sum_{a, k} \frac{h_k \bar{\chi}_k^b \chi_k^a e_a}{n_a}. \quad (16.10.16)$$

Если правую часть сначала просуммировать по  $k$ , а затем, применяя соотношение ортогональности

$$\sum_k h_k \bar{\chi}_k^b \chi_k^a = \delta_{ab} g, \quad (16.10.17)$$

просуммировать по  $a$ , то все члены будут равны нулю, кроме членов, для которых  $a = b$ . Тогда (16.10.16) можно записать так:

$$\sum_k \bar{\chi}_k^b C_k = g e_b / n_b. \quad (16.10.18)$$

Это мы запишем в форме

$$e_b = \frac{n_b}{g} \sum_k \bar{\chi}_k^b C_k. \quad (16.10.19)$$

Так как мы знаем, что характер класса, состоящего из единицы, равен степени представления  $\bar{\chi}_1^b = n_b$ , коэффициент при  $C_1$  в выражении (16.10.19) равен  $n_b^2/g$ . Этим определяется число  $n_b$ , и мы можем затем использовать равенство (16.10.19) для определения остальных характеров.

Используя соотношение (16.10.19) и равенства (16.10.14) для группы вращений тетраэдра, мы можем выписать таблицу характеров для нее:

	$C_1$	$C_2$	$C_3$	$C_4$
$\rho_1$	1	1	1	1
$\rho_2$	3	-1	0	0
$\rho_3$	1	1	$\omega^2$	$\omega$
$\rho_4$	1	1	$\omega$	$\omega^2$

(16.10.20)

Обратно, используя таблицу характеров (16.10.20), мы могли бы с помощью формул (16.10.19) определить минимальные ортогональные идемпотенты (16.10.14).

Три неприводимых представления степени один  $\rho_1$ ,  $\rho_3$  и  $\rho_4$  можно, конечно, найти прямо из таблицы характеров.

По теореме 16.6.15 представление группы вращений тетраэдра  $A_4$  есть сумма единичного представления и неприводимого представления, которое, являясь представлением степени 3, должно совпадать с  $\rho_2$ . Подстановка из  $A_4$  над переменными  $x_1$ ,  $x_2$ ,  $x_3$  и  $x_4$  оставляет на месте линейную форму  $x_1 + x_2 + x_3 + x_4$  и переводит в себя дополнительное пространство, натянутое на

$y_1 = x_1 - x_4$ ,  $y_2 = x_2 - x_4$ ,  $y_3 = x_3 - x_4$ . Подстановка (12)(34) представляет собой следующее линейное преобразование:

$$\begin{aligned}x_1 &= x'_2, \\x_2 &= x'_1, \\x_3 &= x'_4, \\x_4 &= x'_3,\end{aligned}\tag{16.10.21}$$

а для  $y_1$ ,  $y_2$ ,  $y_3$  — преобразование

$$\begin{aligned}y_1 &= y'_2 - y'_3, \\y_2 &= y'_1 - y'_3, \\y_3 &= -y'_3.\end{aligned}\tag{16.10.22}$$

Таким образом,

$$\rho_2[(12)(34)] = \begin{pmatrix} 0, 1, -1 \\ 1, 0, -1 \\ 0, 0, -1 \end{pmatrix}.\tag{16.10.23}$$

Аналогично

$$\rho_2[(123)] = \begin{pmatrix} 0, 1, 0 \\ 0, 0, 1 \\ 1, 0, 0 \end{pmatrix}.\tag{16.10.24}$$

Так как подстановки (12)(34) и (123) порождают всю группу  $A_4$ , мы, таким образом, нашли представление всей этой группы. Это не есть ортогональная форма для представления  $\rho_2$ , но она может быть получена из следующего примера, так как группа вращений тетраэдра является подгруппой группы вращений октаэдра.

Группа симметрий куба была рассмотрена в примере 2 главы 1. Собственные вращения куба образуют группу  $G_{24}$  порядка 24, порожденную элементами

$$a = \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 2, 3, 4, 1, 6, 7, 8, 5 \end{pmatrix} = (1234)(5678)$$

и

$$\begin{aligned}b &= \begin{pmatrix} 1, 2, 3, 4, 5, 6, 7, 8 \\ 1, 4, 8, 5, 2, 3, 7, 6 \end{pmatrix} = \\&= (1)(245)(7)(386).\end{aligned}$$

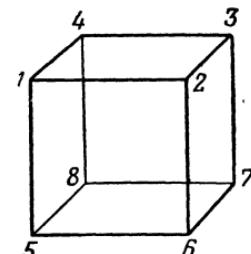


Рис. 8. Симметрии куба.

Группа  $G_{24}$  является также группой симметрий правильного октаэдра, вершинами которого служат центры всех граней данного куба. Таким образом, группу  $G_{24}$  можно также рассматривать как группу подстановок шести граней куба, соответствующих шести

вершинам вписанного октаэдра. Выберем шесть букв, соответствующих шести вершинам вписанного октаэдра, каждую из которых укажем вместе с ее трехмерными координатами.

Буквы	Грани куба	Вершины октаэдра
$x_1$	1234	(0, 0, 1)
$x_2$	1256	(0, 1, 0)
$x_3$	1458	(-1, 0, 0)
$x_4$	5678	(0, 0, -1)
$x_5$	3478	(0, -1, 0)
$x_6$	2367	(1, 0, 0)

Тогда  $a = (x_1)(x_4)(x_2x_6x_5x_3)$ ,  $b = (x_1x_3x_2)(x_4x_6x_5)$ . Выпишем каждый из 24 элементов группы  $G_{24}$  как подстановку букв  $x_i$  и как мономиальное линейное преобразование координат  $x, y, z$ , которому соответствует подстановка вершин октаэдра.

Класс	$g_i$	Подстановка	$x$ ,	$y$ ,	$z$
$C_1$	$g_1$	$(x_1)$	$x$ ,	$y$ ,	$z$
$C_2$	$g_2$	$(x_1)(x_4)(x_2x_5)(x_3x_6)$	$-x$ ,	$-y$ ,	$z$
	$g_3$	$(x_1x_4)(x_2)(x_5)(x_3x_6)$	$-x$ ,	$y$ ,	$-z$
	$g_4$	$(x_1x_4)(x_2x_5)(x_3)(x_6)$	$x$ ,	$-y$ ,	$-z$
$C_3$	$g_5$	$(x_1)(x_4)(x_2x_6x_5x_3)$	$-y$ ,	$x$ ,	$z$
	$g_6$	$(x_1)(x_4)(x_2x_3x_5x_6)$	$y$ ,	$-x$ ,	$z$
	$g_7$	$(x_2)(x_5)(x_1x_3x_4x_6)$	$z$ ,	$y$ ,	$-x$
	$g_8$	$(x_2)(x_5)(x_1x_6x_4x_3)$	$-z$ ,	$y$ ,	$x$
	$g_9$	$(x_3)(x_6)(x_1x_2x_4x_5)$	$x$ ,	$-z$ ,	$y$
	$g_{10}$	$(x_3)(x_6)(x_1x_5x_4x_2)$	$x$ ,	$z$ ,	$-y$
$C_4$	$g_{11}$	$(x_1x_2)(x_3x_6)(x_4x_5)$	$-x$ ,	$z$ ,	$y$
	$g_{12}$	$(x_1x_3)(x_2x_5)(x_4x_6)$	$-z$ ,	$-y$ ,	$-x$
	$g_{13}$	$(x_1x_4)(x_2x_6)(x_3x_5)$	$y$ ,	$x$ ,	$-z$
	$g_{14}$	$(x_1x_4)(x_2x_3)(x_5x_6)$	$-y$ ,	$-x$ ,	$-z$
	$g_{15}$	$(x_1x_5)(x_2x_4)(x_3x_6)$	$-x$ ,	$-z$ ,	$-y$
	$g_{16}$	$(x_1x_6)(x_2x_5)(x_3x_4)$	$z$ ,	$-y$ ,	$x$

$C_5$	$g_{17}$	$(x_1x_2x_3)(x_4x_5x_6)$	$-z, -x, y$
	$g_{18}$	$(x_1x_2x_6)(x_3x_4x_5)$	$z, x, y$
	$g_{19}$	$(x_1x_3x_2)(x_4x_6x_5)$	$-y, z, -x$
	$g_{20}$	$(x_1x_3x_5)(x_2x_4x_6)$	$y, -z, -x$
	$g_{21}$	$(x_1x_5x_3)(x_2x_6x_4)$	$-z, x, -y$
	$g_{22}$	$(x_1x_5x_6)(x_2x_3x_4)$	$z, -x, -y$
	$g_{23}$	$(x_1x_6x_2)(x_3x_5x_4)$	$y, z, x$
	$g_{24}$	$(x_1x_6x_5)(x_2x_4x_3)$	$-y, -z, x$

Мы можем отобразить четные подстановки группы  $G_{24}$  (т. е. подстановки из классов  $C_1, C_2, C_5$ ) в +1, а нечетные (т. е. подстановки из классов  $C_3, C_4$ ) — в -1. Получаем, кроме единичного представления, еще одно представление степени один. Так как степени  $n_i$  неприводимых представлений удовлетворяют соотношению

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24, \quad (16.10.25)$$

при  $n_1 = n_2 = 1$  находим, что числа  $n_3, n_4, n_5$  равны 2, 3, 3. Трехмерное представление в пространстве  $(x, y, z)$ , соответствующее подстановкам вершин октаэдра, имеет следующие характеристики:

$$\begin{aligned} \chi_1 &= 3, \quad \chi_2 = \chi(g_2) = -1, \quad \chi_3 = \chi(g_5) = 1, \\ \chi_4 &= \chi(g_{11}) = -1, \quad \chi_5 = \chi(g_{17}) = 0. \end{aligned} \quad (16.10.26)$$

Вообще говоря, если

$$\rho = \sum_a c_a \rho_a \quad (16.10.27)$$

— сумма неприводимых представлений  $\rho_a$ , то для  $i$ -го класса имеем

$$\chi_i = \sum_a c_a \chi_i^a \quad (16.10.28)$$

и в силу отношений ортогональности

$$\sum_i h_i \chi_i \bar{\chi}_i = g \sum_a c_a^2. \quad (16.10.29)$$

Так как для нашего представления степени 3 из (16.10.26) вытекает, что

$$\sum_i h_i \chi_i \bar{\chi}_i = 24, \quad (16.10.30)$$

то отсюда следует, что  $\sum_a c_a^2 = 1$ . Поэтому наше представление (которое мы обозначим через  $\rho_4$ ) неприводимо. Заметим, что пред-

ствление  $\rho_4$  ортогонально, и так как четные подстановки (элементы классов  $C_1, C_2, C_5$ ) образуют подгруппу, изоморфную группе тетраэдра, мы получаем ортогональное представление степени 3, которое мы хотели получить при рассмотрении предыдущего примера.

Мы имеем теперь частичную таблицу характеров:

	$h_1 = 1$	$h_2 = 3$	$h_3 = 6$	$h_4 = 6$	$h_5 = 8$	
	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	
$\rho_1$	1	1	1	1	1	
$\rho_2$	1	1	-1	-1	1	(16.10.31)
$\rho_3$	2	$y_2$	$y_3$	$y_4$	$y_5$	
$\rho_4$	3	-1	1	-1	0	
$\rho_5$	3	$z_2$	$z_3$	$z_4$	$z_5$	

Отношениями ортогональности при этом являются равенства

$$\begin{aligned} 1 + 1 + 2y_2 - 3 + 3z_2 &= 0, \\ 1 + 1 + y_2^2 + 1 + z_2^2 &= 8, \end{aligned} \quad (16.10.32)$$

первое из которых — соотношение для первого и второго столбцов таблицы, а второе — только для второго столбца. Решениями этой системы являются пары  $y_2 = 2, z_2 = -1$  и  $y_2 = -\frac{22}{13}, z_2 = \frac{19}{13}$ . Так как  $y_2$  есть сумма двух квадратных корней из единицы  $y_2 = \pm 1 \pm 1$ , первое решение системы  $y_2 = 2$  и  $z_2 = -1$  истинно.

Соотношения ортогональности для третьего и первого столбцов и для третьего и второго соответственно дают:

$$\begin{aligned} 1 - 1 + 2y_3 + 3 + 3z_3 &= 0, \\ 1 - 1 + 2y_3 - 1 - z_3 &= 0. \end{aligned} \quad (16.10.33)$$

Из этой системы уравнений получаем, что  $y_3 = 0, z_3 = -1$ . Подобным образом мы можем найти остальные неизвестные таблицы, которая окончательно примет вид

	$h_1 = 1$	$h_2 = 3$	$h_3 = 6$	$h_4 = 6$	$h_5 = 8$	
	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	
$\rho_1$	1	1	1	1	1	
$\rho_2$	1	1	-1	-1	1	(16.10.34)
$\rho_3$	2	2	0	0	-1	
$\rho_4$	3	-1	1	-1	0	
$\rho_5$	3	-1	-1	1	0	

Представление  $\rho$  степени 8 группы  $G_{24}$  как группы подстановок вершин куба имеет следующие характеристики:

	$C_1$	$C_2$	$C_3$	$C_4$	$C_5$	
$\chi$	8	0	0	0	2	

(16.10.35)

Зная эти характеристики, мы можем найти разложение представления  $\rho$ , так как при

$$\rho = \sum_a c_a \rho_a,$$

$$\chi_i = \sum_a c_a \chi_i^a \quad (16.10.36)$$

из соотношений ортогональности получаем, что

$$\sum_i h_i \chi_i \bar{\chi}_i^b = \sum_{i,a} c_a h_i \chi_i^a \bar{\chi}_i^b = g \sum_a c_a \delta_{ab} = g c_b, \quad (16.10.37)$$

т. е. получаем кратность  $c_b$ , с которой каждое неприводимое представление  $\rho_b$  встречается в представлении  $\rho$ . Таким путем из таблицы (16.10.35) мы находим, что

$$\rho = \rho_1 + \rho_2 + \rho_4 + \rho_5. \quad (16.10.38)$$

Мы можем использовать это равенство, чтобы отсюда найти в явном виде представление  $\rho_5$ . Используя формулы (16.10.19) и таблицу характеристик (16.10.34), находим

$$e_5 = (3C_1 - C_2 - C_3 + C_4)/4. \quad (16.10.39)$$

Представление  $\rho$  группы  $G_{24}$  является также представлением группового кольца  $R_G$ . Мы находим следующее выражение для  $\rho(e_5)$ :

$$\rho(e_5) = \frac{1}{4} \begin{pmatrix} 3 & -1 & -1 & -1 & -1 & -1 & -1 & 3 & -1 \\ -1 & 3 & -1 & -1 & -1 & -1 & -1 & -1 & 3 \\ -1 & -1 & 3 & -1 & 3 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 3 & -1 & 3 & -1 & -1 & -1 \\ -1 & -1 & 3 & -1 & 3 & -1 & -1 & -1 & -1 \\ -1 & -1 & -1 & 3 & -1 & 3 & -1 & -1 & -1 \\ 3 & -1 & -1 & -1 & -1 & -1 & 3 & -1 & -1 \\ -1 & 3 & -1 & -1 & -1 & -1 & -1 & -1 & 3 \end{pmatrix}. \quad (16.10.40)$$

Выбрав элементы  $x_i = (0, \dots, \overset{(i)}{1}, \dots, 0)$ ,  $i = 1, \dots, 8$ , в качестве базиса модуля  $M$  представления  $\rho$ , мы получим, что строки матрицы  $\rho(e_5)$  порождают подмодуль  $Me_5$ , имеющий, конечно, размерность 3. Мы можем взять первые три строки  $r_1, r_2, r_3$

в качестве его базиса. Однако удобнее выбрать в качестве базисных векторов векторы, пропорциональные векторам  $r_1 + r_3$ ,  $r_1 + r_2$ ,  $r_2 + r_3$ , а именно

$$\begin{aligned}y_1 &= x_1 - x_2 + x_3 - x_4 + x_5 - x_6 + x_7 - x_8, \\y_2 &= x_1 + x_2 - x_3 - x_4 - x_5 - x_6 + x_7 + x_8, \\y_3 &= x_1 - x_2 - x_3 + x_4 - x_5 + x_6 + x_7 - x_8.\end{aligned}\quad (16.10.41)$$

В этом базисе вычисляем, что

$$\begin{aligned}\rho_5(a) &= \begin{pmatrix} -1, & 0, & 0 \\ 0, & 0, & -1 \\ 0, & 1, & 0 \end{pmatrix} = \begin{pmatrix} y_1, & y_2, & y_3 \\ -y_1, & -y_3, & y_2 \end{pmatrix}, \\ \rho_5(b) &= \begin{pmatrix} 0, & 1, & 0 \\ 0, & 0, & 1 \\ 1, & 0, & 0 \end{pmatrix} = \begin{pmatrix} y_1, & y_2, & y_3 \\ y_2, & y_3, & y_1 \end{pmatrix}.\end{aligned}\quad (16.10.42)$$

Таким образом,  $\rho_5$  — мономиальное ортогональное представление группы  $G_{24}$ , определяемое равенствами (16.10.42). Но  $\rho_5(G_{24})$  не является группой собственных вращений, так как детерминант матрицы  $\rho_5(a)$  равен  $-1$ . Представление, эквивалентное  $\rho_5$ , можно получить из представления  $\rho_4$ , умножая матрицы, соответствующие элементам классов  $C_3$  и  $C_4$ , на  $-1$ , т. е. представление  $\rho_5$  эквивалентно кронекеровскому произведению представлений  $\rho_4$  и  $\rho_2$ .

Представление  $\rho_3$  не является точным, и ядро его порядка 4 состоит из единицы и элементов класса  $C_2$ . Это представление порождается элементами

$$\rho_3(a) = \begin{pmatrix} 0, & 1 \\ 1, & 0 \end{pmatrix}, \quad \rho_3(b) = \begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}. \quad (16.10.43)$$

При представлении  $\rho_4$  группы  $G_{24}$  как группы собственных вращений мы имеем

$$\rho_4(a) = \begin{pmatrix} 0, & -1, & 0 \\ 1, & 0, & 0 \\ 0, & 0, & 1 \end{pmatrix}, \quad \rho_4(b) = \begin{pmatrix} 0, & -1, & 0 \\ 0, & 0, & 1 \\ -1, & 0, & 0 \end{pmatrix}. \quad (16.10.44)$$

Поэтому  $\rho_4(G_{24})$  есть подгруппа группы  $O_3$ . Используя формулы (16.10.5), отображающие группу  $U_2$  на  $O_3$ , находим, что

$$\begin{aligned}\frac{\pm 1}{2} \begin{pmatrix} 1-i, & 0 \\ 0, & 1+i \end{pmatrix} &\rightarrow \rho_4(a), \\ \frac{\pm 1}{2} \begin{pmatrix} 1-i, & -1+i \\ 1+i, & 1+i \end{pmatrix} &\rightarrow \rho_4(b).\end{aligned}\quad (16.10.45)$$

Группа  $D = 2G_{24}$  состоит из восьми классов сопряженных элементов. Вообще в группе  $2G$  классу  $C_i$  из группы  $G$  соответствует класс сопряженных элементов группы  $2G$  либо с удвоенным количеством элементов по сравнению с  $C_i$ , либо он распадается на два класса  $C'_i$  и  $C''_i = -C'_i$ , в каждом из которых столько же элементов, сколько и в классе  $C_i$  группы  $G$ .

Следуя Бетэ [1], мы можем выписать элементы группы  $D$ , выражая их через следующие четыре матрицы:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (16.10.46)$$

Выпишем элементы группы  $D$  по классам:

$$E = [1],$$

$$R = [-1],$$

$$C_2 = \pm [-i\sigma_x, -i\sigma_y, -i\sigma_z],$$

$$C'_3 = \left[ \frac{1 \pm i\sigma_x}{\sqrt{2}}, \frac{1 \pm i\sigma_y}{\sqrt{2}}, \frac{1 \pm i\sigma_z}{\sqrt{2}} \right],$$

$$C''_3 = -C'_3,$$

$$C_4 = \pm \left[ \frac{-i(\sigma_y \pm \sigma_z)}{\sqrt{2}}, \frac{-i(\sigma_z \pm \sigma_x)}{\sqrt{2}}, \frac{-i(\sigma_x \pm \sigma_y)}{\sqrt{2}} \right], \quad (16.10.47)$$

$$C'_5 = \left[ \frac{1}{2} \{1 \pm i(\sigma_x + \sigma_y + \sigma_z)\}, \frac{1}{2} \{1 \pm i(-\sigma_x + \sigma_y - \sigma_z)\}, \right.$$

$$\left. \frac{1}{2} \{1 \pm i(-\sigma_x - \sigma_y + \sigma_z)\}, \frac{1}{2} \{1 \pm i(\sigma_x - \sigma_y - \sigma_z)\} \right],$$

$$C''_5 = -C'_5.$$

Так как группа  $G_{24}$  есть гомоморфный образ группы  $D$ , любое неприводимое представление группы  $G_{24}$  является также неприводимым представлением для  $D$ . Группа  $D$  обладает, однако, еще тремя неприводимыми представлениями, являющимися точными. Вот они:

	$E$	$R$	$C_2$	$C'_3$	$C''_3$	$C_4$	$C'_5$	$C''_5$
$\rho_6$	2	-2	0	$\sqrt{2}$	$-\sqrt{2}$	0	1	-1
$\rho_7$	2	-2	0	$-\sqrt{2}$	$\sqrt{2}$	0	1	-1
$\rho_8$	4	-4	0	0	0	0	-1	0

(16.10.48)

## Г л а в а 17

### СВОБОДНЫЕ ПРОИЗВЕДЕНИЯ И СВОБОДНЫЕ ПРОИЗВЕДЕНИЯ С ОБЪЕДИНЕННЫМИ ПОДГРУППАМИ<sup>1)</sup>

#### 17.1. Определение свободного произведения

Пусть  $G_i$  — множество групп, где  $i \in I$ ,  $I$  — вполне упорядоченное множество. Определим *свободное произведение*  $\prod_i^* G_i$  групп  $G_i$  аналогично тому, как определялась свободная группа с данными образующими.

Рассмотрим слова (или цепочки)

$$a_1 a_2 \dots a_t, \quad (17.1.1)$$

которые или пусты (пустое слово обозначается через 1), или состоят из элементов  $a_i$ , принадлежащих некоторым группам  $G_j$ . Для этих слов определяем отношения *элементарной эквивалентности*. Слово

$$a_1 a_2 \dots a_{i-1} a_i a_{i+1} \dots a_t \quad (E1)$$

эквивалентно слову  $a_1 \dots a_{i-1} a_i a_{i+1} \dots a_t$ , если  $a_i$  — единица некоторой группы  $G_j$ . Слово

$$a_1 a_2 \dots a_{i-1} a_i^* a_{i+1} \dots a_t \quad (E2)$$

эквивалентно слову  $a_1 \dots a_{i-1} a_i^* a_{i+1} \dots a_t$ , если элементы  $a_i$  и  $a_{i+1}$  принадлежат одной и той же группе  $G_j$  и если  $a_i a_{i+1} = a_i^* \in G_j$ .

Очевидно, что эти отношения элементарной эквивалентности являются симметричными. Будем говорить, что два слова  $x$  и  $y$  эквивалентны, если существует конечная последовательность  $x_1 = x, x_2, x_3, \dots, x_n = y$ , члены которой  $x_i$  и  $x_{i+1}$  элементарно эквивалентны при  $i = 1, \dots, n - 1$ . Все эквивалентные слова образуют класс.

Слово  $a_1 a_2 \dots a_t$  называется *редуцированным*, или *приведенным*, если оно пустое или если (1) ни один элемент  $a_i$  не равен единице своей группы  $G_j$  и (2) элементы  $a_i$  и  $a_{i+1}$  принадлежат разным группам  $G_j$  при  $j = 1, \dots, t - 1$ .

<sup>1)</sup> В оригинале „amalgamated products“.—Прим. ред.

Как и в § 7.1, мы можем определить  $W$ -процесс для слова  $f = a_1 a_2 \dots a_t$ , полагая

$$W_0 = 1,$$

$W_1 = 1$ , если  $a_1$  — единица своей группы,

$W_1 = a_1$  в противном случае.

Если слово  $W_t$  уже имеет редуцированный вид  $b_1 b_2 \dots b_s$ , то полагаем

1)  $W_{t+1} = b_1 \dots b_s a_{i+1}$ , если  $a_{i+1}$  — элемент, не равный единице своей группы и не содержащийся в той же группе, что и элемент  $b_s$ ,

2)  $W_{t+1} = b_1 \dots b_s$ , если  $a_{i+1}$  — единица своей группы,

3)  $W_{t+1} = b_1 \dots b_{s-1}$ , если  $b_s$  и  $a_{i+1}$  — элементы одной группы и  $b_s a_{i+1} = 1$ ,

4)  $W_{t+1} = b_1 \dots b_{s-1} b_s^*$ , если  $b_s$  и  $a_{i+1}$  — элементы одной группы и  $b_s a_{i+1} = b_s^* \neq 1$ .

Как и в § 7.1, можно показать, что слово  $W(f) = W_t$  является редуцированным, причем  $W$ -процесс приводит к одному и тому же результату для элементарно эквивалентных слов и, следовательно, для целого класса эквивалентных слов. Отсюда следует существование единственного приведенного слова в каждом классе. Если слово  $f = a_1 \dots a_t$  редуцировано, назовем число  $t$  его *длиной*.

Мы можем теперь определить произведение классов эквивалентных слов, полагая

$$[f_1][f_2] = [f_1 f_2]. \quad (17.1.2)$$

Следуя доказательству теоремы 7.1.1, можно показать, что это произведение не зависит от выбора представителей перемножаемых классов. Это произведение ассоциативно, и множество классов эквивалентных слов образует при этом умножении группу, единицей которой является класс, содержащий пустое слово. Эта группа и есть свободное произведение  $\prod_i^* G_i$  групп  $G_i$ ,  $i \in I$ . Заметим, что, согласно (E1), единица каждой группы  $G_i$  эквивалентна пустому слову 1. Поэтому в дальнейшем мы не будем различать все эти единицы. Элементы различных групп, отличные от единицы, являются неэквивалентными редуцированными словами и поэтому не отождествляются.

**Теорема 17.1.1.** Пусть  $G$  — группа, порожденная подгруппами  $H_i$ ,  $i \in I$ , где подгруппы  $H_i$  изоморфны соответствующим группам  $G_i$ . Тогда группа  $G$  является гомоморфным образом свободного произведения  $Q = \prod_i^* G_i$ .

**Доказательство.** Как и при доказательстве теоремы 7.1.2 рассмотрим элемент  $a_1 a_2 \dots a_t$  группы  $Q$ . Поставим в соответ-

ствие этому элементу произведение  $b_1 b_2 \dots b_t \in G$ , где  $b_i$  — элемент подгруппы  $H_j$ , соответствующий при изоморфизме элементу  $a_i$  группы  $G_j$ . Тогда эквивалентные слова отображаются в один и тот же элемент группы  $G$ . Это отображение группы  $Q$  на группу  $G$  сохраняет произведение и, следовательно, является гомоморфизмом.

## 17.2. Свободные произведения с объединенной подгруппой

Пусть задано множество групп  $G_i$ ,  $i \in I$ . Предположим, что каждая группа  $G_i$  содержит подгруппу  $U_i$  и что все подгруппы  $U_i$  изоморфны некоторой группе  $U$ , причем зафиксирован вполне определенный изоморфизм между подгруппой  $U_i$  и группой  $U$ . Мы хотим построить наиболее общую группу, порожденную группами  $G_i$ , в которой все группы  $U_i$  отождествлены друг с другом и составляют подгруппу  $U^1$ , изоморфную группе  $U$ . Ясно, что этой группой является образ свободного произведения групп  $G_i$ , если отождествить все элементы  $u_i \in U_i$ ,  $u_j \in U_j$ , соответствующие при заданных изоморфизмах групп  $U_i$ ,  $U_j$  с группой  $U$  одному и тому же элементу  $u \in U$ . Конечно, такая группа должна существовать, однако совсем не ясно, как происходят отождествления в свободном произведении групп на основе этих основных отождествлений. В частности, не исключена возможность, что при этом произойдет отождествление всех элементов с единицей. В действительности же этого случиться не может, и фактически это отождествление распространяется только на элементы подгрупп  $U_i$ .

Мы построим группу, порождаемую группами  $G_i$  с отождествленными подгруппами  $U_i$ . Ее и будем называть *свободным произведением групп  $G_i$  с объединенной подгруппой  $U$* . Рассмотрим слова  $a_1 a_2 \dots a_t$ , где каждое  $a_i$  — элемент некоторой группы  $G_j$ . Определим отношения элементарной эквивалентности.

(E1) *Если  $a_i = 1$ , то слово*

$$a_1 a_2 \dots a_{i-1} a_i a_{i+1} \dots a_t$$

*эквивалентно слову  $a_1 a_2 \dots a_{i-1} a_{i+1} \dots a_t$ .*

(E2) *Если  $a_i$  и  $a_{i+1}$  — элементы группы  $G_j$  и  $a_i a_{i+1} = a_i^* \in G_j$ , то слово*

$$a_1 a_2 \dots a_i a_{i+1} \dots a_t$$

*эквивалентно слову  $a_1 a_2 \dots a_i^* \dots a_t$ .*

(E3) *Если  $a_i = u_i$  — элемент подгруппы  $U_j \subseteq G_j$  и  $b_i = u_k \in U_k$  — элемент, образ которого в группе  $U$  при изоморфизме между  $U_k$  и  $U$  совпадает с образом элемента  $u_i$  при*

изоморфизме между  $U_i$  и  $U$ , то слово

$$a_1 \dots a_{i-1} a_i a_{i+1} \dots a_t$$

эквивалентно слову  $a_1 \dots a_{i-1} b_i a_{i+1} \dots a_t$ .

Определим теперь эквивалентность слов. Слова  $x$  и  $y$  эквивалентны, если существует такая конечная последовательность слов  $x = x_1, \dots, x_n = y$ , что слова  $x_i$  и  $x_{i+1}$  элементарно эквивалентны при  $i = 1, \dots, n - 1$ . Классы эквивалентных слов образуют группу относительно умножения  $[f][g] = [fg]$ . Как и в теореме 7.1.1, это произведение вполне определено. Построенная группа  $T$  есть свободное произведение групп  $G_i$  с объединенной подгруппой  $U$ . Или, кратко,  $T$  есть амальгамированное произведение групп  $G_i$ . Но пока мы ничего не знаем о строении группы  $T$ . Для его изучения нам понадобится каноническая запись элементов из  $T$ .

Определим каноническую запись слов вида  $f = a_1 a_2 \dots a_t$ , где  $a_i \in G_i$ , после чего будет необходимо показать, что все эквивалентные слова имеют одну и ту же каноническую запись. Тем самым будет показано, что она действительно является канонической записью элементов группы  $T$ .

В каждой группе  $G_i$ ,  $i \in I$ , выберем представителей  $x_{ik}$  левых смежных классов по подгруппе  $U_i$ , причем в качестве представителя класса  $U_i$  всегда будем выбирать единицу, а остальные представители выберем произвольно. Пусть

$$G_i = U_i + U_i x_{i2} + \dots + U_i x_{in_i}, \quad i \in I. \quad (17.2.1)$$

В силу элементарной эквивалентности (Е1) пустое слово играет роль единицы группы  $T$  и каждой группы  $G_i$ , а в силу эквивалентности (Е3) мы можем отождествить все подгруппы  $U_i$ ,  $i \in I$ , с группой  $U$ . После этого (17.2.1) можно переписать так:

$$G_i = U + U x_{i2} + \dots + U x_{in_i}, \quad i \in I. \quad (17.2.2)$$

Поэтому любой элемент  $g_i \in G_i$  может быть записан в виде

$$g_i = u \text{ или } g_i = uz, \quad u \in U, \quad z = x_{ik} \neq 1. \quad (17.2.3)$$

Для амальгамированного произведения удобно несколько видоизменить обычное определение длины слова. По определению полагаем, что  $l(a_0 a_1 \dots a_t) = t$ , если  $a_0 \in U$ , и  $l(a_1 \dots a_t) = t$ , если  $a_1 \notin U$ . Другими словами, мы не считаем первую букву, если она обозначает элемент из подгруппы  $U$ .

Будем говорить, что запись элемента группы  $T$  каноническая, если она имеет вид

$$f = uz_1 z_2 \dots z_t,$$

где  $u \in U$ , а  $z_j$ ,  $j = 1, \dots, t$ , — представители  $x_{ik} \neq 1$  смежных классов из (17.2.2), причем элементы  $z_j$  и  $z_{j+1}$ ,  $j = 1, \dots, t-1$  принадлежат различным группам  $G_i$ .

**Теорема 17.2.1.** В свободном произведении групп  $G_i$  с объединенной подгруппой  $U$  каждый класс эквивалентных слов содержит одно-единственное слово в канонической записи  $f = uz_1z_2 \dots z_t$ , где  $u \in U$ , а  $z_i$ ,  $i = 1, \dots, t$ , — представители  $x_{jk} \neq 1$  смежных классов групп  $G_i$  по подгруппе  $U$ , причем элементы  $z_i$  и  $z_{i+1}$ ,  $i = 1, \dots, t-1$ , принадлежат различным группам  $G_j$ .

Доказательство этой теоремы аналогично доказательству леммы из § 7.1. Из-за недостатка места мы его опустим. Более глубокое рассмотрение этого вопроса содержится в работах Х. Неймана [1, 2].

### 17.3. Теорема Куроша

Курош<sup>1)</sup> показал, что любая подгруппа свободного произведения есть опять свободное произведение. Мы докажем здесь этот результат. Аналогичное утверждение для подгрупп свободного произведения с объединенной подгруппой не имеет места. Если  $U$  — амальгамированная подгруппа, то в случае, когда число групп  $G_i$  больше двух, мы можем выбрать подгруппы  $H_i$  групп  $G_i$ , которые совершенно произвольно пересекаются с подгруппой  $U$ . Тогда подгруппы  $H_i$  будут объединяться разными способами, и мы получаем так называемые *обобщенные амальгамированные произведения*. Здесь возникает ряд затруднений, и теория в настоящее время еще не завершена.

**Теорема 17.3.1.** (Теорема Куроша.) Всякая подгруппа  $H \neq 1$  свободного произведения

$$G = \coprod_v^* A_v$$

опять является свободным произведением

$$H = F^* \coprod_j^* x_j^{-1} U_j x_j,$$

где  $F^*$  — свободная группа, а каждая из подгрупп  $x_j^{-1} U_j x_j$  — подгруппа, сопряженная с подгруппой  $U_j$  одного из свободных сомножителей  $A_v$  группы  $G$ .

Доказательство. Элементы свободных сомножителей группы  $G$  можно вполне упорядочить: первым элементом будем считать еди-

<sup>1)</sup> А. Курош [1]. Излагаемое здесь доказательство принадлежит автору [6].

ницу, затем упорядочиваем сами свободные сомножители и, наконец, внутри каждого сомножителя упорядочиваем элементы, не равные единице. Определим основанный на этом порядке лексикографический порядок элементов группы  $G$ . Пусть

$$g = a_1 a_2 \dots a_t$$

— приведенное представление элемента  $g \in G$ . Пустым произведением является единица; при  $g \neq 1$  каждая буква  $a_i \neq 1$  принадлежит одному из свободных сомножителей  $A_v$ , и ни одна пара соседних элементов  $a_i, a_{i+1}$  ( $i = 1, \dots, t - 1$ ) не принадлежит одной и той же группе  $A_v$ . Длина  $l(g)$  элемента  $g$ , по определению, равна нулю для  $g = 1$  и числу  $t$  букв в приведенном представлении для  $g \neq 1$ . Тогда лексикографический порядок элементов группы  $G$  определим следующим образом:

- 1) более короткое слово предшествует более длинному;
- 2) слова равной длины сравниваются побуквенно, начиная с первой буквы. Если первые члены не равны, то меньший из них определяет предшествующее слово; если же первые члены равны, то переходим к сравнению вторых и т. д.

Очевидно, что это полная упорядоченность элементов группы  $G$ .

Определим теперь другой, полулексикографический порядок элементов группы  $G$ . Для этого представим элемент  $g$  четной длины  $t = 2r$  в виде  $g = \alpha\beta^{-1}$ , где  $l(\alpha) = l(\beta) = r$ , а элемент  $g$  нечетной длины  $t = 2s + 1$  — в виде  $g = \alpha a_{s+1} \beta^{-1}$ , где  $l(\alpha) = l(\beta) = s$ . Полулексикографический порядок элементов определяется:

- 1) по длине слова  $g$ ;
- 2) при равных четных длинах элементы  $g = \alpha\beta^{-1}$  сравниваются по лексикографическому порядку слов  $\alpha$ , а в случае их равенства — по лексикографическому порядку слов  $\beta$ ;
- 3) при равных нечетных длинах элементы  $g = \alpha a_{s+1} \beta^{-1}$ , как и в предыдущем случае, сравниваются сначала по  $\alpha$ , а затем по  $\beta$ . Если же подслова  $\alpha$  и  $\beta$  равны у сравниваемых слов, то сравниваются элементы  $a_{s+1}$ .

Доказательство того основного факта, что подгруппа  $H$  группы  $G$  является свободным произведением, будет состоять в выборе при помощи полулексикографического порядка такого подмножества  $K$  элементов группы  $H$ , что (1) множество  $K$  порождает подгруппу  $H$  и (2) множество  $K$  порождает свободное произведение

$$F^* \prod_j^* x_j^{-1} U_j x_j, \quad (17.3.1)$$

где  $F^*$  — свободная группа,  $U_j$  — подгруппа некоторого свободного сомножителя  $A_v$  группы  $G$ .

Пусть множество  $K$  состоит из всех таких элементов  $k \neq 1$ , что (1)  $k \in H$  и (2)  $k$  не принадлежит группе, порожденной элементами из  $H$ , предшествующими элементу  $k$  в полулексикографическом порядке.

Так как  $H \neq 1$ , первый элемент  $h \neq 1$  подгруппы  $H$  принадлежит множеству  $K$ , которое, следовательно, не пусто. Рассмотрим группу  $|K|$ , порожденную множеством  $K$ . Очевидно,  $|K| \subseteq H$ . Если бы  $|K| \neq H$ , то существовал бы такой первый элемент  $h \in H$ , что  $h \notin |K|$ . Этот элемент  $h$  не принадлежит множеству  $K$  и поэтому является произведением элементов  $h_i$ , предшествующих  $h$  и принадлежащих подгруппе  $H$ . Но эти элементы  $h_i$  принадлежат подгруппе  $|K|$ , и поэтому элемент  $h$ , будучи произведением этих  $h_i$ , также принадлежит группе  $|K|$ . Итак,  $|K| = H$ , и первая часть утверждения доказана.

Будем пользоваться знаком  $<$  как для обозначения числовых неравенств, так и для обозначения лексикографического и полулексикографического порядка. Из контекста будет ясно, в каком смысле этот знак употребляется: полулексикографический порядок относится к целым словам, а лексикографический — к начальной или конечной части слова. Записывая элемент  $u \neq 1$  в виде  $u = \alpha\beta^{-1}$  или  $u = \alpha\alpha\beta^{-1}$ , мы не можем получить равенство  $\alpha = \beta$  для слов четной длины, так как  $\alpha\alpha^{-1} = 1$ . Для слов нечетной длины равенство  $\alpha = \beta$  возможно; элементы группы  $H$  вида  $\alpha\alpha\alpha^{-1}$  для фиксированного  $\alpha$  и  $a$ , принадлежащего некоторой определенной группе  $A_v$ , вместе с единицей образуют подгруппу  $\alpha B \alpha^{-1}$ , сопряженную с подгруппой  $B \subseteq A_v$ . Назовем элементы вида  $\alpha\alpha\alpha^{-1}$  трансформами. Расширим множество  $K$  до более объемлющего множества  $T$ , состоящего из  $K$  и для каждого  $\alpha$  и  $A_v$  из трансформ  $\alpha a^1 \alpha^{-1}$ ,  $a^1 \in A_v$ , порожденных трансформами  $\alpha\alpha\alpha^{-1}$ ,  $\alpha \in A_v$ , принадлежащими множеству  $K$ . Следовательно, множество  $T$  состоит из элементов подгруппы  $H$ , которые не порождаются предшествующими им элементами, и трансформ  $\alpha a^1 \alpha^{-1}$ , порождаемых предшествующими трансформами того же вида.

Элемент  $h \in H$  можно записать в виде

$$h = u_1 u_2 \dots u_t, \quad (17.3.2)$$

где  $u_i \in T$  или  $u_i \in T^{-1}$  (множество обратных элементов из  $T$ ). Более того, мы можем считать, что в. (17.3.2), во-первых,  $u_i u_{i+1} \neq 1$  ( $i = 1, \dots, t - 1$ ) и, во-вторых, никакие два соседних элемента  $u_i$ ,  $u_{i+1}$  не принадлежат одной и той же сопряженной подгруппе  $\alpha B \alpha^{-1}$ , где  $B \subseteq A_v$ . При этих условиях мы будем говорить, что выражение  $u_1 \dots u_t$  полуприведено.

Доказательство теоремы можно будет легко закончить, как только мы покажем, что никакое непустое полуприведенное слово

не равно единице. Действительно, тогда отсюда получим, что элементы из множества  $K$ , не являющиеся трансформами, порождают свободную группу  $F$  и что  $H$  совпадает со свободным произведением группы  $F$  и сопряженных подгрупп  $\alpha Ba^{-1}$ ,  $B \subseteq A_v$ .

Если  $u$  — элемент из  $K$  и  $u^{-1} \neq u$ , то  $u < u^{-1}$ , так как  $u = (u^{-1})^{-1}$ , и элемент  $u^{-1}$  не может предшествовать элементу  $u$ . Далее, если  $u \neq v$  — элементы из  $K$ , то элемент  $w = u^\varepsilon v^\eta$  ( $\varepsilon, \eta = \pm 1$ ) следует и за  $u$ , и за  $v$ , так как любые два элемента из  $u$ ,  $v$ ,  $w$  порождают третий, но в силу выбора множества  $K$  ни один из элементов  $u$  и  $v$  не порождается предшествующими элементами. Эти два принципа лежат в основе изучения умножения элементов из множеств  $T$  и  $T^{-1}$ . В процессе приведения элемента  $a_1 a_2 \dots a_m$  группы  $G$ , где каждый сомножитель  $a_i$  принадлежит одной из перемножаемых групп, будем говорить, что элементы  $a_i$  и  $a_{i+1}$  объединяются в  $a_i^1$ , если они принадлежат одному и тому же свободному сомножителю  $A_v$  и  $a_i a_{i+1} = a_i^1 \neq 1$ , и будем говорить, что они сокращаются, если  $a_i a_{i+1} = 1$ .

**Лемма 17.3.1.** *Если  $u = \alpha\beta^{-1}$  или  $\alpha a\beta^{-1} \in T$ , причем  $\alpha \neq \beta$ , то  $\alpha < \beta$ .*

**Доказательство.** Так как  $\beta \neq \alpha$ , то  $u \in K$ . Если  $\beta < \alpha$ , то мы имели бы, что  $u^{-1} < u$ . Таким образом, элементы из  $T$  могут быть трех типов:

- 1)  $l(u)$  — четное число,  $u = \alpha\beta^{-1}$ ,  $\alpha < \beta$ ,  $u \in K^-$ ;
- 2)  $l(u)$  — нечетное число,  $u = \alpha a\beta^{-1}$ ,  $\alpha < \beta$ ,  $u \in K$ ;
- 3)  $l(u)$  — нечетное число,  $u = \alpha a \alpha^{-1}$  — элемент, порожденный трансформами того же вида из множества  $K$ .

**Лемма 17.3.2.** *Если элементы  $u \neq v$  принадлежат множеству  $T$  и не содержатся в одной и той же подгруппе  $\alpha Ba^{-1}$ , а  $w$  — любой из элементов  $u^\varepsilon v^\eta$ ,  $v^\eta u^\varepsilon$  ( $\varepsilon, \eta = \pm 1$ ), то элемент  $w$  следует за  $u$  и  $v$  в полулексикографическом порядке. Отсюда вытекают следующие ограничения на сокращения и объединения в произведении  $w$ :*

- 1) если  $u = \alpha\beta^{-1}$ ,  $\beta$  не сокращается, а  $\alpha$  сокращается, то буква, соседняя с  $\beta^{-1}$ , не объединяется<sup>1)</sup>;
- 2) если  $u = \alpha a\beta^{-1}$ ,  $\alpha < \beta$ ,  $\alpha$  и  $a$  не сокращаются, а  $\beta$  сокращается, то  $a$  не объединяется;
- 3) если  $u = \alpha a \alpha^{-1} \in \alpha Ba^{-1}$ , то  $\alpha$  и  $a$  не сокращаются,

<sup>1)</sup> В случае объединения даже одной буквы из  $\beta$  с буквой из  $v$  длина  $w$  будет меньше, чем длина  $v$ , что противоречит утверждению леммы. — Прим. ред.

а если при этом  $v^\eta = aa^1\sigma$ ,  $a, a^1 \in A_v$ , то  $a^1$  — первый элемент в смежном классе  $Ba^*$ ).

**Доказательство.** Пусть из двух различных элементов  $u$  и  $v$  множества  $T$  первый предшествует второму,  $u < v$ . Если элемент  $w$  не следует ни за  $u$ , ни за  $v$ , то  $w < v$ . При этом случай  $w = v$  исключается сразу, так как отсюда следовало бы, что 1)  $u = 1$ , что невозможно, или 2)  $u = v^2$ , или 3)  $u = v^{-2}$ . Если элемент  $v$  — трансформа, то его квадрат или равен единице, или есть опять трансформа; если же  $v$  — не трансформа, то  $l(v^2) > l(v)$ . В обоих случаях равенства  $u = v^2$ ,  $u = v^{-2}$  невозможны.

Так как любые два из элементов  $u$ ,  $v$ ,  $w$  порождают третий, этим третьим должен быть элемент  $w$ , если  $v \in K$ . Поэтому нам нужно только рассмотреть случай, когда элемент  $v = aax^{-1} \in aBa^{-1}$  — трансформа. Так как  $u \notin aBa^{-1}$  и  $u < v$ , мы имеем также отношение  $u < v^*$ , где  $v^*$  — любая трансформа из группы  $aBa^{-1}$ . Поэтому если в произведении  $u$  и  $v = aax^{-1}$  сокращение распространяется только на  $a$  (или на  $a^{-1}$ ), то то же самое происходит при перемножении  $u$  и некоторого элемента  $v^* = aa^*\alpha^{-1} \in K$ , результатом которого является произведение  $w^* = u^*v^*$  или  $v^*u^*$ , где  $w^* < v^*$ . Последнее же отношение противоречит тому, что  $v^* \in K$ . Поэтому сокращению между  $u$  и  $v = aax^{-1}$  подлежит  $a$  целиком, и, кроме того, центральный член  $a$  или сокращается, или объединяется. Таким образом,  $u^* = aa''\alpha^{-1}$ , где элемент  $a''$  объединяется или сокращается с  $a$ . Так как  $u < v = aax^{-1}$ , имеем  $l(\sigma) < l(a)$  или же  $l(\sigma) = l(a)$  и  $u = \sigma a''^{-1}\alpha^{-1}$ ,  $\sigma < a$ . В обоих случаях элементы  $u$  и  $\sigma(a''^{-1}a^*\alpha'')\sigma^{-1}$  предшествуют элементу  $v^* = aa^*\alpha^{-1} \in K$  и порождают его. Тем самым получено противоречие. Таким образом, во всех случаях мы приходим к противоречию, предположив, что  $w < v$ . Поэтому элемент  $w$  следует за  $u$  и  $v$ .

Как следствие того факта, что все восемь произведений  $u^e v^\eta$  и  $v^\eta u^e$  следуют за  $u$  и  $v$ , получаем ограничения на сокращения и объединения, перечисленные в теореме. Эти ограничения явно говорят о том, что сокращается не более половины каждого из слов  $u$  и  $v$  и что в тех случаях, когда сокращение и объединение заменяют начальный (или конечный) отрезок другим отрезком той же длины, результатом является более поздний элемент при введенном порядке.

\* ) Действительно, если бы для некоторого  $a^* \in B$   $a^*a^1 < a^1$  в лексикографическом порядке, то для  $u^* = \sigma a^*\alpha^{-1} \in T$  имели бы  $w^* = u^* \cdot v^\eta = aa^*\alpha^{-1}aa^1\sigma = aa^*a^1\sigma < aa^1\sigma = v^\eta$ , что противоречит утверждению леммы. — Прим. ред.

Лемма 17.3.3. Для произведения  $u_1 u_2 \dots u_t$ , где  $u_i \in T \cup T^{-1}$  ( $i = 1, \dots, t$ ),  $u_i u_{i+1} \neq 1$  ( $i = 1, \dots, t-1$ ) и соседние элементы  $u_i$  и  $u_{i+1}$  не содержатся в одной группе  $\alpha B \alpha^{-1}$  ( $B \subseteq A_v$ ), приведенная запись имеет следующие окончания:

- 1)  $\beta^{-1}$ , если  $u_t = \alpha \beta^{-1}$ ,
- 2)  $b^* \alpha^{-1}$ , если  $u_t = (\alpha \beta^{-1})^{-1}$ ,
- 3)  $a^* \beta^{-1}$ , если  $u_t = \alpha a \beta^{-1}$ ,  $\alpha < \beta$ ,
- 4)  $a^{-1} \alpha^{-1}$ , если  $u_t = (\alpha a \beta^{-1})^{-1}$ ,  $\alpha < \beta$ ,
- 5)  $a^* \alpha^{-1}$ , если  $u_t = \alpha a \alpha^{-1}$ .

Здесь  $b^*$  в случае 2) и  $a^*$  в случае 5)—или буквы, непосредственно предшествующие в произведении  $u_t$ , или объединения с аналогичными буквами произведения  $u_{t-1}$ ; элемент  $a^*$  в случае 3) может объединять сомножители  $u_{t-1}$  и  $u_{t-2}$ .

Доказательство этой леммы проведем индукцией по  $t$ . При  $t=1$  лемма очевидна. При  $t=2$  результаты вытекают непосредственно из леммы 17.3.2, если дополнительно учесть, что в выражении  $u = \alpha \beta^{-1}$  или  $\alpha a \beta^{-1}$  сокращение  $u^2$  не может полностью сократить  $\alpha$  или  $\beta$ . При переходе от  $t$  к  $t+1$  мы только применяем лемму 17.3.2 к каждому из пяти случаев нашей леммы и к каждой из пяти возможностей для  $u_{t+1}$ , используя при этом только одно дополнительное свойство, не являющееся прямым следствием леммы 17.3.2. Это свойство состоит в следующем. Может случиться, что  $u_t = \alpha a \alpha^{-1}$ ,  $\alpha$  сокращается и  $a$  объединяется с  $u_{t-1} = \sigma a'^{-1} \alpha^{-1}$  и аналогично с  $u_{t+1} = \alpha a'' \lambda$ . Тогда по лемме 17.3.2  $a'$  и  $a''$  являются первыми элементами в своем смежном классе  $Ba'$  и  $Ba''$  соответственно. Если бы  $a'^{-1} a a'' = 1$ , то это означало бы, что элементы  $a'$  и  $a''$  принадлежат одному смежному классу, т. е. означало бы, что  $a' = a''$ ,  $a = 1$ ,  $u_t = 1$ , что невозможно. Поэтому  $a'^{-1} a a'' \neq 1$ , приведенная запись произведения  $u_{t-1} u_t u_{t+1}$  имеет вид  $\sigma(a'^{-1} a a'') \lambda$ . Это единственный случай, когда объединение может включать три последовательных члена из полу-приведенного произведения  $u_1 u_2 \dots u_m$ .

Установив возможные окончания приведенного представления для полуприведенных произведений  $h = u_1 u_2 \dots u_t$ , мы установили тем более, что  $h \neq 1$ , т. е. что  $H$  есть свободное произведение бесконечных циклических групп, порожденных элементами  $\alpha \beta^{-1}$  и  $\alpha a^{-1} \beta^{-1}$  ( $\alpha < \beta$ ), и подгрупп  $\alpha B \alpha^{-1}$ , сопряженных с подгруппами  $B$  свободных сомножителей  $A_v$ -группы  $G$ .

## Г л а в а 18

### ПРОБЛЕМА БЕРНСАЙДА

#### 18.1. Постановка проблемы

В 1902 году Бернсайд [1] писал: „Еще не решенным вопросом теории дискретных групп является вопрос о том, может ли быть порядок группы бесконечным, в то время как порядок любого ее элемента конечен“. Он имел в виду, разумеется, группы с конечным числом образующих. Этот вопрос остается нерешенным и в настоящее время<sup>1)</sup>. Бернсайд рассматривал этот вопрос при некоторых ограничениях, а именно он предполагал, что данная группа обладает конечным числом образующих и что порядки ее элементов ограничены в совокупности.

Если группа  $G$  порождается  $r$  элементами и  $n$  — наименьшее общее кратное порядков ее элементов, то проблема ставится так: является ли группа  $G$  конечной? Эта проблема известна как проблема Бернсайда. Если  $x_1, \dots, x_r$  — образующие элементы группы  $B(n, r)$  с отношениями  $g^n = 1$  для любого элемента  $g \in B(n, r)$ , то эта группа называется *группой Бернсайда порядка  $n$  с  $r$  образующими*<sup>2)</sup>. Очевидно, что любая группа с  $r$  образующими и элементами, порядки которых делят  $n$ , является гомоморфным образом группы  $B(n, r)$ . Таким образом, проблема Бернсайда сводится к вопросу: какие из групп  $B(n, r)$  конечны?

Если  $F_r$  — свободная группа, порожденная элементами  $x_1, \dots, x_r$ , и  $N$  — ее вполне характеристическая подгруппа, порожденная всеми элементами вида  $z^n$ ,  $z \in F_r$ , то  $B(n, r) = F_r/N$ .

#### 18.2. Проблема Бернсайда для $n = 2$ и $n = 3$

Если каждый элемент группы  $G$ , кроме единицы, имеет порядок 2, то из равенств  $x^2 = 1$ ,  $y^2 = 1$ ,  $(xy)^2 = 1$  получаем, что  $xyx = 1$ ,  $xy = y^{-1}x^{-1} = yx$ , т. е.  $G$  — абелева группа. Таким образом, группа Бернсайда  $B(2, r)$ , порожденная элементами  $x_1, \dots, x_r$ , является абелевой группой порядка  $2^r$  с базисом  $x_1, \dots, x_r$ . Тем самым вопрос решен для  $n = 2$ .

<sup>1)</sup> П. С. Новиковым получено в 1959 г. отрицательное решение проблемы Бернсайда. — *Прим. ред.*

<sup>2)</sup> П. С. Новиковым было доказано, что для  $n \geqslant 72$  существует бесконечная группа с конечным числом образующих, порядок каждого элемента которой является делителем  $n$ . — *Прим. ред.*

Если  $n = 3$ , легко показать, что группа  $B(3, r)$  конечна. Докажем это индукцией по  $r$ . Группа  $B(3, 1)$  циклическая порядка 3. Предположим, что порядок группы  $B_h = B(3, h)$  равен  $3^{m(h)}$ . Воспользуемся соотношением

$$yxy = x^{-1}y^{-1}x^{-1}, \quad (18.2.1)$$

которое получается из равенства  $(xy)^3 = 1$ . Группа  $B_{h+1}$  получается присоединением нового образующего элемента  $z$  к группе  $B_h$ . Поэтому элементы группы  $B_{h+1}$  имеют вид

$$g = u_1 z^{\pm 1} u_2 z^{\pm 1} \dots z^{\pm 1} u_n, \quad (18.2.2)$$

где  $u_i \in B_h$ . Покажем, что элемент  $g$  можно представить как произведение, в которое элемент  $z$  входит не более двух раз. Если в произведении (18.2.2) два последовательных вхождения элемента  $z$  имеют одинаковые показатели степени, то, применяя соотношение (18.2.1), получаем  $zu_i z = u_i^{-1} z^{-1} u_i^{-1}$  или  $z^{-1} u_j z^{-1} = u_j^{-1} z u_j^{-1}$ ; таким образом, число вхождений элемента  $z$  уменьшено на единицу. Итак, элемент  $g$  может быть представлен в виде (18.2.2), где показатели элемента  $z$ , равные  $+1$  и  $-1$ , чередуются. Если теперь представление элемента  $g$  имеет три вхождения элемента  $z$ , то преобразуем его следующим образом:

$$\begin{aligned} g = u_1 z u_2 \cdot z^{-1} u_3 \cdot z \dots &= u_1 z u_2 z \cdot z u_3 z \dots = \\ &= u_1 u_2^{-1} \cdot z^{-1} u_2^{-1} u_3^{-1} z^{-1} u_3^{-1} \dots, \end{aligned}$$

сокращая число вхождений  $z$  на единицу. Если  $g = u_1 z^{-1} u_2 z u_3 z^{-1}$ , поступаем аналогичным образом. Итак, элемент  $g$  можно представить как произведение только с двумя вхождениями образующего  $z$ . При этом  $u_1 z^{-1} u_2 z u_3 = u_1 z^{-1} u_2 z^{-1} z^{-1} u_3 = u_1 u_2^{-1} z u_2^{-1} z^{-1} u_3$ . Таким образом, любой элемент группы  $B_{h+1}$  может быть представлен одним из следующих выражений:

$$\begin{aligned} &u_1, \\ &u_1 z u_2, \\ &u_1 z^{-1} u_2, \\ &u_1 z u_2 z^{-1} u_3. \end{aligned} \quad (18.2.3)$$

Следовательно, группа  $B_{h+1}$  состоит самое большое из  $3^m + 2 \cdot 3^{2m} + 3^{3m} < 3^{3m+1}$  элементов; поэтому  $m(h+1) \leq 3m(h)$ , откуда  $m(r) \leq 3^{r-1}$ , т. е. группа  $B(3, r)$  имеет порядок не больше  $3^{3^{r-1}}$ . В своей первой работе Бернсайд, используя более сложные методы, получил более точную оценку  $m(r) \leq 2^r - 1$ . Мы докажем сейчас точное равенство  $m(r) = \binom{r}{3} + \binom{r}{2} + r$ , полученное Леви и Ван дер Варденом [1].

Применяя трижды равенство (18.2.1) к выражению  $x^{-1}yxzx^{-1}$  получаем формулу

$$\begin{aligned} x^{-1}yxzx^{-1} &= (x^{-1}yx^{-1})(x^{-1}zx^{-1}) = \\ &= y^{-1}(xy^{-1}z^{-1}x)z^{-1} = y^{-1}zyx^{-1}zyz^{-1}. \end{aligned} \quad (18.2.4)$$

Как частный случай формулы (18.2.4) при  $z = y$  получаем, что

$$x^{-1}yxux^{-1} = yx^{-1}y,$$

откуда

$$(x^{-1}yx)y = y(x^{-1}yx). \quad (18.2.5)$$

Таким образом, любой элемент  $y$  перестановочен с любым своим сопряженным элементом  $x^{-1}yx$ . Следовательно, элемент  $y$  перестановочен с коммутатором  $y^{-1}x^{-1}yx$ , откуда в обозначениях коммутаторов получаем

$$(y, x, y) = 1. \quad (18.2.6)$$

Отсюда же получаем

$$(x, y)^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}yx = x^{-1}yxy^{-1} = (x, y^{-1}). \quad (18.2.7)$$

Теперь мы имеем

$$\begin{aligned} (x^{-1}, y) &= (y, x^{-1})^{-1} = (y, x) = (x, y)^{-1}, \\ (y, x, x) &= ((x, y)^{-1}, x) = (x, y, x)^{-1} = 1. \end{aligned} \quad (18.2.8)$$

Рассмотрим теперь элемент  $(a, c, b)^{-1} = b^{-1}(c^{-1}a^{-1}cabab^{-1}c^{-1})ac$  и применим формулу (18.2.4) к произведению в скобках, полагая  $x = c$ ,  $y = a^{-1}$ ,  $z = abab^{-1}$ :

$$\begin{aligned} (a, c, b)^{-1} &= b^{-1}(a \cdot abab^{-1}a^{-1}c^{-1}abab^{-1}a^{-1}ab^{-1}a^{-1})ac = \\ &= b^{-1}a^{-1}bac^{-1}aba^{-1}b^{-1}c = (a, b, c). \end{aligned}$$

Кроме этого, мы знаем, что  $(a, c, b)^{-1} = ((a, c)^{-1}, b) = (c, a, b)$ . Таким образом,

$$\begin{aligned} (a, b, c) &= (c, a, b) = (b, c, a), \\ (a, c, b)^{-1} &= (a, b, c). \end{aligned} \quad (18.2.9)$$

Теперь мы можем показать, что любой коммутатор веса четыре равен единице. Для этого рассмотрим сначала сложный коммутатор  $(a, b; c, d)$ ; используя тождества (18.2.9), получаем

$$\begin{aligned} (a, b; (c, d)) &= ((c, d), a, b) = ((c, d, a), b) = (a, c, d, b) = \\ &= (a, c, b, d)^{-1} = ((a, b, c)^{-1}, d)^{-1} = (a, b, c, d). \end{aligned}$$

Но, кроме этого,  $(c, d; a, b) = ((a, b), c, d) = (a, b, c, d)$ . Поэтому  $(a, b; c, d) = (c, d; a, b) = (a, b; c, d)^{-1}$ , откуда

$$(a, b; c, d) = (a, b, c, d) = 1. \quad (18.2.10)$$

Как видно из предыдущих соотношений, коммутатор веса три равен единице, если в нем два элемента совпадают. При трех различных образующих элементах в силу тождеств (18.2.9) коммутатор веса три можно представить в виде  $(x_i, x_j, x_k)$ , где  $i < j < k$ , или как обратный элемент для этого элемента. Согласно равенству (18.2.10), коммутаторы веса три содержатся в центре, и коммутант абелев. Следовательно, любой элемент группы  $B(3, r)$  представим в виде

$$g = x_1^{a_1} \dots x_r^{a_r} (x_1, x_2)^{b_{12}} \dots (x_i x_j)^{b_{ij}} \dots (x_i, x_j, x_k)^{c_{ijk}}, \quad (18.2.11)$$

где  $i < j$  для коммутатора  $(x_i, x_j)$ ,  $i < j < k$  для  $(x_i, x_j, x_k)$ , а показатели степени равны 0, 1 или 2. Общее число таких выражений равно  $3^{m(r)}$ , где  $m(r) = r + \binom{r}{2} + \binom{r}{3}$  — число сочетаний из  $r$  образующих  $x_1, x_2, \dots, x_r$  по 1, по 2 и по 3 элемента. Поэтому порядок группы Бернсайда  $B(3, r)$  не превосходит  $3^{m(r)}$ ; этот порядок равен точно  $3^{m(r)}$ , если только элементы вида (18.2.11) с некоторыми показателями степени, не равными нулю, не равны единице. Действительно, если два различных выражения  $g_1$  и  $g_2$  представляют один и тот же элемент группы  $B(3, r)$ , то они представляют один и тот же элемент также и в любом гомоморфном образе группы  $B(3, r)$  и, в частности, в элементарной абелевой группе порядка  $3^r$ , откуда следует, что показатели степени  $a_i$ ,  $i = 1, \dots, r$ , должны совпадать. Так как коммутант абелев, элемент  $g = g_1 g_2^{-1} = 1$  с некоторыми показателями степени  $b_{ij}$  или  $c_{ijk}$ , отличными от нуля по модулю 3, представлял бы единицу, если бы различные выражения  $g_1$  и  $g_2$  представляли один и тот же элемент. Рассматривая равенство  $g = 1$  как соотношение в группе  $B(3, r)$ , находим, что оно остается верным, если добавить еще соотношения  $x_s = 1$ ,  $s \neq i, j, k$ . Поэтому чтобы показать, что порядок группы  $B(3, r)$  равен  $3^{m(r)}$ , достаточно установить, что порядок группы  $B(3, 3)$  равен  $3^7$ .

Для построения группы  $B(3, 3)$  как группы порядка  $3^7$  применим полуправильное произведение, рассмотренное в теоремах 6.5.1 и 6.5.2. Пусть

$$\begin{aligned} C_1 &= x, & C_2 &= y, & C_3 &= z, & C_4 &= (x, y), \\ C_5 &= (x, z), & C_6 &= (y, z), & C_7 &= (x, y, z). \end{aligned} \quad (18.2.12)$$

Сначала строим элементарную абелеву группу  $A = \{C_4, C_5, C_6, C_7\}$ , порядок которой равен  $3^4$ . Затем присоединяем к ней элемент  $C_3$ , при помощи соотношений

$$\begin{aligned} C_3^3 &= 1, \quad C_3^{-1}C_4C_3 = C_4C_7, \quad C_3^{-1}C_5C_3 = C_5, \\ C_3^{-1}C_6C_3 &= C_6, \quad C_3^{-1}C_7C_3 = C_7. \end{aligned} \quad (18.2.13)$$

Согласно теоремам 6.5.1 и 6.5.2, группа  $B = \{A, C_3\}$  имеет порядок  $3^5$  и является расширением группы  $A$  при помощи циклической группы  $\{C_3\}$ . Чтобы этот вывод обосновать, нужно только проверить, что при соотношениях (18.2.13) трансформирование элементом  $C_3$  индуцирует автоморфизм порядка 3 группы  $A$ . Далее, аналогичным способом расширяем группу  $B$  элементом  $C_2$  до группы  $H = \{B, C_2\}$  порядка  $3^6$ , используя при этом соотношения

$$\begin{aligned} C_2^3 &= 1, \quad C_2^{-1}C_3C_2 = C_3C_2^{-1}, \quad C_2^{-1}C_4C_2 = C_4, \\ C_2^{-1}C_5C_2 &= C_5C_2^{-1}, \quad C_2^{-1}C_6C_2 = C_6, \quad C_2^{-1}C_7C_2 = C_7. \end{aligned} \quad (18.2.14)$$

Наконец, расширяем группу  $H$  элементом  $C_1$  до группы  $G = \{C_1, H\}$  порядка  $3^7$  при помощи соотношений

$$\begin{aligned} C_1^3 &= 1, \quad C_1^{-1}C_2C_1 = C_2C_4^{-1}, \quad C_1^{-1}C_3C_1 = C_3C_5^{-1}, \\ C_1^{-1}C_4C_1 &= C_4, \quad C_1^{-1}C_5C_1 = C_5, \quad C_1^{-1}C_6C_1 = C_6C_7, \\ C_1^{-1}C_7C_1 &= C_7. \end{aligned} \quad (18.2.15)$$

При таких соотношениях класс nilпотентности группы  $G$  равен 3 и имеет место формула

$$(PQ)^3 = P^3(Q, P)^3(Q, P, P)(Q, P, Q)^5. \quad (18.2.16)$$

Полагая  $P = z$  и считая  $Q$  произвольным элементом из группы  $A$ , получаем, что показатель <sup>1)</sup> группы  $B$  равен 3. Это же утверждение можно доказать для группы  $H$ , а затем для  $G$ . Таким образом, группа  $G = B(3, 3)$  имеет порядок  $3^7$ . Как мы уже отмечали, отсюда следует общее утверждение теоремы.

**Теорема 18.2.1.** Порядок группы Бернсайда  $B(3, r)$  равен  $3^{m(r)}$ , где  $m(r) = r + \binom{r}{2} + \binom{r}{3}$ . Элемент группы  $B(3, r)$  однозначно представим в виде (18.2.11).

### 18.3. Конечность группы $B(4, r)$

В своей статье Бернсайд показал, что порядок группы  $B(4, 2)$  не больше  $2^{12}$ . Санову [1] удалось доказать, что группа  $B(4, r)$

<sup>1)</sup> То есть наименьшее общее кратное порядков всех элементов группы  $B$ . — Прим. перев.

конечна при любом  $r$ . Порядок ее точно не известен, однако установлено, что порядок группы  $B(4, 2)$  равен точно  $2^{12}$ .

**Теорема 18.3.1.** *Группы  $B(4, r)$  конечны.*

**Доказательство.** Пусть  $H$  — произвольная конечная группа, порядки элементов которой делят число 4. Мы хотим показать, что, присоединяя к  $H$  некоторый элемент четвертой степени  $b$  и потребовав, чтобы четвертые степени элементов расширенной группы  $G = H \cup \{b\}$  были равны 1, мы получим вновь конечную группу  $G$ . Осуществим присоединение такого элемента  $b$  к группе  $H$  в два этапа: сначала, присоединив элемент  $b^2$  к группе  $H$ , получим группу  $H_1 = H \cup \{b^2\}$ , а затем, присоединив элемент  $b$  к группе  $H_1$ , получим группу  $G = H_1 \cup \{b\} = H \cup \{b\}$ . Каждое из этих двух расширений таково, что мы присоединяем элемент, квадрат которого принадлежит расширяемой группе. Поэтому достаточно показать, что, присоединяя к конечной группе  $H$  элемент  $x$ , такой, что  $x^2 \in H$ , и полагая  $z^4 = 1$  для  $z \in H \cup \{x\}$ , мы получаем конечную группу  $H \cup \{x\}$ .

Любой элемент  $g$  группы  $H \cup \{x\}$ , где  $x^2 \in H$ , имеет вид

$$g = h_1 x h_2 x h_3 x \dots h_{n-1} x h_n, \quad h_i \in H. \quad (18.3.1)$$

Из соотношения  $(xh)^4 = 1$  мы получаем

$$xhx = h^{-1} x^{-1} h^{-1} x^{-1} h^{-1} = h^{-1} x (x^2 h^{-1} x^2) x h^{-1} = h^{-1} x h^* x h^{-1}, \quad (18.3.2)$$

где  $h^* \in H$ . Таким образом, не увеличивая длины  $n$  слова (18.3.1), мы можем при помощи соотношения (18.3.2) придать ему следующую форму:

$$h_1 x h_2 \dots x h_{i-1} h_i^{-1} x h_i^* x h_i^{-1} h_{i+1} x \dots x h_n. \quad (18.3.3)$$

Если в слове (18.3.1) некоторый элемент  $h_j$  равен единице при  $2 \leq j \leq n-1$ , то мы можем уменьшить длину слова, полагая  $x^2 = h \in H$ . Можно также использовать несколько раз равенство (18.3.2), чтобы заменить несколько элементов  $h_j$  единицей.

Санов заметил, что, последовательно применяя соотношение (18.3.2), можно  $h_{i-1}$  заменить произведением  $h_{i-1} h_i^{-1}$ , затем  $h_{i-2}$  — произведением  $h_{i-2} (h_{i-1} h_i^{-1})^{-1} = h_{i-2} h_i h_{i-1}^{-1}$  и т. д. Таким способом можно заменить элемент  $h_2$  любым из элементов  $h_2, h_2 h_3^{-1}, h_2 h_4 h_3^{-1}, h_2 h_4 h_5^{-1} h_3^{-1}, \dots, h_2 h_4 \dots h_{2s} h_{2s-1}^{-1} \dots h_3^{-1}, h_2 h_4 \dots h_{2s} h_{2s+1}^{-1} \dots h_3^{-1}$ . Если хоть один из этих элементов равен единице, можно уменьшить длину слова  $g$ . Если же порядок группы  $H$  равен  $M$  и  $n \geq M + 2$ , то или одно из этих выражений

равно единице, или среди них есть равные, скажем,  $h_2 \dots h_{2r} h_{2r+1}^{-1} \dots h_3^{-1} = h_2 \dots h_{2r} \dots h_{2s} h_{2s+1}^{-1} \dots h_{2r+1}^{-1} \dots h_3^{-1}$ , откуда  $h_{2r+2} \dots h_{2s} h_{2s+1} h_{2r+3}^{-1} = 1$ . Но это не что иное, как одно из произведений, которым можно заменить элемент  $h_{2r+2}$ . Аналогично если повторяется произведение  $h_2 h_4 \dots h_{2r} h_{2r-1}^{-1} \dots h_3^{-1}$ , то элемент  $h_{2r+1}$  можно заменить произведением, равным единице. Во всех случаях, если  $n \geq M + 2$ , мы можем уменьшить длину слова  $g$ . Следовательно, любой элемент  $g$  можно представить словом длины  $n \leq M + 1$ . Поэтому порядок группы  $H \cup \{x\}$  равен самое большее  $M^{M+1}$ .

#### 18.4. Ослабленная проблема Бернсайда. Теоремы Ф. Холла и Г. Хигмэна. Конечность группы $B(6, r)$

Более слабой формой проблемы Бернсайда является следующее утверждение; доказательство этого утверждения известно в литературе как ослабленная проблема Бернсайда.

$R_n$ : Для любого натурального числа  $r$  существует такое целое число  $b_{n, r}$ , что любая конечная группа показателя  $n$ , порожденная  $r$  элементами, имеет порядок не больше  $b_{n, r}$ .

Если для некоторого  $n$  утверждение  $R_n$  справедливо, то этим не исключается возможность существования бесконечной группы показателя  $n$  с  $r$  образующими. Но если утверждение  $R_n$  верно, то существует наибольшая конечная группа  $R(n, r)$  показателя  $n$  с  $r$  образующими. Действительно, каждая конечная группа показателя  $n$ , порожденная  $r$  элементами, изоморфна фактор-группе  $F_r/N_i$ , где  $F_r$  — свободная группа с  $r$  образующими, а  $N_i$  — некоторая инвариантная подгруппа, содержащая все элементы, являющиеся  $n$ -ми степенями элементов группы  $F_r$ . Если утверждение  $R_n$  истинно, то существует только конечное число таких инвариантных подгрупп  $N_i$ , а их пересечение  $N$  есть инвариантная подгруппа конечного индекса, причем фактор-группа  $F_r/N = R(n, r)$  является конечной группой показателя  $n$ , обладающей  $r$  образующими и такой, что все другие группы являются ее гомоморфными образами.

Пусть  $G$  — группа с нижним центральным рядом

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots \quad (18.4.1)$$

Предположим, что  $G_s = G_{s+1}$ . Тогда в силу свойств нижних центральных рядов  $G_s = G_{s+1} = \dots = G_{s+i} = \dots$ . Если группа  $G$  нильпотента, то  $G_{s+i} = 1$ , откуда  $G_s = 1$ . Так как конечная группа  $G$  показателя  $n = p^t$ , где  $p$  — простое число, нильпотента, то для нее из равенства  $G_s = G_{s+1}$  следует, что  $G_s = 1$ . Предположим теперь, что показатель группы  $G$  равен  $p^t$  и  $G$  порождается  $r$  элементами. Тогда каждая фактор-группа  $G_i/G_{i+1}$  является

конечной абелевой группой. Если мы сумеем показать, что для любой такой группы  $G$  существует такое число  $s = s(p^t, r)$ , что  $G_s = G_{s+1}$ , то ослабленная проблема Бернсайда будет решена для показателя  $n = p^t$ .

Применяя собирательный процесс (теорема 12.3.1) к элементу  $(xy)^n$ , мы установили, что

$$(xy)^n = x^n y^n c_1^{a_1(n)} \dots c_t^{a_t(n)}. \quad (18.4.2)$$

Здесь показатель степени  $a_i(n)$  равен

$$u_{i1}n + u_{i2}\binom{n}{2} + \dots + u_{im}\binom{n}{m}, \quad (18.4.3)$$

где  $m$  — вес коммутатора  $c_i$ .

Если коммутатор  $c_i$  имеет вид

$$c_i = \left( y, \overbrace{x, \dots, x}^s \right), \quad (18.4.4)$$

то показатель степени  $a_i(n)$  равен числу таких множеств индексов  $j_1, j_2, \dots, j_{s+1}$  коммутатора

$$(y_{j_1}, x_{j_2}, x_{j_3}, \dots, x_{j_{s+1}}), \quad (18.4.5)$$

что

$$j_1 < j_2 < j_3 < \dots < j_{s+1}, \quad 1 \leq j_k \leq n. \quad (18.4.6)$$

Это число возможных выборов  $s+1$  различных чисел из последовательности 1, 2, ...,  $n$  равно  $\binom{n}{s+1}$ .

Если число  $n = p$  простое, то показатели степени коммутаторов, веса которых не превосходят  $p-1$ , все кратны  $p$ , так как биномиальные коэффициенты  $\binom{p}{i}$  при  $1 \leq i \leq p-1$  кратны  $p$ . Но для коммутатора

$$\left( y, \overbrace{x, \dots, x}^{p-1} \right) \quad (18.4.7)$$

показатель степени  $\binom{p}{p} = 1$ . Поэтому в группе  $G$  показателя  $p$  мы имеем

$$1 = (xy)^p = \left( y, \overbrace{x, x, \dots, x}^{p-1} \right) v_1 \dots v_t, \quad (18.4.8)$$

где  $v_1, v_2, \dots, v_t$  — коммутаторы, веса которых не меньше  $p$ , а в коммутаторах веса  $p$  элемент  $y$  участвует не менее двух раз.

Отсюда получаем следующие отношения в группе  $G_p$  по модулю  $G_{p+1}$ :

$$\left( y, \overbrace{x, \dots, x}^{p-1} \right) v_1 \dots v_s \equiv 1 \pmod{G_{p+1}}; \quad (18.4.9)$$

здесь  $v_1, \dots, v_s$  — коммутаторы веса  $p$  от  $x$  и  $y$ , причем вес в  $x$  не меньше 1 и не больше, чем  $p - 1$ . Из формул (10.2.1) мы получаем, что в любой группе

$$(u^i, v^j) \equiv (u, v)^{ij} \pmod{G_{p+1}}, \quad (18.4.10)$$

если вес коммутатора  $(u, v)$  равен  $m$ . Пользуясь этим сравнением, мы находим, что если в некотором коммутаторе  $v_j$  из произведения (18.4.9) вес в  $x$  точно равен  $r$ , то замена элемента  $x$  его степенью  $x^i$  ведет к замене коммутатора  $v_j$  его степенью  $v_j^{i^r}$ . Полагая здесь поочередно  $i = 1, 2, \dots, p - 1$  и перемножая эти соответствия, мы получаем соотношение

$$1^r + 2^r + 3^r + \dots + (p-1)^r \equiv 0 \pmod{p} \quad (18.4.11)$$

для показателя степени коммутатора  $v_j$ , где  $1 \leq r \leq p - 2$ . Для главного же члена  $\left( y, \overbrace{x, \dots, x}^{p-1} \right)$  имеем  $r = p - 1$  и  $t^r \equiv 1 \pmod{p}$ . Поэтому соответствующее произведение принимает вид

$$\left( y, \overbrace{x, \dots, x}^{p-1} \right)^{p-1} \equiv 1 \pmod{G_{p+1}}, \quad (18.4.12)$$

откуда

$$\left( y, \overbrace{x, \dots, x}^{p-1} \right) \equiv 1 \pmod{G_{p+1}}. \quad (18.4.13)$$

Последнее соотношение было основным при исследовании ослабленной проблемы Бернсайда для групп с показателем  $p$ , где  $p$  — простое число. Исходя из этого соотношения, Кострикин [1] решил ослабленную проблему Бернсайда для группы показателя 5 с двумя образующими. Он же показал, что  $G_{13} = G_{14}$  и что группа  $G$ , если она конечна, имеет порядок не больше  $5^{34}$ .

Ослабленная проблема Бернсайда изучалась рядом авторов, при этом часто оказывалось удобным рассматривать сопоставленное группе лиево кольцо, которое мы сейчас рассмотрим.

В ассоциативном кольце  $R$  определим лиево произведение  $[x, y]$ , полагая

$$[x, y] = xy - yx. \quad (18.4.14)$$

Тогда относительно сложения в кольце  $R$  и лиева произведения элементы кольца  $R$  образуют лиево кольцо  $L$ . Лиево кольцо удовлетворяет следующим аксиомам:

L0. Сложение  $x+y$  и лиево произведение  $[x, y]$  — вполне определенные операции.

L1. Относительно сложения  $L$  — абелева группа с нулевым элементом 0.

$$L2. [x+y, z] = [x, z] + [y, z],$$

$$[x, y+z] = [x, y] + [x, z].$$

$$L3. [x, x] = 0.$$

$$L4. [[x, y], z] + [[y, z], x] + [[z, x], y] = 0.$$

Легко проверить, что произведение  $[x, y]$ , определенное равенством (18.4.14), удовлетворяет этим требованиям.

Из соотношений L2 и L3 получается, что

$$0 = [x+y, x+y] = [x, x] + [x, y] + [y, x] + \\ + [y, y] = [x, y] + [y, x], \quad (18.4.15)$$

откуда

$$[y, x] = -[x, y]. \quad (18.4.16)$$

Если кольцо  $R$  порождается элементами  $x_1, \dots, x_r$ , то элементами, полученными из  $x_1, \dots, x_r$  путем сложения, и лиевыми произведениями  $[x, y]$  не исчерпывается все ассоциативное кольцо  $R$ . Элементы, порождаемые лиевыми произведениями, называются *лиевыми элементами*. Так,  $x_1^2$  — не лиев элемент, а  $x_1^2x_2 - 2x_1x_2x_1 + x_2x_1^2 = x_1(x_1x_2 - x_2x_1) - (x_1x_2 - x_2x_1)x_1$  — лиев элемент. В силу соотношений в кольце  $R$  может, конечно, случиться, что элемент  $x_1^2$  равен некоторому лиеву элементу.

Мы можем взять законы L0, L1, L2, L3, L4 в качестве определения лиева кольца  $L$ . Г. Биркгоф [1] и Е. Витт [1] показали, что всякое лиево кольцо  $L$  может быть представлено как кольцо элементов Ли соответствующим образом подобранного ассоциативного кольца  $R$ . Этот важный результат, однако, здесь нам не понадобится.

Пусть

$$G = G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots \supseteq G_n \supseteq \dots \quad (18.4.17)$$

— нижний центральный ряд группы  $G$ . *Лиево кольцо  $L$ , сопоставленное группе  $G$* , строится следующим образом:

1)  $L$  есть декартова сумма аддитивно записанных фактор-групп  $G_i/G_{i+1}$ , и сложение в этой декартовой сумме определяет сложение в  $L$ ;

2) элементы фактор-группы  $G_i/G_{i+1}$  считаются однородными степени  $i$ ;

3) лиево произведение однородного элемента  $A$  степени  $i$  и однородного элемента  $B$  степени  $j$  — это групповой коммутатор  $(A, B)$ , взятый по модулю  $G_{i+j+1}$ ;

4) лиево произведение произвольных элементов из  $L$  определяется предыдущим правилом и дистрибутивным законом.

Мы не будем здесь доказывать, что эти правила действительно определяют лиево кольцо. Заметим только, что закон L2 соответствует тождествам (10.2.1.2) и (10.2.1.3) для коммутаторов, а закон L4 соответствует тождеству (10.2.1.5). Можно переформулировать результаты из § 11.2, чтобы показать, что кольцо Ли, соответствующее свободной группе с  $r$  образующими, является свободным кольцом Ли с  $r$  образующими, если в нем рассматривать только конечные суммы. Для доказательства того, что эти правила определяют кольцо Ли, можно воспользоваться несколько видоизмененными методами из § 11.2.

В кольце Ли  $L$  для упрощения записи будем обозначать произведение  $[x_1, x_2]$  через  $x_1, x_2$ , а произведение  $[x_1, \dots, x_{n-1}, x_n]$  через  $x_1 \dots x_{n-1} x_n$ . Следующая теорема принадлежит Грехэму Хигмэну [1].

**Теорема 18.4.1.** В ассоциированном кольце Ли группы показателя  $p$  ( $p$  — простое число) выполняется соотношение  $yx^{p-1} = 0$ .

**Доказательство.** Соотношение (18.4.13) справедливо в группе  $G$  показателя  $p$ . Его мы перепишем в виде

$$\left( y, \underbrace{x, \dots, x}_{p-1} \right) = c_1 c_2 \dots c_t, \quad (18.4.18)$$

где  $c_1, c_2, \dots, c_t$  — коммутаторы от  $x$  и  $y$ , веса которых не меньше  $p+1$ , и, конечно, веса  $\geqslant 1$  от  $y$ .

Пусть теперь  $x = x_1 x_2 \dots x_{p-1}$ . Применяя формулы (10.2.1), преобразуем равенство (18.4.18) так, чтобы слева оставались только коммутаторы с различными компонентами  $x_i$ . Тогда получим

$$X = \prod_{\sigma} \left( y, x_{1\sigma}, \dots, x_{(p-1)\sigma} \right) = d_1 d_2 \dots d_s, \quad (18.4.19)$$

где подстановка  $\sigma$  пробегает в некотором порядке все  $(p-1)!$  подстановок чисел  $1, 2, \dots, p-1$ , а  $d_1, d_2, \dots, d_s$  — коммутаторы положительного веса от  $y$ . Каждый из них или (1) общего веса не меньше  $p+1$  от элементов  $y, x_1, \dots, x_{p-1}$ , или (2) общего веса  $p$  от  $y, x_1, \dots, x_{p-1}$ , но некоторые  $x_j$  в нем не встречаются. Мы можем предположить теперь, что каждый коммутатор  $d_i$  имеет положительный вес относительно каждого из аргументов  $y, x_1, \dots, x_{p-1}$ . Это доказывается полной индукцией. Действительно, предположим, что это утверждение справедливо для любого коммутатора  $d_i$  и аргументов  $y, x_1, \dots, x_{j-1}, x_j$ . Вводя, если нужно, дальнейшие коммутаторы, мы, очевидно, можем предположить, что коммутаторы  $d_i$ , в которых не участвует аргумент  $x_j$ ,

составляют начальный отрезок  $d_1 \dots d_t$  произведения. Полагая  $x_j = 1$ , мы находим, что  $d_1 \dots d_t = 1$ , т. е. это произведение можно опустить. Поэтому мы можем считать, что  $d_i$  — коммутаторы положительных весов относительно каждого из аргументов  $y, x_1, \dots, x_{p-1}$  и общего веса  $p+1$ . Коммутаторы, имеющие вес  $p$  и не зависящие от некоторого  $x_j$ , которые, может быть, встречались в исходном произведении, были исключены на некотором этапе описанного процесса. Но это в терминах кольца Ли  $L$ , сопоставленного группе, означает, что если  $y, x_1, x_2, \dots, x_{p-1}$  — однородные элементы какого угодно веса, то мы имеем

$$\sum_{\sigma} yx_{1\sigma} x_{2\sigma} \dots x_{(p-1)\sigma} = 0. \quad (18.4.20)$$

Но (18.4.20) — тождество в кольце  $L$ , справедливое для однородных элементов  $y, x_1, \dots, x_p$ . Так как оно линейно относительно каждого аргумента, это тождество должно выполняться для любых аргументов. Поэтому при  $x_1 = x_2 = \dots = x_{p-1} = x$  и при произвольном  $y$  тождество (18.4.20) принимает вид

$$(p-1)! yx^{p-1} = 0, \quad (18.4.21)$$

а так как характеристика кольца  $L$  равна, очевидно,  $p$ , отсюда имеем

$$yx^{p-1} = 0, \quad (18.4.22)$$

что и требовалось доказать.

Используя соотношение  $yx^4 = 0$  в кольце Ли  $L$  характеристики 5 (точнее, характеристики, взаимно простой с 2 и 3), Г. Хигмэн [1] показал, что если кольцо  $L$  порождается  $r$  элементами, то в нем произведения, в которых сумма показателей степеней всех сомножителей не меньше  $Nr$ , равны нулю; здесь  $N$  — некоторое натуральное число, не зависящее от  $r$ . Нетрудно показать, что он доказал свое утверждение для  $N = 25$ , однако им выдвинута гипотеза, что с помощью дальнейших выкладок возможно доказать тот же результат для  $N = 9$ ; по всей вероятности, это еще не наилучший возможный результат.

В очень важной работе Ф. Холл и Г. Хигмэн [1] среди других вопросов рассмотрели связь ослабленной проблемы Бернсайда для любого показателя с той же проблемой для показателей, равных степени простого числа. При этом необходимо ограничиться конечными разрешимыми группами. Тогда предположение, более слабое, чем  $R_n$ , состоит в следующем:

$S_n$ : Для любого натурального числа  $r$  существует такое целое число  $b_{n,r}$ , что любая конечная разрешимая группа показателя  $n$ , порожденная  $r$  элементами, имеет порядок не больше  $b_{n,r}$ .

Сформулируем результат Холла и Хигмэна в виде теоремы.

**Теорема 18.4.2.** *Если  $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$  и если утверждения  $S_{p_i^{e_i}}$  истинны при  $i = 1, \dots, s$ , то утверждение  $S_n$  также истинно.*

Мы здесь не будем доказывать эту теорему, так как доказательство опирается на ряд громоздких и сложных вспомогательных результатов. Так как конечная группа порядка  $p^a q^b$  разрешима (теорема 16.8.7), утверждения  $R_n$  и  $S_n$  совпадают, когда  $n$  делится не больше чем на два простых числа. Но так как известно, что группы Бернсайда  $B(2, r)$ ,  $B(3, r)$  и  $B(4, r)$  конечны, а Г. Хигмэн установил, что утверждение  $R_5$  истинно, теорема 18.4.2 устанавливает истинность утверждений  $R_6, R_{12}, R_{10}, R_{15}, R_{20}$ , а также  $S_{30}$  и  $S_{60}$ . Воодушевленный этими результатами, автор показал, что группы  $B(6, r)$  конечны; набросок доказательства этого результата будет дан ниже.

Мы изложим сейчас лишь небольшую часть результатов Ф. Холла и Г. Хигмэна и укажем направления дальнейших результатов.

Назовем группу  $p'$ -группой, где  $p$  — простое число, если ее порядок не делится на  $p$ , и, как обычно,  $p$ -группой, если ее порядок равен степени числа  $p$ .

**Определение.** Конечная группа  $G$  называется  *$p$ -разрешимой*, если она обладает инвариантным рядом

$$1 = V_0 \subset V_1 \subset \dots \subset V_n = G, \quad (18.4.23)$$

в котором каждая фактор-группа  $V_{i+1}/V_i$  является либо  $p$ -группой, либо  $p'$ -группой.

Заметим, что, согласно теореме 9.2.4, конечная разрешимая группа  $G$   $p$ -разрешима при любом простом  $p$ . Определим для  $p$ -разрешимой группы  $G$  верхний  $p$ -ряд

$$1 = P_0 \subseteq N_0 \subset P_1 \subset N_1 \subset P_2 \subset \dots \subset P_l \subseteq N_l = G \quad (18.4.24)$$

рекуррентно: подгруппа  $N_k$  находится из условия, что  $N_k/P_k$  — наибольшая инвариантная  $p'$ -подгруппа группы  $G/P_k$ , а  $P_{k+1}$  — из условия, что  $P_{k+1}/N_k$  — наибольшая инвариантная  $p$ -подгруппа группы  $G/N_k$ . Наименьшее число  $l$ , такое, что  $N_l = G$ , назовем  $p$ -длиной группы  $G$ , обозначив ее  $l_p$  или  $l_p(G)$ . Легко видеть, что  $l_p$  есть наименьшее число  $p$ -фактор-групп в любых нормальных рядах группы  $G$  типа (18.4.23), в которых любой фактор  $V_{i+1}/V_i$  — либо  $p$ -группа, либо  $p'$ -группа.

Целью упомянутой выше работы Ф. Холла и Хигмэна является установление связи между  $p$ -длиной  $p$ -разрешимой группы  $G$  и свойствами силовских  $p$ -подгрупп  $S(p)$  группы  $G$ . Пусть, в частности,  $p^{ep}$  — показатель подгруппы  $S(p)$ , т. е. н.о.к. порядков

элементов группы  $S(p)$ . Тогда показателем группы  $G$ , т. е. наименьшим общим кратным  $n$  порядков элементов из  $G$ , является число  $n = \prod_p p^{e_p}$ . Основные теоремы Ф. Холла и Хигмэна справедливы для нечетных простых чисел  $p$ , причем эти результаты слегка отличаются для простых чисел Ферма вида  $p = 2^n + 1$  и для остальных простых чисел. Следующая теорема имеет отношение к проблеме Бернсайда. Из нее теорема 18.4.2 легко получается как частный случай.

**Теорема 18.4.3.** *Если  $G$  —  $p$ -разрешимая группа, где  $p$  — нечетное простое число, то*

- 1)  $e_p \geq l_p$ , если  $p$  не есть простое число Ферма;
- 2)  $e_p \geq \left\lceil \frac{1}{2} (l_p + 1) \right\rceil$ , если  $p$  — простое число Ферма.

Пусть  $n = p_1^{e_1} p_2^{e_2} \dots p_s^{e_s}$ . Если число  $n$  четно, мы можем считать, что  $p_1 = 2$ , и доказывать утверждение  $S_n$  индукцией по  $s$ , полагая, что утверждение  $S_m$  истинно для  $m = p_1^{e_1} p_2^{e_2} \dots p_{s-1}^{e_{s-1}}$ . По теореме 18.4.3,  $p_s$  — длина конечной разрешимой группы  $G$  показателя  $n$  не превосходит  $2e_s : l = l_{p_s} \leq 2e_s$ . Если группа  $G$  порождается  $r$  элементами, то из утверждения  $S_m$  следует, что порядок группы  $G/P_1$  ограничен числом  $b_{m,r}$ , и поэтому (согласно следствию из теоремы 7.2.2) подгруппа  $P_1$  также имеет ограниченное число образующих, скажем  $r_1$ . Тогда из утверждения  $S_{p_s^{e_s}}$  получаем, что порядок группы  $P_1/N_{l-1}$  ограничен так же, как и число образующих подгруппы  $N_{l-1}$ . Продолжая рассуждения такого рода, приходим к выводу, что порядки фактор-групп  $N_i/P_i$  и  $P_i/N_{i-1}$  ограничены некоторыми числами  $b_{m,k}$  или  $b_{p_s^{e_s},k}$  откуда, так как  $l \leq 2e_s$ , получаем верхнюю грань для порядка группы  $G$ .

**Теорема 18.4.4.** *Если*

$$1 = P_0 \subset N_0 \subset P_1 \subset N_1 \subset P_2 \subset \dots \subset P_l \subset N_l = G$$

— верхний  $p$ -ряд конечной  $p$ -разрешимой группы  $G$ , то подгруппа  $P_1/N_0$  содержит свой централизатор в группе  $G/N_0$ .

**Следствие 18.4.1.** *Подгруппа  $P_1$  содержит свой централизатор в группе  $G$ .*

**Доказательство следствия.** Если  $x$  — элемент централизатора подгруппы  $P_1$  в группе  $G$ , то в группе  $G/N_0$  элемент  $xN_0/N_0$  принадлежит централизатору подгруппы  $P_1/N_0$ . Поэтому в силу теоремы элемент  $xN_0/N_0$  содержится в подгруппе  $P_1/N_0$ . Это означает, что в группе  $G$  смежный класс  $xN_0$  содержится в  $P_1$ , откуда  $x \in P_1$ .

**Доказательство теоремы.** В группе  $G_1 = G/N_0$  не существует инвариантной  $p'$ -подгруппы, так как  $N_0$  — наибольшая

инвариантная  $p'$ -подгруппа группы  $G$ . Подгруппа  $\bar{P}_1 = P_1/N_0$  группы  $G_1$  является ее наибольшей инвариантной  $p$ -подгруппой (по построению). Пусть  $Z$  — централизатор подгруппы  $\bar{P}_1$  группы  $G_1$ . Предположим, что утверждение теоремы ложно, т. е. что  $Z \not\subseteq \bar{P}_1$ . Тогда  $Z$  — инвариантная подгруппа группы  $G_1$ , и поэтому  $Z \cup \bar{P}_1 = Z\bar{P}_1$  — инвариантная подгруппа в группе  $G_1$ . Так как, по предположению,  $Z\bar{P}_1 \supset \bar{P}_1$ , пусть  $M$  — такая минимальная инвариантная подгруппа группы  $G_1$ , что  $\bar{P}_1 \subset M \subseteq Z\bar{P}_1$ . Тогда фактор-группа  $M/\bar{P}_1$  не может быть  $p$ -группой, так как  $\bar{P}_1$  — максимальная инвариантная  $p$ -подгруппа группы  $G_1$ . Следовательно,  $M/\bar{P}_1$  —  $p'$ -подгруппа, так как группа  $G$   $p$ -разрешима. Но тогда порядки подгрупп  $\bar{P}_1$  и  $M/\bar{P}_1$  взаимно просты, и по теореме 15.2.2 расширение подгруппы  $\bar{P}_1$  расщепляется, т. е.  $M = K\bar{P}_1$ , где  $K \cap \bar{P}_1 = 1$  и подгруппа  $K$  изоморфна фактор-группе  $M/\bar{P}_1$ . Так как  $K \subseteq Z\bar{P}_1$ , трансформирование группы  $\bar{P}_1$  элементом  $u$  из  $K$  индуцирует внутренний автоморфизм группы  $\bar{P}_1$ , а так как порядки групп  $K$  и  $\bar{P}_1$  взаимно просты, этот автоморфизм может быть только тождественным. Следовательно,  $M$  есть прямое произведение подгрупп  $K$  и  $\bar{P}_1$ ,  $M = K \times \bar{P}_1$ . Но тогда подгруппа  $K$ , будучи характеристической подгруппой группы  $M$ , инвариантна в группе  $G_1$ , что противоречит тому, что в группе  $G_1$  нет инвариантных  $p'$ -подгрупп. Таким образом, предположение, что  $Z \not\subseteq \bar{P}_1$ , приводит к противоречию, и теорема доказана.

Следующая теорема существенно уточняет результат предыдущей.

**Теорема 18.4.5.** *Если  $G$  —  $p$ -разрешимая группа с верхним  $p$ -рядом*

$$1 = P_0 \leq N_0 \subset P_1 \subset N_1 \subset P_2 \dots \subset P_l \leq N_l = G$$

*и если  $F/N_0$  — подгруппа Фраттини группы  $P_1/N_0$ , то автоморфизмы группы  $P_1/F$ , индуцируемые трансформированием элементами из  $G$ , дают точное представление группы  $G/P_1$ .*

**Доказательство.** Группа  $F/N_0$  является пересечением максимальных подгрупп  $p$ -группы  $P_1/N_0$ , а группа  $P_1/F$ , согласно теореме 12.2.1, есть элементарная абелева  $p$ -группа. Так как подгруппа  $F/N_0$  содержит коммутант группы  $P_1/N_0$ , любой элемент из группы  $P_1$  индуцирует при трансформировании тождественный автоморфизм группы  $P_1/F$ . Поэтому множество элементов группы  $G$ , индуцирующих тождественный автоморфизм группы  $P_1/F$ , составляет инвариантную подгруппу  $K$ , причем  $K \supseteq P_1$ . Покажем, что строгое включение  $K \supset P_1$  ведет к противоречию, т. е. что  $K = P_1$ , и поэтому группа  $G/P_1$  точно представляется внутренними автоморфизмами группы  $P_1/F$ . Если  $K \supset P_1$ , то фактор-группа  $K/P_1$

не есть  $p$ -группа, так как по построению  $P_1/N_0$  — максимальная инвариантная  $p$ -подгруппа группы  $G/N_0$ . Тогда  $K$  содержит элемент  $x \notin P_1$ , порядок которого взаимно прост с  $p$ ; этот элемент  $x$  индуцирует при трансформировании тождественный автоморфизм группы  $P_1/F$ . Но, согласно теореме 12.2.2, автоморфизм  $p$ -группы  $P_1/N_0$ , действующий тождественно на группе  $P_1/F$ , имеет порядок  $p^a$ . Тогда, так как порядок элемента  $x$  взаимно прост с  $p$ ,  $x$  индуцирует тождественный автоморфизм в группе  $P_1/N_0$ ; в силу теоремы 18.4.4 это означает, что  $x \in P_1$ , а это противоречит нашему выбору элемента  $x$ . Таким образом, включение  $K \supset P_1$  приводит к противоречию. Поэтому  $K = P_1$ , и теорема доказана.

Согласно теореме 18.4.5, мы располагаем точным представлением группы  $G/P_1$  некоторыми автоморфизмами элементарной абелевой  $p$ -группы  $P_1/F$ . При этом  $G/P_1$  —  $p$ -разрешимая группа и  $l_p(G/P_1) = l_p(G) - 1$ . Далее, по определению, фактор-группа  $G/P_1$  не содержит инвариантных  $p$ -подгрупп. Остальная часть рассматриваемой работы Ф. Холла и Хигмэна состоит в изучении свойств представления группы  $G/P_1$  автоморфизмами группы  $P_1/F$ , т. е. фактически представления линейными преобразованиями векторного пространства над полем из  $p$  элементов.  $G/P_1$  является  $p$ -разрешимой группой, не содержащей инвариантных  $p$ -подгрупп. Дальнейшая теория зависит от того, что можно сказать о таких группах, которые допускают точное представление над полем характеристики  $p$ . Эти исследования проводятся индукцией по  $p$ -длине, использующей равенство  $l_p(G) = l_p(G/P_1) + 1$ .

Обратимся к конечным группам  $G$  показателя 6, чтобы изучить строение групп Бернсайда  $B(6, r)$  и установить их конечность.

**Теорема 18.4.6.** В конечной группе  $G$  показателя 6  $l_2(G) \leqslant 1$  и  $l_3(G) \leqslant 1$ .

**Доказательство.** Конечная группа  $G$  показателя 6 имеет порядок  $2^a3^b$  и потому разрешима. В верхнем 2-ряду для группы  $G$  фактор-группа  $P_1/N_0$  является 2-группой, содержащей свой централизатор в  $G/N_0$ . Но так как показатель группы  $G$  равен 6, показатель силовской 2-подгруппы группы  $G$  равен 2, и, значит, она является элементарной абелевой группой. Следовательно, силовская 2-подгруппа группы  $G/N_0$  содержится в централизаторе подгруппы  $P_1/N_0$  группы  $G/N_0$  и тем самым содержится в  $P_1/N_0$ . Поэтому группа  $P_1/N_0$  совпадает с силовской 2-подгруппой группы  $G/N_0$ , откуда  $l_2(G) = 1$ , и верхний 2-ряд группы  $G$  имеет вид

$$1 = P_0 \leq N_0 \subset P_1 \leq N_1 = G, \quad (18.4.25)$$

где  $N_0/P_0$  — 3-группа,  $P_1/N_0$  — 2-группа и  $N_1/P_1$  — 3-группа.

Так как (18.4.25) — инвариантный ряд для группы  $G$ , имеющей не больше двух факторов, являющихся 3-группами, очевидно, что

$I_3(G) \leqslant 2$ . Предположение  $I_3(G) = 2$  приводит к тому, что группа  $C$  содержит элемент порядка 9. Но это противоречит тому, что показатель группы  $G$  равен 6. Отсюда получаем, что  $I_3(G) \leqslant 1$ . Верхний 3-ряд имеет вид

$$1 = A_0 \subseteq B_0 \subset A_1 \subset B_1 \subset A_2 \subseteq B_2 = G, \quad (18.4.26)$$

где  $B_0/A_0$ ,  $B_1/A_1$  и  $B_2/A_2$  — 2-группы, а  $A_1/B_0$  и  $A_2/B_1$  — 3-группы. Заметим, что

$$1 = B_0/B_0 \subset A_1/B_0 \subset B_1/B_0 \subset A_2/B_0 \subseteq G/B_0 \quad (18.4.27)$$

— верхний 2-ряд для группы  $G/B_0$ , а так как ее 2-длина равна единице, то  $A_2 = B_2 = G$ . По теореме 18.4.4 2-группа  $B_1/A_1$  совпадает со своим централизатором в группе  $A_2/A_1$ . Поэтому если в группе  $A_2/A_1$  элемент  $x$  имеет порядок 3, то в подгруппе  $B_1/A_1$  существует элемент  $u$  порядка 2, не перестановочный с элементом  $x$ . Если

$$u = u_1, \quad x^{-1}u_1x = u_2, \quad x^{-1}u_2x = u_3, \quad (18.4.28)$$

то  $x^{-1}u_3x = u_1$ , так как  $x^3 = 1$ . Положим  $y = y_1 = u_1u_2$  и  $y_2 = u_2u_3$ . Так как элементы  $u_1$ ,  $u_2$ ,  $u_3$  принадлежат элементарной абелевой 2-группе, то  $u_3u_1 = (u_1u_2)(u_2u_3) = y_1y_2$ . Поэтому в группе  $C = \{x, y_1, y_2\}$  выполняются соотношения

$$\begin{aligned} x^3 &= 1, \quad y_1^2 = y_2^2 = 1, \quad y_2y_1 = y_1y_2, \\ x^{-1}y_1x &= y_2, \quad x^{-1}y_2x = y_1y_2. \end{aligned} \quad (18.4.29)$$

Так как элемент  $x$  не перестановочен с  $u_1$ ,  $u_2 \neq u_1$ , поэтому  $y_1 = u_1u_2 \neq 1$ . Далее, равенство  $y_2 = y_1$  означало бы, что  $x^{-1}y_2x = 1$  и  $1 = y_2 = y_1$ . Поэтому  $y_2 \neq y_1$ , и, как видно из соотношений (18.4.29), порядок группы  $C$  равен 12; следовательно, в действительности она изоморфна знакопеременной группе степени 4. Согласно теореме 18.4.5, если  $F/B_0$  — подгруппа Фраттини группы  $A_1/B_0$ , то группа  $G/A_1$  точно представима трансформированиями элементарной абелевой 3-группы  $A_1/F$ . В частности, группа  $C$  точно представляется трансформированиями группы  $A_1/F = W$ . Если записать группу  $W$  аддитивно, то трансформирование ее элементом  $z$  группы  $G/A_1$  можно представить как действие оператора справа. При этом областью операторов на группе  $W$  является не только группа  $C$ , но и групповое кольцо  $C^*$ . Операторы из  $C^*$ , отображающие любой элемент группы  $W$  в нуль, как легко проверить, образуют двусторонний идеал кольца  $C^*$ . Будем считать, что группа  $C$  задана образующими  $x$  и  $y = y_1$  и определяющими отношениями

$$x^3 = 1, \quad y^2 = 1, \quad (xy)^3 = 1. \quad (18.4.30)$$

Тогда двусторонний идеал кольца  $C^*$ , содержащий элемент  $1 + x + x^2$ , также содержит элемент

$$\begin{aligned} x^2y(1+x+x^2)yx - (1+x+x^2)y - y(1+x+x^2) + \\ + xy(1+x+x^2)yx^2 = 2 - 2y. \end{aligned} \quad (18.4.31)$$

Если бы для любого элемента  $w \in W$  выполнялось соотношение  $w(1+x+x^2)=0$ , то из равенства (18.4.31) мы получили бы, что  $w(2-2y)=0$ , а так как элементы группы  $W$  имеют порядок 3, это значило бы, что  $wy=w$  для любого  $w \in W$ . Но в этом случае элемент  $y$  не представляется точно трансформированием группы  $W=A_1/F$ , что противоречит теореме 18.4.5. Таким образом, для некоторого элемента  $w \in W$  мы имеем  $w(1+x+x^2) \neq 0$ .

В мультиликативной записи это означает, что для представителя  $\bar{x}$  смежного класса  $\bar{x}A_1$ , являющегося элементом  $x$  группы  $A_2F$ , имеем

$$w(\bar{x}^{-1}w\bar{x})(\bar{x}^{-2}w\bar{x}^2) \neq 1, \quad (18.4.32)$$

или

$$(w\bar{x}^{-1})^3 \bar{x}^3 \neq 1; \quad (18.4.33)$$

здесь  $\bar{x}^3$  и  $(w\bar{x}^{-1})^3$  — элементы группы  $W$ , не равные единице одновременно в силу неравенства (18.4.33). Поэтому или  $\bar{x}$ , или  $w\bar{x}^{-1}$  — элемент порядка 9. Таким образом, из равенства  $I_3(G)=2$  следует существование элемента порядка 9, но это противоречит тому, что показатель группы  $G$  равен 6. Следовательно,  $I_3(G) \leqslant 1$ , и теорема доказана.

Опираясь на теорему 18.4.6, мы можем точно определить порядок наибольшей конечной группы показателя 6, порожденной  $r$  элементами.

**Теорема 18.4.7.** Порядок группы  $R(6,r)$  равен

$$2^{a_3} 3^{b + \binom{b}{2} + \binom{b}{3}}, \quad (18.4.34)$$

где

$$a = 1 + (r-1) 3^{r + \binom{r}{2} + \binom{r}{3}}, \quad b = 1 + (r-1) 2^r.$$

**Доказательство.** Пусть  $F_r$  — свободная группа с  $r$  образующими. Если  $S$  — подгруппа, порожденная квадратами элементов группы  $F_r$ , то  $F_r/S$  — элементарная абелева группа порядка  $2^r$ . Следовательно, в силу теоремы 7.2.8,  $S$  есть свободная группа с  $b = 1 + (r-1) \cdot 2^r$  образующими. Вполне характеристическая подгруппа  $T$  группы  $S$ , порожденная кубами элементов группы  $S$ , такова, что  $S/T \cong B(3, b)$ , и поэтому индекс подгруппы  $T$  в группе  $S$  равен  $3^{b + \binom{b}{2} + \binom{b}{3}}$ . При этом  $F_r/T$  — конечная группа показателя 6, так как при  $g \in F_r$ ,  $g^2 \in S$  и  $(g^2)^3 \in T$ . Аналогично

группа  $F_r$  обладает подгруппой  $C$  индекса  $3^{r+{r \choose 2}+{r \choose 3}}$ , порожденной кубами элементов из  $F_r$ . Согласно теореме 7.2.8, подгруппа  $C$  имеет  $a = 1 + (r - 1) \cdot 3^{r+{r \choose 2}+{r \choose 3}}$  свободных образующих. Индекс вполне характеристической подгруппы  $D$ , порождаемой квадратами элементов из группы  $C$ , равен  $2^a$ . Пусть теперь  $X = D \cap T$ .  $F_r/X$  — конечная группа показателя 6, так как подгруппы  $D$  и  $T$  содержат элементы  $g^6$ , где  $g$  — любой элемент из  $F_r$ . Нетрудно убедиться в том, что верхний 2-ряд группы  $F_r/X$  имеет вид

$$1 = X/X \subset D/X \subset C/X \subset F_r/X, \quad (18.4.35)$$

а верхний 3-ряд —

$$1 = X/X \subset T/X \subset S/X \subset F_r/X. \quad (18.4.36)$$

Группа  $C/D$  изоморфна силовской 2-подгруппе группы  $F_r/X$ , а  $S/T$  — силовской 3-подгруппе, откуда порядок группы  $F_r/X$  равен числу (18.4.34).

Пусть  $G$  — произвольная конечная группа показателя 6, порожденная  $r$  элементами. Если

$$1 = P_0 \subseteq N_0 \subseteq P_1 \subseteq N_1 = G \quad (18.4.37)$$

— верхний 3-ряд группы  $G$ , то порядок фактор-группы  $N_1/P_1$  превосходит  $2^r$ ; поэтому подгруппа  $P_1$  порождается не более чем  $b$  элементами, откуда группа  $P_1/N_0$ , изоморфная силовской 3-подгруппе группы  $G$ , имеет порядок не больше  $3^{b+{b \choose 2}+{b \choose 3}}$ . Аналогично порядок группы  $G$  делится не более чем на  $2^a$ .

Так как доказательство конечности группы Бернсайда  $B(6, r)$  содержит большие вычисления, то из-за недостатка места мы не будем здесь излагать его полностью. Оно не использует предыдущие результаты и указывает степень 2, которая делит порядок группы  $B(6, r)$ , однако, чтобы получить степень 3, необходимо применить теорему 18.4.7. Доказательство состоит в том, что группа  $G$  с конечным числом образующих показателя 6 имеет 2-длину, равную единице, а потому в силу конечности групп  $B(2, r)$  и  $B(3; r)$  группа  $G$  сама конечна. Доказательство последнего факта равносильно доказательству того, что существует инвариантная цепь

$$G \supset M \supset M' \supset 1, \quad (18.4.38)$$

в которой  $G/M$  — конечная 3-группа,  $M/M'$  — конечная 2-группа, а  $M'$  — подгруппа с конечным числом образующих показателя 3, которая поэтому конечна. Основная трудность состоит в доказательстве того, что показатель подгруппы  $M'$  равен 3.

**Теорема 18.4.8.** *Группа  $G$  показателя 6, порожденная  $r$  элементами, конечна.*

**Следствие 18.4.2.** Порядок группы  $B(6, r)$  равен числу (18.4.34).

**Лемма 18.4.1.** Кубы элементов группы  $G$  порождают инвариантную подгруппу  $M$ , индекс которой не превосходит  $3^{r+{r \choose 2}+{r \choose 3}}$ .

**Лемма 18.4.2.** Подгруппа  $M$  порождается конечным числом элементов порядка 2. Индекс коммутанта  $M'$  группы  $M$  в самой группе  $M$  равен степени двойки;  $M'$  порождается конечным числом элементов вида  $abab$ , где  $a^2 = b^2 = 1$ .

**Лемма 18.4.3.** Если группа  $H$  порождается элементами  $x_1, \dots, x_n$  и если показатель любой ее подгруппы, порожденной четырьмя из этих образующих, равен 3, то и показатель самой группы  $H$  равен 3.

**Лемма 18.4.4.** Если  $H = \{a, b, c, d\}$  — группа показателя 6, а показатели подгрупп  $\{a, b, c\}, \{a, b, d\}, \{a, c, d\}$  и  $\{b, c, d\}$  равны 3, то и показатель группы  $H$  равен 3.

**Лемма 18.4.5.** Если показатель группы  $H = \{x, a, b\}$  равен 6 и если  $x^2 = 1, a^3 = b^3 = 1, xax = a^{-1}, xb = b^{-1}$ , то показатель подгруппы  $\{a, b\}$  равен 3.

Это самая трудная лемма, доказывается она при помощи сложных преобразований соотношений для элементов группы  $H$ .

**Лемма 18.4.6.** Если  $H = \{x, a, b\}$  — группа показателя 6 и если  $x^2 = 1, a^3 = b^3 = 1, xax = a^{-1}, xb = b$ , то показатель подгруппы  $\{a, b\}$  равен 3.

**Лемма 18.4.7.** Если группа  $H = \{x, a, b, c\}$  показателя 6 и если  $x^2 = 1, a^3 = b^3 = c^3 = 1, xax = a^{-1}, xb = b^{-1}, xc = c^{-1}$ , то показатель подгруппы  $\{a, b, c\}$  равен 3.

**Лемма 18.4.8.** Если  $H = \{x, a_i\}, i = 1, \dots, n$ , — группа показателя 6 и если  $x^2 = 1, a_i^3 = 1, x a_i x = a_i^{-1}, i = 1, \dots, n$ , то показатель подгруппы  $\{a_i\}, i = 1, \dots, n$ , равен 3.

Как нетрудно заметить, эта лемма следует из лемм 18.4.3, 18.4.4 и 18.4.7.

**Лемма 18.4.9.** Если  $H = \{a, b, c\}$  — группа показателя 6 и если  $a^2 = b^2 = c^2 = 1$ , то  $H'$  — подгруппа показателя 3.

**Лемма 18.4.10.** Если показатель группы  $H = \{a, b, c, d\}$  равен 6 и  $a^2 = b^2 = c^2 = d^2 = 1$ , то показатель подгруппы  $\{abab, cdcd\}$  равен 3.

**Лемма 18.4.11.** Если показатель группы  $H = \{a, b, c, d, e, f\}$  равен 6 и  $a^2 = b^2 = c^2 = d^2 = e^2 = f^2 = 1$ , то показатель подгруппы  $\{abab, cdcd, efef\}$  равен 3.

**Лемма 18.4.12.** Подгруппа  $M'$  показателя 3 конечна. Следовательно, конечна и группа  $G$ .

Последняя лемма является прямым следствием лемм 18.4.2, 18.4.3, 18.4.4 и 18.4.11.

## Г л а в а 19

### СТРУКТУРЫ ПОДГРУПП

#### 19.1. Общие свойства

Подгруппы произвольной группы  $G$  можно рассматривать как элементы структуры  $L(G)$  относительно операций объединения и пересечения. Любая циклическая группа простого порядка обладает только подгруппой, совпадающей со всей группой, и единичной подгруппой; поэтому все такие циклические группы обладают одной и той же структурой подгрупп, состоящей просто из двух-элементной цепи. Мы уже показали в теореме 1.5.4, что верно и обратное: группа, не имеющая истинных подгрупп, состоит только из единицы или является конечной циклической группой простого порядка. Отметим также, что неабелева группа порядка  $pq$ , где  $p < q$ ,  $p/q = 1$ , и элементарная абелева группа порядка  $q^2$  обе имеют одинаковые структуры подгрупп, состоящие из единицы,  $q+1$  подгрупп простого порядка и всей группы; при этом пересечение любой пары истинных подгрупп равно единичной подгруппе, а их объединение — всей группе.

Таким образом, хотя группа  $G$  определяет структуру  $L(G)$  однозначно, вообще говоря, одной и той же структуре  $L(G)$  может соответствовать несколько групп  $G$ . Нетрудно построить примеры структур  $L$ , не являющихся структурами подгрупп никакой группы. Но многие группы  $G$  определяются однозначно структурой  $L(G)$ , например это верно для знакопеременной и симметрической групп степени 4. Возможно даже, что, за исключением нескольких групп сравнительно простого строения, структура  $L(G)$  определяет группу  $G$  однозначно.

В терминах теории структур структура  $L(G)$  является полной в том смысле, что существуют бесконечные пересечения и объединения ее элементов. Действительно, множество элементов, принадлежащих всем подгруппам произвольного семейства подгрупп, образует подгруппу, которая и является пересечением этих подгрупп; аналогично множество всех конечных произведений элементов некоторого семейства подгрупп составляет группу, являющуюся объединением этого семейства подгрупп.

Для дальнейшего изучения структуры подгрупп отсылаем читателя к монографии Судзуки [1].

## 19.2. Локально циклические группы и дистрибутивные структуры

В структуре оба дистрибутивных закона

$$D1. \quad a \cap (b \cup c) = (a \cap b) \cup (a \cap c),$$

$$D2. \quad a \cup (b \cap c) = (a \cup b) \cap (a \cup c)$$

эквивалентны друг другу. Покажем, что из D1 следует D2. Используя D1, получаем

$$\begin{aligned} (a \cup b) \cap (a \cup c) &= [(a \cup b) \cap a] \cup [(a \cup b) \cap c] = \\ &= a \cup [(a \cap c) \cup (b \cap c)] = \\ &= [a \cup (a \cap c)] \cup (b \cap c) = a \cup (b \cap c), \end{aligned}$$

т. е. получаем закон D2. Аналогично показывается, что из D2 следует D1. Выполнение дистрибутивного закона является очень сильным требованием для структур. Мы докажем сейчас, что для групп  $G$  условие дистрибутивности структуры  $L(G)$  является очень сильным и что из него следует, что группа  $G$  локально циклическая.

**Определение.** Группа  $G$  называется локально циклической, если любое конечное множество ее элементов порождает циклическую группу. (Ср. с § 13.1.)

Так как элемент конечного порядка, отличный от единицы, вместе с элементом бесконечного порядка не могут порождать циклическую группу, то в локально циклической группе все отличные от единицы элементы одновременно или бесконечного порядка, или все имеют конечные порядки. Аддитивная группа рациональных чисел  $R_+$  — локально циклическая группа без кручения, а группа  $R_+$  по модулю 1 — локально циклическая периодическая группа. Нетрудно показать, что произвольная локально циклическая группа является подгруппой одной из этих двух групп.

**Теорема 19.2.1.** Структура  $L(G)$  дистрибутивна тогда и только тогда, когда  $G$  — локально циклическая группа.

**Доказательство.** Пусть  $G$  — локально циклическая группа, и пусть  $A, B$  и  $C$  — три ее подгруппы. Докажем свойство D1.

Вообще

$$\begin{aligned} A &\supseteq A \cap B, \\ B \cup C &\supseteq B \supseteq A \cap B, \end{aligned}$$

откуда  $U = A \cap (B \cup C) \supseteq A \cap B$ . Далее,

$$\begin{aligned} A &\supseteq A \cap C, \\ B \cup C &\supseteq C \supseteq A \cap C, \end{aligned}$$

откуда  $U = A \cap (B \cup C) \supseteq A \cap C$ . В итоге

$$U = A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C).$$

Осталось доказать обратное включение

$$U = A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C) = V.$$

Рассмотрим произвольный элемент  $g \in U$ . Он имеет вид

$$g = a = bc, \quad a \in A, \quad b \in B, \quad c \in C,$$

так как  $B \cup C = BC$  в силу абелевости группы  $G$ . Поскольку группа  $G$  локально циклическая, элементы  $b$  и  $c$  порождают циклическую группу  $\{u\}$ ,  $u^r = b$ ,  $u^s = c$ , а так как для некоторых  $m$  и  $n$   $b^m c^n = u$ , то отсюда следует, что  $u^{rm+sn} = u$ . Тогда  $a = bc = u^{r+s}$ ;  $x = u^{r(r+s)} = a^r = b^{r+s} \in A \cap B$  и  $y = u^{s(r+s)} = a^s = c^{r+s} \in A \cap C$ . Поэтому  $a = u^{r+s} = u^{mr(r+s)+ns(r+s)} = x^m y^n$  есть элемент  $(A \cap B) \cup (A \cap C)$ , что и требовалось доказать. Итак, доказано равенство

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

для любых подгрупп локально циклической группы.

Докажем обратное утверждение. Пусть структура  $L(G)$  дистрибутивна, т. е. обладает свойствами D1 и D2. Докажем, что группа  $G$  локально циклическая. Пусть  $b$  и  $c$  — два произвольных элемента группы  $G$ , пусть также  $a = bc$ ,

$$A = \{a\}, \quad B = \{b\}, \quad C = \{c\}.$$

Тогда, так как  $a \in B \cup C$ , мы имеем

$$A = A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$

Группы  $A \cap B$  и  $A \cap C$  как подгруппы циклических групп цикличны; пусть

$$A \cap B = \{u\}, \quad A \cap C = \{v\},$$

где при соответствующих показателях степени

$$a^x = b^y = u, \quad a^z = c^w = v.$$

Здесь элементы  $u$  и  $v$  как степени элемента  $a$  перестановочны; так как  $A = \{u\} \cup \{v\}$ , то для  $a \in A$  мы имеем равенство  $a = u^r v^s = v^s u^r$ . Но  $a = bc$ , следовательно,  $bc = u^r v^s = b^{yr} c^{ws} = c^{ws} b^{yr}$ . Поэтому  $b^{1-yr} = c^{ws-1}$ , откуда  $c^{-ws+1} = b^{yr-1}$  или  $v^{-s} c = u^r b^{-1}$ . Поэтому  $cb = v^s u^r = u^r v^s = bc$ , т. е. элементы  $b$  и  $c$  перестановочны, и группа  $G$  абелева.

Группа  $G$  не может одновременно содержать элемент  $a \neq 1$  конечного порядка и элемент  $b$  бесконечного порядка. Действительно, в противном случае элемент  $c = ab$  также имеет бесконечный порядок. Тогда  $\{a\} = \{a\} \cap (\{b\} \cup \{c\})$ , так как  $a = b^{-1}c$ , и в то же время  $(\{a\} \cap \{b\}) \cup (\{a\} \cap \{c\}) = (1) \cup (1) = 1 \neq \{a\}$ , так как бесконечные циклические группы  $\{b\}$  и  $\{c\}$ , не содержащие

не равных единице элементов конечного порядка, пересекаются с подгруппой  $\{a\}$  по единичной подгруппе. Таким образом, достаточно рассмотреть только два случая: первый, когда группа  $G$  без кручения, и второй, когда группа  $G$  периодическая. В каждом из этих случаев, если два элемента не порождают циклическую группу, согласно основной теореме об абелевых группах, они порождают прямое произведение двух циклических групп, скажем,  $\{b\}$  и  $\{c\}$ . Тогда в первом случае при  $a = bc$ ,  $A = \{a\}$ ,  $B = \{b\}$  и  $C = \{c\}$  мы получаем, что  $A = A \cap (B \cup C)$ , между тем как  $(A \cap B) \cup (A \cap C) = (1) \cup (1) = (1)$ , т. е. свойство D1 не выполняется. В периодическом случае если порядки элементов  $b$  и  $c$  взаимно просты, то  $\{b\} \cup \{c\} = \{bc\}$ , т. е. они действительно порождают циклическую группу. Однако прямое произведение двух циклических групп  $\{b\}$  и  $\{c\}$ , порядки которых имеют общий делитель, скажем, простое число  $p$ , не имеет дистрибутивной структуры подгрупп, так как для элементов  $b_1 \in \{b\}$  и  $c_1 \in \{c\}$  порядка  $p$  и  $a_1 = b_1 c_1$  свойство D1 нарушается при  $A = \{a_1\}$ ,  $B = \{b_1\}$  и  $C = \{c_1\}$ . Таким образом, чтобы дистрибутивный закон имел место, необходимо, чтобы любые два элемента порождали циклическую группу. Но если два любых элемента порождают циклическую группу, то отсюда сразу следует, что любое конечное число элементов порождает циклическую группу, т. е. что группа  $G$  локально циклическая. Теорема доказана.

### 19.3. Теорема Ивасава

Композиционные (или главные) ряды, как показано в § 8.5, обладают тем свойством, что все они имеют одну и ту же длину. Это свойство является следствием модулярности структуры инвариантных подгрупп и слабой формы модулярности для композиционных рядов. Однако, вообще говоря, максимальные цепи произвольных подгрупп могут иметь разную длину. Из теоремы 10.5.5 следует, что в конечной сверхразрешимой группе все максимальные цепи подгрупп имеют одну и ту же длину. Следующая теорема Ивасава [1] показывает, что обратное утверждение также верно.

**Теорема 19.3.1.** *Максимальные цепи подгрупп конечной группы  $G$  имеют равные длины тогда и только тогда, когда группа  $G$  сверхразрешима.*

**Доказательство.** Как отмечалось выше, теорема 10.5.5 показывает, что в сверхразрешимой группе  $G$  все максимальные цепи подгрупп имеют одинаковую длину, равную числу простых чисел, которые делят порядок группы  $G$  (с учетом повторений).

Если группа  $G$  обладает тем свойством, что все ее максимальные цепи подгрупп имеют одинаковую длину, то мы будем в дальнейшем говорить, что она обладает *эквицепным свойством*.

Очевидно, что это свойство выполняется также для подгрупп и фактор-групп таких групп. Пусть  $G$  — конечная группа с эквидепенным свойством. Так как группа, структурой подгрупп которой является цепь длины один, есть циклическая группа простого порядка, т. е. сверхразрешимая группа, то, применяя индукцию по длине максимальных цепей, предположим, что все истинные подгруппы и фактор-группы группы  $G$  сверхразрешимы.

Нам понадобится лемма о сверхразрешимых группах.

**Лемма 19.3.1.** *Пусть  $G$  — конечная сверхразрешимая группа порядка  $n = p_1^{e_1} p_2^{e_2} \dots p_m^{e_m}$ , где  $p_1 \leqslant p_2 \leqslant \dots \leqslant p_m$ . Тогда группа  $G$  обладает главным рядом*

$$K_0 = 1 \subset K_1 \subset K_2 \subset \dots \subset K_m = G,$$

где  $K_i/K_{i-1}$  — группа порядка  $p_{m-i+1}$ ,  $i = 1, \dots, m$ .

Эта лемма является следствием из теоремы 10.5.2.

Следующий и самый трудный шаг доказательства состоит в том, чтобы установить существование инвариантной подгруппы группы  $G$ .

**Лемма 19.3.2.** *Если  $G$  — конечная группа, порядок которой делится на простое число  $p$ , то или (1) она  $p$ -нормальна, или (2) группа  $G$  обладает  $p$ -подгруппой  $P$ , инвариантной в одной силовской подгруппе  $S_1(p)$ , но неинвариантной в другой силовской подгруппе  $S_2(p)$ .*

**Доказательство.** Напомним, что группа  $G$ , по определению,  $p$ -нормальна, если центр  $Z$  одной силовской подгруппы  $S_1(p)$  является центром любой другой силовской подгруппы  $S_2(p)$ , в которой он содержится. Поэтому если группа  $G$  не  $p$ -нормальна, то центр  $Z$  некоторой силовской подгруппы  $S_1(p)$  содержитя в другой силовской подгруппе  $S_2(p)$ , но не является ее центром. В этом случае, как мы покажем, выполняется вторая альтернатива леммы. В качестве подгруппы  $P$  возьмем  $Z$  и докажем, что подгруппа  $Z$  неинвариантна в группе  $S_2(p)$ . Предположим противное, т. е. что  $Z$  инвариантна в  $S_2(p)$ . Тогда подгруппы  $S_1(p)$  и  $S_2(p)$  содержатся в нормализаторе  $N = N_G(Z)$  и, будучи его силовскими подгруппами, сопряжены в  $N$ , т. е. для некоторого  $x \in N$ ,  $x^{-1}S_1(p)x = S_2(p)$ . Так как  $Z$  — центр группы  $S_1(p)$ , то центром для  $S_2(p) = x^{-1}S_1(p)x$  является подгруппа  $x^{-1}Zx = Z$ , так как  $x \in N_G(Z)$ . Это противоречит допущению, что  $Z$  не есть центр группы  $S_2(p)$ . Этим лемма доказана. Заметим, что в доказательстве применялась теорема Бернсайда 4.2.5.

Пусть теперь порядок группы  $G$  равен  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ , где  $p_1 < p_2 < \dots < p_r$  — простые числа. Применим лемму 19.3.2 для наименьшего простого числа  $p_1$ , которое делит  $n$ . Покажем, что для группы  $G$  вторая альтернатива леммы исключена. Действи-

тельно, в силу теоремы 4.2.5 существует  $t \not\equiv 0 \pmod{p_1}$   $p_1$ -групп  $h_1, h_2, \dots, h_t$ , инвариантных в их объединении  $H$  и сопряженных в нормализаторе  $N = N_G(H)$  подгруппы  $H$  группы  $G$ . Если  $H$  — инвариантная подгруппа в  $G$ , то мы имеем инвариантную подгруппу, т. е. то, что искали. Если же  $N$  — собственная подгруппа группы  $G$ , то, по предположению индукции, она сверхразрешима. Применяя лемму 19.3.1 к подгруппе  $N$ , находим, что она содержит инвариантную подгруппу  $Q$ , индекс которой в  $N$  равен наивысшей степени числа  $p_1$ , делящей порядок подгруппы  $N$ . Но тогда  $Q$  и  $H$  — инвариантные подгруппы в  $N$ , и так как  $Q \cap H = 1$  ( $H$  —  $p_1$ -подгруппа), то  $Q \cup H = Q \times H$ . Таким образом, подгруппа  $Q$  перестановочна с любым элементом из  $H$ , и поэтому нормализатор подгруппы  $h_1$  содержит  $Q$  и не может иметь индекса  $t$ , взаимно простого с  $p_1$ . Итак, мы показали, что вторая альтернатива осуществиться не может, если  $N$  — собственная подгруппа. Строго говоря, мы доказали только, что вторая альтернатива не имеет места только для случая, когда  $N$  — собственная подгруппа. Но когда закончим наше доказательство и покажем, что группа  $G$  сверхразрешима, то вышеприведенная аргументация будет применима и к случаю  $N = G$ .

Рассмотрим теперь первую альтернативу, а именно что  $G$  есть  $p_1$ -нормальная группа. Пусть  $Z$  — центр силовской подгруппы  $S_1(p_1)$  и  $K = N_G(Z)$ . Если  $K = G$ , то  $Z$  — собственная инвариантная подгруппа группы  $G$ , которую мы и искали. Поэтому предположим, что  $K$  есть собственная подгруппа группы  $G$ , которая, по предположению индукции, сверхразрешима. Тогда, применяя лемму 19.3.1 к подгруппе  $K$ , получаем, что  $K$  содержит инвариантную подгруппу  $W$  индекса  $p_1$ , а, так как фактор-группа  $K/W$  — циклическая группа порядка  $p_1$ ,  $W \trianglelefteq K'$ , и группа  $K$  имеет нетривиальный гомоморфный образ, являющийся абелевой  $p_1$ -группой, который мы обозначим через  $K/K'(p_1)$ . Но, согласно теореме 14.4.5, так как группа  $G$   $p_1$ -нормальна, фактор-группа  $G/G'(p_1)$  изоморфна группе  $K/K'(p_1)$ ; таким образом,  $G'(p_1)$  — собственная инвариантная подгруппа. Показав, что во всех случаях группа  $G$  обладает собственной инвариантной подгруппой, и учитывая, что, по предположению индукции, инвариантная подгруппа и соответствующая фактор-группа сверхразрешимы, мы заключаем, что группа  $G$  разрешима.

Пусть порядок группы  $G$  равен  $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ ,  $p_1 < p_2 < \dots < p_r$ . Доказав разрешимость  $G$ , мы теперь знаем, что все максимальные цепи имеют длину  $m$ , где  $m = e_1 + e_2 + \dots + e_r$ , и что любое отношение покрытия  $A > B$  обладает тем свойством, что  $[A : B]$  — простое число. Пусть  $S(p_r)$  — силовская подгруппа порядка  $p_r^{e_r}$ , и пусть  $1 \subset A_1 \subset A_2 \subset \dots \subset A_{e_r} = S(p_r) \subset B_1 \subset \dots \subset B_{m-e_r} =$

$= G$  — максимальная цепь, начинающаяся максимальной цепью группы  $S(p_r)$ . Покажем, что  $S(p_r)$  — нормальный делитель в  $G$ . Индекс  $[B_1 : S(p_r)]$  есть некоторое простое число  $p_j < p_r$ . Так как число подгрупп, сопряженных с  $S(p_r)$  в  $B_1$ , должно делить  $p_j$  и иметь вид  $1 + kp_r$ , в силу третьей теоремы Силова, оно равно 1, и поэтому  $S(p_r) \triangleleft B_1$ . Аналогично, если мы уже показали, что  $S(p_r) \triangleleft B_i$ , то число подгрупп, сопряженных с  $S(p_r)$  в группе  $B_{i+1}$ , во-первых, имеет вид  $1 + kp_r$  и, во-вторых, делит индекс  $[B_{i+1} : B_i] = p_j < p_r$ . Поэтому  $S(p_r) \triangleleft B_{i+1}$ . Продолжив до конца эти рассуждения, получим, что  $S(p_r)$  — нормальный делитель в  $G$ . Будучи разрешимой, группа  $G$  обладает силовским дополнением  $C$  подгруппы  $S(p_r)$  порядка  $p_1^{e_1} \dots p_{r-1}^{e_{r-1}}$  (теорема 9.3.1). Пусть  $Z$  — центр подгруппы  $S(p_r)$ . Являясь характеристической подгруппой группы  $S(p_r)$ , центр  $Z$  — инвариантная подгруппа группы  $G$ . Поэтому  $C \cup Z = CZ = U$ . В группе  $U$  максимальная цепь подгруппы  $C$  может быть продолжена до максимальной цепочки для  $U$ , причем так, что для подгруппы  $V$ , покрывающей  $C$ ,  $[V : C] = p_r$ . Аналогично тому, как доказывалось, что  $S(p_r) \triangleleft G$ , можно установить, что подгруппа  $V$  обладает инвариантной подгруппой  $R$  порядка  $p_r$ .  $R$  содержится в подгруппе  $Z$ , являющейся единственной силовской  $p_r$ -подгруппой группы  $U$ . Подгруппа  $C$  принадлежит нормализатору подгруппы  $R$ ;  $S(p_r)$  также принадлежит ему, так как  $R$  содержится в центре подгруппы  $S(p_r)$ . Следовательно,  $R \triangleleft G$ . Так как группа  $G$  содержит инвариантную подгруппу  $R$  простого порядка  $p_r$  и, по предположению индукции, фактор-группа  $G/R$  сверхразрешима, группа  $G$  сверхразрешима. Доказательство теоремы окончено.

## Г л а в а 20

### ТЕОРИЯ ГРУПП И ПРОЕКТИВНЫЕ ПЛОСКОСТИ

#### 20.1. Аксиомы

*Проективная плоскость* — это множество точек, определенные подмножества которого называются прямыми и которое удовлетворяет следующим аксиомам:

P1. *Две произвольные различные точки лежат на одной и только на одной прямой.*

P2. *Две произвольные различные прямые пересекаются в одной и только одной точке.*

P3. *Существуют четыре точки, никакие три из которых не лежат на одной прямой.*

Однозначно определенную прямую  $k$ , содержащую две различные точки  $A$  и  $B$ , будем называть *прямой, соединяющей точки  $A$  и  $B$* . Однозначно определенную точку  $P$ , лежащую одновременно на двух различных прямых  $k$  и  $t$ , будем называть *пересечением прямых  $k$  и  $t$* .

Пусть  $A_1, A_2, A_3, A_4$  — четыре точки, никакие три из которых не лежат на одной прямой (существование такой четверки точек обеспечивается аксиомой P3). Этим точкам соответствуют шесть различных прямых, соединяющих их попарно:

$$L_1 : A_1A_2B_1,$$

$$L_2 : A_1A_3B_2,$$

$$L_3 : A_1A_4B_3,$$

$$L_4 : A_2A_3B_3,$$

$$L_5 : A_2A_4B_2,$$

$$L_6 : A_3A_4B_1.$$

Здесь  $B_1, B_2, B_3$  — точки пересечения этих прямых. Из того, что все шесть прямых различны, легко получается, что все точки  $B_1, B_2, B_3$  различны и все они отличны от точек  $A_i$ .

**ЛЕММА 20.1.1.** *Каждая прямая содержит не менее трех точек.*

*Доказательство.* Каждая из прямых  $L_1, \dots, L_6$ , указанных выше, содержит по меньшей мере три точки. Если произвольная прямая  $L$  не содержит  $A_1$ , то она пересекается с прямыми  $L_1, L_2, L_3$  в трех различных точках. Если  $L$  не содержит  $A_2$ , то она

пересекает прямые  $L_1, L_4, L_5$  в трех различных точках. Если же прямая  $L$  содержит и  $A_1$ , и  $A_2$ , то  $L = L_1$ , но прямая  $L_1$  содержит, во всяком случае, три точки  $A_1, A_2, B_1$ .

**Лемма 20.1.2.** *Существуют четыре прямые, никакие три из которых не содержат общей точки.*

**Доказательство.** Такими прямыми являются, как мы видели, прямые  $L_1, L_2, L_5, L_6$ .

Если поменять местами слова „точка“ и „прямая“, „содержать“ и „лежать на“, то аксиома Р1 заменяется аксиомой Р2, и наоборот, а аксиома Р3 — леммой 20.1.2, и наоборот. Так мы приходим к *принципу двойственности*, точный смысл которого заключается в следующем. Если  $\pi$  — некоторая проективная плоскость, то существует плоскость  $\pi^*$ , *двойственная* первой. Она строится следующим образом.

Пусть  $\{P_i\}$  — множество точек плоскости  $\pi$ , а  $\{k_j\}$  — множество прямых на плоскости  $\pi$ . Тогда плоскость  $\pi^*$  состоит из прямых  $\{p_i\}$ , находящихся во взаимно однозначном соответствии с точками  $\{P_i\}$  плоскости  $\pi$ , и из точек  $\{K_j\}$ , находящихся во взаимно однозначном соответствии с прямыми  $\{k_j\}$  плоскости  $\pi$ . При этом если  $P_i \in k_j$  в плоскости  $\pi$ , то мы считаем, что  $K_j \in p_i$  в плоскости  $\pi^*$ , где точка  $K_j$  соответствует прямой  $k_j$ , а  $p_i$  — прямая, соответствующая точке  $P_i$ . Ясно, что из выполнимости аксиом проективной плоскости для некоторого множества точек  $\pi$  следует справедливость этих аксиом для множества  $\pi^*$ . Далее, плоскостью, двойственной к  $\pi^*$ , является плоскость  $\pi$ , т. е.  $(\pi^*)^* = \pi$ . Следовательно, меняя местами понятия точки и прямой и заменяя знак включения обратным, мы любое утверждение о плоскости  $\pi$  превращаем в утверждение о двойственной ей плоскости  $\pi^*$ . Это и есть *принцип двойственности*. В частности, из принципа двойственности следует, что если некоторое утверждение справедливо для произвольной проективной плоскости  $\pi$ , то двойственное ему утверждение также справедливо. Так, применив принцип двойственности к лемме 20.1.1, получаем лемму.

**Лемма 20.1.3.** *Каждая точка принадлежит самое меньшее трем прямым.*

Читатель без труда убедится в том, что аксиомы Р1, Р2, Р3 проективной плоскости эквивалентны аксиомам проективной геометрии, приведенным в книге Веблена и Юнга „Проективная геометрия“<sup>1)</sup>.

Предположим, что некоторая прямая  $L_1$  проективной плоскости  $\pi$  содержит конечное число точек, а именно  $n+1$ , где, в силу леммы 20.1.1,  $n \geqslant 2$ . Согласно аксиоме Р3, существует по меньшей мере две точки, скажем,  $P_3$  и  $P_4$ , не лежащие на прямой  $L_1$ .

<sup>1)</sup> Веблен, Юнг [1], т. I, стр. 16—18.

Пусть прямая  $P_3P_4$  пересекает  $L_1$  в точке  $B_1$ , и пусть  $P_1, P_2$  — две другие точки прямой  $L_1$ . Тогда прямые  $P_1P_3$  и  $P_2P_4$  пересекаются в новой точке  $B_2$ , не лежащей ни на  $L_1$ , ни на  $P_1P_2$ . Если  $P$  — произвольная точка, не лежащая на  $L_1$ , то, соединяя  $P$  с  $n+1$  точками прямой  $L_1$ , мы получаем  $n+1$  прямых, проходящих через  $P$ , причем никакая другая прямая точку  $P$  не содержит, так как всякая прямая, проходящая через  $P$ , должна пересекать  $L_1$ . В частности,  $n+1$  прямых проходят через каждую из точек  $P_3, P_4$  и  $B_2$ . Так как через точку  $P$  проходят только  $n+1$  прямых, они пересекают произвольную прямую  $L$ , не содержащую  $P$ , в  $n+1$  точках, причем других точек прямая  $L$  не содержит. Поэтому произвольная прямая  $L$  плоскости  $\pi$  содержит ровно  $n+1$  точек, так как по крайней мере одна из точек  $P_3, P_4, B_2$  не лежит на прямой  $L$ . Кроме того, через произвольную точку  $P$  плоскости  $\pi$  проходит  $n+1$  прямых, а именно прямые, соединяющие точку  $P$  с  $n+1$  точками некоторой прямой  $L$ , не содержащей точку  $P$ . Этим мы доказали основную часть следующей теоремы.

**Теорема 20.1.1.** *Пусть  $n \geq 2$  — произвольное целое число. Следующие свойства проективной плоскости эквивалентны:*

- 1) некоторая прямая содержит точно  $n+1$  точек;
- 2) некоторая точка принадлежит точно  $n+1$  прямым;
- 3) каждая прямая содержит точно  $n+1$  точек;
- 4) каждая точка лежит точно на  $n+1$  прямых;
- 5) в плоскости  $\pi$  ровно  $n^2+n+1$  точек;
- 6) в плоскости  $\pi$  ровно  $n^2+n+1$  прямых.

*Доказательство.* Мы уже показали, что из (1) следуют свойства (2), (3) и (4). Докажем свойство (5), исходя из (1). Пусть  $P_0$  — некоторая точка плоскости  $\pi$ , и пусть  $L_1, \dots, L_{n+1}$  —  $n+1$  прямых, проходящих через  $P_0$ . Эти прямые содержат все точки плоскости  $\pi$ , причем каждая из них содержит  $P_0$  и  $n$  других точек.  $P_0$  — единственная точка, принадлежащая любым двум из прямых  $L_1, \dots, L_{n+1}$ . Следовательно, плоскость  $\pi$  содержит  $1 + (n+1)n = n^2 + n + 1$  точек. Установим теперь свойство (6). Пусть  $L_0$  — некоторая прямая плоскости  $\pi$ , и пусть  $P_1, \dots, P_{n+1}$  —  $n+1$  точек этой прямой. Каждая из этих точек лежит на  $L_0$  и на  $n$  других прямых. Таким способом мы получаем все прямые плоскости  $\pi$ ; их, следовательно,  $1 + (n+1)n = n^2 + n + 1$ . Итак, из свойства (1) вытекают все остальные. В силу двойственности из (2) также следуют все остальные свойства. Очевидно, что из (3) следует (1), а из (4) — (2). Если справедливо утверждение (5) и некоторая прямая состоит из  $m+1$  точек, где  $m$  — натуральное число, то плоскость  $\pi$  состоит из  $m^2+m+1=n^2+n+1$  точек, откуда  $m=n$ , т. е. из (5) следует (1). Аналогично из (6) следует (2).

## 20.2. Коллинеации и теорема Дезарга<sup>1)</sup>

Говорят, что плоскость  $\pi_1$  изоморфна плоскости  $\pi_2$ , если существует взаимно однозначное соответствие  $P_1 \xrightarrow{\alpha} P_2 = (P_1)\alpha$  между точками  $\{P_1\}$  плоскости  $\pi_1$  и точками  $\{P_2\}$  плоскости  $\pi_2$  и взаимно однозначное соответствие  $k_1 \xrightarrow{\beta} k_2 = (k_1)\beta$  между прямыми  $\{k_1\}$  плоскости  $\pi_1$  и прямыми  $\{k_2\}$  плоскости  $\pi_2$  такие, что из отношения  $P_1 \in k_1$  следует отношение  $(P_1)\alpha \in (k_1)\beta$ . Очевидно, что каждое из соответствий  $\alpha$  и  $\beta$  вполне определяет другое, и взаимно однозначное соответствие  $P_1 \xrightarrow{\alpha} (P_1)\alpha$  точек определяет изоморфизм плоскостей, если из того, что три точки  $P_1, Q_1, R_1$  плоскости  $\pi_1$  лежат на одной прямой, следует, что точки  $(P_1)\alpha, (Q_1)\alpha$  и  $(R_1)\alpha$  также лежат на одной прямой. Аналогично взаимно однозначное соответствие  $\beta$  прямых определяет изоморфизм, если любая тройка пересекающихся в одной точке прямых отображается на тройку прямых, также пересекающихся в одной точке. Можно было бы определить гомоморфизм плоскостей как однозначное (но не взаимно однозначное) соответствие между точками и прямыми, сохраняющее отношение инцидентности, но для плоскостей это не такое важное понятие, как для других объектов.

Изоморфизм  $\alpha$  плоскости  $\pi$  на себя называется *коллинеацией*. Коллинеации плоскости образуют группу.

Плоскость  $\pi_1$ , которую можно погрузить в трехмерное пространство  $E_3$ , всегда обладает большим числом коллинеаций. Пусть  $\pi_2$  — другая плоскость в пространстве  $E_3$ , и пусть  $L$  — прямая пересечения плоскостей  $\pi_1$  и  $\pi_2$ . Выберем две произвольные точки  $P_1$  и  $P_2$  пространства  $E_3$ , не принадлежащие ни  $\pi_1$ , ни  $\pi_2$ . Определим *перспективную коллинеацию* плоскостей  $\pi_1$  и  $\pi_2$  с центром  $P_1$  как отображение произвольной точки  $Q$  плоскости  $\pi_1$  в точку  $R$  плоскости  $\pi_2$ , где  $R$  — точка пересечения плоскости  $\pi_2$  с прямой  $P_1Q$ , и будем записывать

$$Q \xrightarrow{P_1} R. \quad (20.2.1)$$

При этом  $P_1QR$  — прямая,  $Q \in \pi_1$ ,  $R \in \pi_2$ . Перспективная коллинеация (20.2.1) определяет изоморфное отображение плоскости  $\pi_1$  на  $\pi_2$ , так как, если  $M_1$  — прямая на плоскости  $\pi_1$ , плоскость  $\pi_3$ , содержащая  $M_1$  и  $P_1$ , пересекает  $\pi_2$  по прямой  $M_2$ , и потому перспективная коллинеация отображает точки прямой  $M_1$  в точки прямой  $M_2$ . Далее, любая точка прямой  $L$  отображается на себя, так как  $L$  — прямая пересечения  $\pi_1$  и  $\pi_2$ . Перспективная коллинеация плоскости  $\pi_2$  на плоскость  $\pi_1$  с центром  $P_2$

$$R \xrightarrow{P_2} S \quad (20.2.2)$$

<sup>1)</sup> Об используемых здесь свойствах трехмерных пространств см. Веблен и Юнг [1], стр. 20—25.

также является изоморфизмом  $\pi_2$  на  $\pi_1$ , отображающим все точки прямой  $L$  на себя. Последовательное применение этих двух перспективных коллинеаций

$$Q \xrightarrow{P_1} R \xrightarrow{P_2} S \quad (20.2.3)$$

является коллинеацией  $\alpha$  плоскости  $\pi_1$ , оставляющей на месте все точки прямой  $L$ . Пусть далее  $O$  — точка пересечения прямой  $P_1P_2$  с плоскостью  $\pi_1$  и  $T$  — точка пересечения  $P_1P_2$  с плоскостью  $\pi_2$ . Тогда

$$O \xrightarrow{P_1} T \xrightarrow{P_2} O, \quad (20.2.4)$$

т. е.  $P_1P_2OT$  — прямая, откуда  $(O)\alpha = O$ . Далее, пусть  $k$  — некоторая прямая, проходящая через точку  $O$ . Если прямая  $k$  проходит через некоторую точку  $Q$ , то точка  $R$  [см. отображение (20.2.3)] принадлежит плоскости  $\pi_4$ , содержащей пересекающиеся прямые  $k$  и  $P_1P_2OT$ , откуда точка  $S$  в (20.2.3) также лежит в плоскости  $\pi_4$  и, следовательно, на прямой  $k$ . Таким образом, соответствие  $\alpha$  отображает любую прямую, проходящую через точку  $O$ , в себя. Такая коллинеация называется *перспективной* и иногда *перспективой*. Прямая  $L$ , все точки которой остаются на месте под действием коллинеаций  $\alpha$ , называется *осью* перспективы, а точка  $O$  называется *центром* перспективной коллинеации, если любая проходящая через нее прямая отображается на себя. Центр  $O$  может лежать, а может и не лежать на прямой  $L$ . Чтобы различать эти два случая, перспективу будем называть *элацией*, если центр  $O$  лежит на оси  $L$ , и *гомологией*, если  $O$  не лежит на оси  $L$ . Сущность перспективной коллинеации видна из рис. 9.

Пусть  $\alpha$  — перспективная коллинеация с центром  $O$  и осью  $L$ , и пусть  $A_1$  — точка на плоскости  $\pi$ , не лежащая на прямой  $L$  и отличная от  $O$ . Тогда точка  $(A_1)\alpha = A_2$  должна находиться на прямой  $OA_1$ . Теперь в нашем распоряжении  $O$ ,  $L$ ,  $A_1$  и  $A_2$ , причем точки  $O$ ,  $A_1$ ,  $A_2$  лежат на одной прямой и ни одна из точек  $A_1$ ,  $A_2$  не лежит на прямой  $L$  и не совпадает с  $O$ . Утверждаем, что центром  $O$ , осью  $L$  и отображением  $(A_1)\alpha = A_2$  коллинеация  $\alpha$  вполне определена. Действительно, пусть  $B_1$  — произвольная точка плоскости  $\pi$ , не лежащая на прямых  $OA_1A_2$  и  $L$ . Пусть  $A_1B_1$  пересекает  $L$  в точке  $C_3$ . Тогда  $(B_1)\alpha$  лежит на прямой  $OB_1$ . Кроме того, в силу коллинеарности точек  $A_1$ ,  $B_1$ ,  $C_3$ , точки

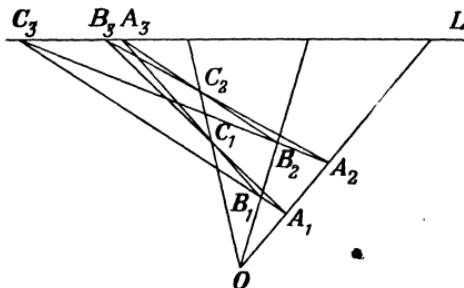


Рис. 9. Теорема Дезарга.

$(A_1)\alpha = A_2$ ,  $(B_1)\alpha$  и  $(C_3)\alpha = C_3$  также должны быть коллинеарными. Поэтому точка  $(B_1)\alpha$  должна лежать одновременно на прямых  $OB_1$  и  $C_3A_2$ , откуда точка  $(B_1)\alpha = B_2$  является пересечением прямых  $OB_1$  и  $C_3A_2$ . Таким образом, условием  $(A_1)\alpha = A_2$  образ произвольной точки  $B_1$ , не лежащей на  $OA_1A_2$ , однозначно определен. В свою очередь условием  $(B_1)\alpha = B_2$  образы точек прямой  $OA_1A_2$  однозначно определены.

Пусть теперь  $C_1$  — точка, не лежащая ни на прямой  $OA_1A_2$ , ни на прямой  $OB_1B_2$ , и прямая  $B_1C_1$  пересекает  $L$  в точке  $A_3$ , а  $A_1C_1$  — в точке  $B_3$ . Тогда точка  $(C_1)\alpha = C_2$  определяется как пересечение прямых  $A_2B_3$  и  $OC_1$ . Но, так как точки  $B_1$ ,  $C_1$ ,  $A_3$  лежат на одной прямой, точки  $(B_1)\alpha = B_2$ ,  $(C_1)\alpha = C_2$  и  $(A_3)\alpha = A_3$  также лежат на одной прямой. Выполняя описанное построение, мы получаем фигуру, называемую *конфигурацией Дезарга*. Утверждение о существовании этой конфигурации называется теоремой Дезарга. Будем говорить, что треугольники  $A_1B_1C_1$  и  $A_2B_2C_2$  *перспективны* относительно центра  $O$ , если соответствующие вершины лежат на прямой, проходящей через точку  $O$ , т. е. если  $OA_1A_2$ ,  $OB_1B_2$  и  $OC_1C_2$  — прямые. Треугольники перспективны относительно оси  $L$ , если соответствующие стороны пересекаются в точках прямой  $L$ .

**Теорема 20.2.1.** (Теорема Дезарга.) *Если два треугольника  $A_1B_1C_1$  и  $A_2B_2C_2$  перспективны относительно центра  $O$ , то соответствующие стороны  $A_1B_1$  и  $A_2B_2$ ,  $A_1C_1$  и  $A_2C_2$ ,  $B_1C_1$  и  $B_2C_2$  пересекаются в точках  $C_3$ ,  $B_3$  и  $A_3$ , лежащих на прямой  $L$ .*

Выполнимость теоремы Дезарга на плоскости  $\pi$  равносильна существованию всевозможных перспективных коллинеаций в  $\pi$ . Это видно из следующей теоремы.

**Теорема 20.2.2.** *Пусть на плоскости  $\pi$  дана некоторая прямая  $L$ , точка  $O$  и две точки  $A_1$ ,  $A_2$ , отличные от  $O$ , не лежащие на  $L$  и такие, что  $OA_1A_2$  — прямая. Тогда существует не более одной перспективной коллинеации  $\alpha$  плоскости  $\pi$  с центром  $O$ , осью  $L$  и такой, что  $(A_1)\alpha = A_2$ . Если плоскость  $\pi$  может быть погружена в трехмерное пространство, то такая перспективная коллинеация существует в действительности.*

**Доказательство.** Как мы видели, задание центра  $O$ , оси  $L$  и отображения  $(A_1)\alpha = A_2$  при условии, что точки  $O$ ,  $A_1$ ,  $A_2$  лежат на одной прямой, однозначно определяет перспективную коллинеацию  $\alpha$ . Следовательно, существует не более одной такой коллинеации. Предположим теперь, что плоскость  $\pi$  можно погрузить в трехмерное пространство  $E_3$ . Выберем в пространстве  $E_3$  плоскость  $\pi_2$ , пересекающуюся с  $\pi$  по прямой  $L$ , и выберем некоторую точку  $P_1$  пространства  $E_3$ , не лежащую в плоскостях  $\pi$  и  $\pi_2$ .

Соединим  $P_1$  с  $O$ . Пусть прямая  $P_1O$  пересекает плоскость  $\pi_2$  в точке  $T$  (рис. 10).

Если  $A_1P_1$  пересекает  $\pi_2$  в точке  $Q$ , то  $Q$  и  $A_2$  лежат в плоскости  $\pi_3$  прямых  $OP_1$  и  $OA_1A_2$ .  $\pi_3$  — плоскость рисунка. Поэтому  $A_2Q$  пересекает  $OP_1$  в точке  $P_2$ .  $P_2$  не лежит в плоскости  $\pi_2$ , так как в противном случае она совпадала бы с  $T$  и точка  $A_2$  совпадала бы с точкой  $X$  пересечения прямых  $OA_1A_2$  и  $L$ , что противоречит тому, что, по предположению, точка  $A_2$  не принадлежит прямой  $L$ . Аналогично, так как точки  $A_2$  и  $O$  различны, точка  $P_2$  не лежит в плоскости  $\pi_1$ . Как мы теперь видим, прямая  $L$  является осью, а точка  $O$  — центром перспективной коллинеации  $\alpha$ .

$$\pi \xrightarrow{P_1} \pi_2 \xrightarrow{P_2} \pi,$$

причем  $A_1 \xrightarrow{P_1} Q \xrightarrow{P_2} A_2$ . Поэтому  $A_2 = (A_1)\alpha$ , и искомая коллинеация действительно существует.

**Теорема 20.2.3.** Теорема Дезарга справедлива в плоскости  $\pi$  тогда и только тогда, когда в плоскости  $\pi$  все возможные перспективные коллинеации существуют.

**Следствие 20.2.1.** Теорема Дезарга справедлива в любой плоскости  $\pi$ , которую можно погрузить в проективное трехмерное пространство.

*Доказательство.* Если докажем теорему, то следствие будет вытекать из предыдущей теоремы. Поэтому докажем лишь эту теорему.

Предположим сначала, что все возможные перспективные коллинеации плоскости  $\pi$  существуют. Рассмотрим два таких треугольника  $A_1B_1C_1$  и  $A_2B_2C_2$ , что три прямые  $A_1A_2$ ,  $B_1B_2$  и  $C_1C_2$  пересекаются в точке  $O$  (см. рис. 9). Пусть прямые  $A_1B_1$  и  $A_2B_2$  пересекаются в точке  $C_3$ , а прямые  $A_1C_1$  и  $A_2C_2$  — в точке  $B_3$ . Прямую, соединяющую точки  $B_3$  и  $C_3$ , обозначим через  $L$ . Тогда, по нашему предположению, существует перспективная коллинеация  $\alpha$  с центром  $O$ , осью  $L$  и такая, что  $(A_1)\alpha = A_2$ . Тогда по построению  $(B_1)\alpha = B_2$  и  $(C_1)\alpha = C_2$ . Пусть прямая  $B_1C_1$  пересекается с  $L$  в точке  $A_3$ . Тогда точки  $(B_1)\alpha = B_2$ ,  $(C_1)\alpha = C_2$  и  $(A_3)\alpha = A_3$  лежат на одной прямой, откуда  $A_3$ , точка пересечения прямых  $B_1C_1$  и  $B_2C_2$ , лежит на прямой  $L$ , как и точки  $B_3$ ,  $C_3$ . Этим справедливость теоремы Дезарга установлена.

Обратно, предположим теперь, что теорема Дезарга имеет место в плоскости  $\pi$ . Пусть  $L$  — прямая,  $O, A_1, A_2$  — различные

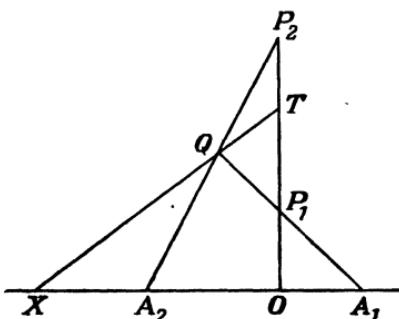


Рис. 10. Перспективность.

точки одной прямой, причем точки  $A_1$  и  $A_2$  не лежат на прямой  $L$  (хотя  $L$  может проходить через  $O$ ). Определим отображение  $\alpha$  точек плоскости  $\pi$  и покажем, что это коллинеация. При этом будем обращаться к рис. 9, иллюстрирующему теорему Дезарга. Для любой точки  $X$  прямой  $L$  полагаем  $(X)\alpha = X$ ; кроме того, пусть  $(O)\alpha = O$  и  $(A_1)\alpha = A_2$ . Если точка  $B_1$  не лежит на прямых  $L$  и  $OA_1A_2$ , то пусть прямая  $A_1B_1$  пересекает  $L$  в точке  $C_3$ . Если  $A_2C_3$  пересекает  $OB_1$  в точке  $B_2$ , то полагаем  $(B_1)\alpha = B_2$ . Этим определяется отображение  $\alpha$  для всех точек плоскости  $\pi$ , кроме точек прямой  $OA_1A_2$ . Далее, если  $A_1C_1$  пересекает  $L$  в точке  $B_3$  и если  $A_2A_3$  пересекает  $OC_1$  в точке  $C_2$ , то полагаем  $C_2 = (C_1)\alpha$ . Если  $OA_1$ ,  $OB_1$  и  $OC_1$  — различные прямые, то треугольники  $A_1B_1C_1$  и  $A_2B_2C_2$  перспективны относительно центра  $O$ , и, согласно теореме Дезарга, соответствующие стороны пересекаются в точках одной прямой. Но точки  $C_3$  и  $B_3$  принадлежат прямой  $L$ , откуда прямые  $B_1C_1$  и  $B_2C_2$  пересекаются в точке  $A_3$  прямой  $L$ . Если бы мы исходили из отображения  $(B_1)\beta = B_2$ , то мы бы определили точку  $(C_1)\beta$  как пересечение прямых  $B_2A_3$  и  $OC_1$ . Но это точка  $C_2$ , и, следовательно, мы получаем равенства  $(C_1)\alpha = (C_1)\beta = C_2$  как вывод или из условия  $(A_1)\alpha = A_2$ , или из условия  $(B_1)\beta = B_2$ . Таким образом, отображения  $\alpha$  и  $\beta$  совпадают на всех таких прямых  $OC_1C_2$ , для которых они определены. Но отображение  $\alpha$  определено на всех прямых  $OB_1B_2$ , а  $\beta$  — на всех прямых  $OA_1A_2$ . Таким образом, отображение  $\alpha$  определено для всех точек плоскости  $\pi$ .

Снова обращаемся к рис. 9. Пусть  $(A_1)\alpha = A_2$ ,  $k$  — произвольная прямая, не проходящая ни через  $O$ , ни через  $A_1$ . Пусть  $k$  пересекает  $L$  в точке  $A_3$ , и пусть  $B_1$ ,  $C_1$  — две другие точки прямой  $k$ . Пусть также  $(B_1)\alpha = B_2$ ,  $(C_1)\alpha = C_2$  и  $(A_3)\alpha = A_3$ . Тогда, применяя теорему Дезарга к треугольникам  $A_1B_1C_1$  и  $A_2B_2C_2$ , мы получаем, что точки  $B_2$ ,  $C_2$  и  $A_3$  лежат на одной прямой. Это обстоятельство говорит нам о том, что отображение  $\alpha$  переводит точки  $C_1$  прямой  $k = A_3B_1$  в точки прямой  $A_3B_2$ , за исключением, возможно, случая, когда  $C_1$  — точка пересечения прямых  $A_3B_1$  и  $OA_1A_2$ . Но если  $C_1 = D_1$  — пересечение прямых  $B_1A_3$  и  $OA_1A_2$ , то из равенств  $(B_1)\alpha = (B_1)\beta = B_2$  мы определяем образ  $(D_1)\beta = D_2$  как пересечение  $D_2$  прямых  $A_3B_2$  и  $OA_1A_2$ . Следовательно, отображение  $\alpha$  переводит все точки прямой  $k$  в точки прямой  $A_3B_2$ . Понятно, что оно переводит прямую  $L$  в себя так же, как и прямые, проходящие через точку  $O$ . Поэтому отображение  $\alpha$  является искомой коллинеацией.

На самом деле мы доказали несколько более точный результат, чем теорема 20.2.3. Сформулируем его как теорему.

**Теорема 20.2.4.** *Плоскость  $\pi$  обладает всеми возможными перспективными коллинеациями с данным центром  $O$  и дан-*

ной осью  $L$  тогда и только тогда, когда справедлива теорема Дезарга для всех треугольников, перспективных относительно точки  $O$  и таких, что две пары соответствующих сторон пересекаются на прямой  $L$  (отсюда следует, что и точка пересечения третьей пары соответствующих сторон находится на прямой  $L$ ).

Не всякая плоскость  $\pi$  может быть погружена в трехмерное пространство, а также возможны случаи, когда теорема 20.2.4 применима только для некоторого ограниченного числа осей  $L$  и центров  $O$ .

### 20.3. Введение координат

Пусть  $\pi$  — произвольная проективная плоскость;  $X, Y, O, I$  — четыре точки, никакие три из которых не лежат на одной прямой. Назовем прямую  $XY$  бесконечно удаленной прямой  $L_\infty$ , а прямую  $OI$  — прямой  $y = x$ .

На прямой  $OI$  приписываем координаты  $(0, 0)$  точке  $O$ ,  $(1, 1)$  точке  $I$  и единственную координату  $(1)$  точке  $C$  пересечения прямых  $OI$  и  $XY$ . Другим точкам прямой  $OI$  приписываем координаты  $(b, b)$ , где  $b$  — символы, различные для различных точек. Пусть теперь  $P$  — точка, не принадлежащая прямой  $L_\infty$ , и пусть  $XP$  пересекает  $OI$  в точке  $(b, b)$ , а  $YP$  — в точке  $(a, a)$ . Тогда приписываем точке  $P$  координаты  $(a, b)$ . По этому правилу точкам прямой  $OI$  приписываются прежние координаты. Пусть прямая, соединяющая точки  $(0, 0)$  и  $(1, m)$ , пересекает  $L$  в некоторой точке  $M$ . Припишем точке  $M$  единственную координату  $(m)$ , которую можно представлять себе как характеризующую наклон. Итак, мы приписали координаты каждой точке плоскости, кроме точки  $Y$ . Ей мы приписываем в качестве координаты символ  $(\infty)$ .

Воспользуемся прямыми, отмеченными на рис. 11, для определения алгебраических операций на системе координат. Эта алгебраическая система будет так называемым *тернарным кольцом*, и для любой прямой плоскости  $\pi$ , кроме  $L_\infty$ , получим уравнение, выражаемое в терминах операций этого тернарного кольца. Если  $(x, y)$  — конечная точка прямой  $OI$ , то  $x = y$ , и поэтому равен-

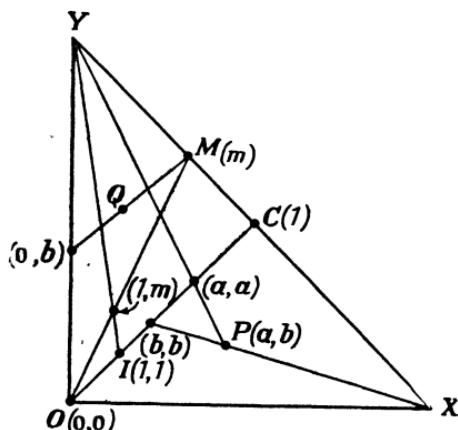


Рис. 11. Введение координат.

ство  $y = x$  мы считаем уравнением прямой  $OI$ . Прямая, проходящая через точку  $Y$  и отличная от  $L_\infty$ , имеет то свойство, что все ее конечные точки  $(x, y)$  имеют одну и ту же координату  $x$ , скажем  $x = c$ ; это равенство будем считать уравнением этой прямой.

Если  $(x, y)$  — конечная точка прямой, соединяющей точки  $C = (1)$  и  $(0, b)$ , то мы определяем бинарную операцию сложения, полагая

$$y = x + b. \quad (20.3.1)$$

Будем называть равенство (20.3.1) уравнением этой прямой. Если  $(x, y)$  — конечная точка прямой, соединяющей  $O(0, 0)$  и  $(m)$ , определим бинарную операцию умножения, полагая

$$y = xm, \quad (20.3.2)$$

и рассмотрим это равенство как уравнение последней прямой. В общем случае произвольная прямая, не проходящая через точку  $Y$ , пересекает  $L_\infty$  в некоторой точке  $(m)$  и  $OY$  — в некоторой точке  $(0, b)$ . Если  $Q = (x, y)$  — произвольная точка этой прямой, то мы определяем тернарную операцию

$$y = x \cdot m \circ b. \quad (20.3.3)$$

Это равенство принимаем за уравнение этой прямой. Сложение и умножение, введенные выше, являются частными случаями тернарной операции, и мы видим, что

$$\begin{aligned} x + b &= x \cdot 1 \circ b, \\ xm &= x \cdot m \circ 0. \end{aligned} \quad (20.3.4)$$

Элементы  $0$  и  $1$  обладают известными свойствами:

$$\begin{aligned} 0 + a &= a + 0 = a, \\ 0m &= m0 = 0, \\ 1m &= m1 = m. \end{aligned} \quad (20.3.5)$$

Плоскость  $\pi$  можно представить как тернарное кольцо  $R$ , тернарная операция которого обладает определенными свойствами, и обратно, тернарное кольцо с такими же свойствами однозначно определяет плоскость. Сформулируем этот факт как основную теорему о тернарных кольцах.

**Теорема 20.3.1.** *Произвольный выбор четырех точек  $X, Y, O, I$ , никакие три из которых не лежат на одной прямой плоскости  $\pi$ , определяет тернарное кольцо  $R$ . Среди элементов этого кольца есть нуль  $0$  и единица  $1 \neq 0$ . Тернарная операция  $x \cdot m \circ b$  удовлетворяет следующим требованиям:*

T1.  $0 \cdot m \circ c = a \cdot 0 \circ c = c$ .

T2.  $1 \cdot m \circ 0 = m \cdot 1 \circ 0 = m$ .

T3. При заданных  $a, m, c$  существует точно только один такой элемент  $z$ , что  $a \cdot m \circ z = c$ .

T4. Если  $m_1, m_2$  ( $m_1 \neq m_2$ ),  $b_1, b_2$  — данные элементы, то существует такой единственный элемент  $x$ , что

$$x \cdot m_1 \circ b_1 = x \cdot m_2 \circ b_2.$$

T5. Если заданы элементы  $a_1, a_2$  ( $a_1 \neq a_2$ ),  $c_1, c_2$ , то существует такая единственная пара элементов  $m, b$ , что

$$a_1 \cdot m \circ b = c_1 \text{ и } a_2 \cdot m \circ b = c_2.$$

*Доказательство.* Выбрав четыре точки  $X, Y, O, I$ , никакие три из которых не лежат на одной прямой плоскости  $\pi$ , мы образуем тернарное кольцо с операцией  $x \cdot m \circ b$  так, как это делалось выше. Свойства T1 и T2 немедленно следуют из определения. Свойство T3 означает, что прямая, соединяющая точки  $(m)$  и  $(a, c)$ , пересекает  $OY$  во вполне определенной точке  $(0, z)$ . Смысл требования T4 заключается в том, что две прямые  $y = x \cdot m_1 \circ b_1$  и  $y = x \cdot m_2 \circ b_2$  с различными направлениями  $m_1$  и  $m_2$  пересекаются в одной-единственной конечной точке. Требование T5 говорит о том, что если  $(a_1, c_1)$  и  $(a_2, c_2)$  — две конечные точки при  $a_1 \neq a_2$ , то существует одна-единственная прямая  $y = x \cdot m \circ b$ , проходящая через эти две точки.

Обратно, пусть  $R$  — тернарное кольцо со свойствами T1—T5. Образуем конечные точки  $(a, b)$  и бесконечные точки  $(m)$  и  $(\infty)$ , где  $a, b, m$  — все возможные элементы кольца  $R$ . Прямую  $L_\infty$  определяем как множество всех бесконечных точек  $(m)$ ,  $(\infty)$  и никаких других. Все точки  $(c, y)$  при фиксированном  $c$  и точка  $(\infty)$  образуют прямую  $x = c$ . Точка  $(m)$  и такие точки  $(x, y)$ , что  $y = x \cdot m \circ b$  при фиксированных элементах  $m$  и  $b$ , образуют прямую  $y = x \cdot m \circ b$ . Проверка того, что полученная система точек и прямых составляет проективную плоскость, требует рассмотрения нескольких случаев, но конечным следствием аксиом рассматриваемого кольца, как нетрудно заметить, является то, что две различные точки лежат на одной-единственной прямой, а две различные прямые пересекаются в одной-единственной точке. Кроме того, четыре точки  $(\infty), (0), (0, 0)$  и  $(1, 1)$  таковы, что никакие три из них не лежат на одной прямой. Так как проверки этих утверждений аналогичны, мы сделаем только одну из них. Рассмотрим две различные прямые  $y = x \cdot m \circ b_1$  и  $y = x \cdot m \circ b_2$ . Обе они содержат единственную бесконечную точку  $(m)$ . Если бы они содержали также общую конечную точку  $(a, c)$ , то мы бы имели  $a \cdot m \circ b_1 = c = a \cdot m \circ b_2$ , что противоречит аксиоме T3, так как  $b_1 \neq b_2$ .

## 20.4. Системы Веблена — Веддербарна. Системы Холла

Исследуем свойства плоскостей с определенными группами коллинеаций и свяжем эти свойства с тернарными кольцами, определяющими координаты.

**Лемма 20.4.1.** *Коллинеация проективной плоскости  $\pi$ , оставляющая на месте каждую из точек двух различных прямых, является тождественной коллинеацией.*

*Доказательство.* Пусть коллинеация  $\alpha$  оставляет на месте все точки прямых  $L_1$  и  $L_2$ , пересекающихся в точке  $Q$ . Пусть  $P$ —произвольная точка плоскости  $\pi$ , не лежащая ни на  $L_1$ , ни на  $L_2$ . Выберем на прямой  $L_1$  две точки  $R$  и  $S$ , отличные от  $Q$ . Пусть прямая  $PR$  пересекает  $L_2$  в точке  $T$ , а прямая  $PS$  пересекает  $L_2$  в точке  $U$ . Тогда  $R, S, T, U$  остаются на месте при коллинеации  $\alpha$ , и, следовательно, прямые  $RT$  и  $SU$  инвариантны относительно коллинеации  $\alpha$ . Поэтому точка их пересечения  $P$  под действием  $\alpha$  также остается на месте. Значит, не только точки прямых  $L_1$  и  $L_2$ , но и произвольная точка  $P$ , не лежащая на  $L_1$  и  $L_2$ , остается на месте при  $\alpha$ . Поэтому  $\alpha$ —тождественная коллинеация.

**Лемма 20.4.2.** *Коллинеация проективной плоскости, индуцирующая тождество на некоторой прямой и оставляющая на месте две точки, не лежащие на ней, — тождественная коллинеация.*

*Доказательство.* Пусть  $\alpha$ —коллинеация, оставляющая на месте точки прямой  $L$  и две точки  $P_1$  и  $P_2$ , не лежащие на  $L$ . Пусть  $P$ —произвольная точка плоскости, не принадлежащая ни прямой  $L$ , ни прямой  $P_1P_2$ . Пусть  $P_1P$  пересекает  $L$  в точке  $Q_1$ , а  $P_2P$  пересекает  $L$  в точке  $Q_2$ . Так как точка  $P$  не лежит на прямых  $P_1P_2$  и  $L$ , прямые  $P_1PQ_1$  и  $P_2PQ_2$  различные. Так как  $P_1, Q_1, P_2, Q_2$ —различные точки, оставляемые на месте коллинеацией  $\alpha$ , прямые  $P_1Q_1$  и  $P_2Q_2$  при действии  $\alpha$  отображаются на себя, значит, их пересечение  $P$  при  $\alpha$  также остается на месте. Поэтому  $\alpha$  действует тождественно в каждой точке прямой  $L$  и в каждой точке, находящейся вне прямой  $P_1P_2$ . Следовательно,  $\alpha$  отображает в себя точки прямой  $L$  и некоторой другой прямой, скажем  $P_1Q_1$ , проходящей через  $P_1$ , но отличной от  $P_1P_2$ . Применяя лемму 20.4.1, получаем, что  $\alpha$ —тождественная коллинеация.

Таким образом, коллинеация, индуцирующая тождество на некоторой прямой, может оставлять неподвижной не более одной точки вне этой прямой.

**Теорема 20.4.1.** *Пусть  $\alpha$ —коллинеация плоскости, оставляющая на месте некоторую прямую  $L$  и все точки на  $L$ . Тогда существует такая точка  $C$ , что  $\alpha$  оставляет на месте*

точку  $C$  и любую прямую, проходящую через  $C$ . Если коллинеация  $\alpha$  не тождественна, то она не оставляет на месте ни одной точки и прямой, кроме указанных. Двойственное предложение: если некоторая коллинеация  $\alpha$  оставляет на месте некоторую точку  $C$  и все прямые, проходящие через нее, то существует такая прямая  $L$ , что  $\alpha$  оставляет на месте все точки прямой  $L$ . Если при этом  $\alpha$  — нетождественная коллинеация, то она не оставляет на месте никаких других точек и прямых.

**Доказательство.** Пусть  $\alpha \neq 1$  — коллинеация плоскости  $\pi$ , оставляющая на месте каждую точку прямой  $L$ . Тогда, согласно лемме 20.4.2,  $\alpha$  оставляет на месте не более одной точки, не лежащей на прямой  $L$ . Предположим сначала, что  $\alpha$  оставляет на месте одну точку  $C$  вне прямой  $L$ . Тогда произвольная прямая, проходящая через  $C$ , пересекает  $L$  в некоторой точке  $Q$ , отличной от  $C$ , и, так как точки  $C$  и  $Q$  остаются неподвижными при  $\alpha$ , прямая  $CQ$  отображается при  $\alpha$  в себя. Поэтому любая прямая, проходящая через  $C$ , отображается на себя коллинеацией  $\alpha$ . Если бы существовала прямая  $L_2$ , инвариантная относительно  $\alpha$  и отличная от  $L$  и прямых, проходящих через точку  $C$ , то любая точка прямой  $L_2$  как пересечение  $L_2$  и некоторой прямой, проходящей через точку  $C$ , оставалась бы неподвижной при  $\alpha$ , и тогда в силу леммы 20.4.1 коллинеация  $\alpha$  была бы тождественной. Аналогично в силу леммы 20.4.2 не существует других точек, инвариантных относительно  $\alpha$ .

Предположим теперь, что  $\alpha$  оставляет неподвижными только точки прямой  $L$ . Пусть  $P$  — точка вне прямой  $L$ . Тогда точка  $P\alpha$ , образ точки  $P$  при  $\alpha$ , отлична от  $P$  и находится вне прямой  $L$ . Поэтому прямая  $M = PP\alpha$  пересекает  $L$  в точке  $C$ , отличной как от  $P$ , так и от  $P\alpha$ . Следовательно,  $M = PC$  и  $M\alpha = P\alpha C\alpha = P\alpha C$ . Но точки  $P$ ,  $P\alpha$ ,  $C$  лежат на одной прямой, и поэтому  $M = Ma$ . Таким образом, любая точка  $P$ , находящаяся вне  $L$ , лежит на некоторой инвариантной относительно  $\alpha$  прямой  $M$ . Кроме того, такая точка  $P$  не может находиться на двух различных неподвижных прямых, так как тогда она сама была бы инвариантной относительно  $\alpha$ . Если теперь  $M = PC$  — одна неподвижная относительно  $\alpha$  прямая, рассмотрим некоторую точку  $Q$  вне прямых  $L$  и  $M$ . Точка  $Q$  также принадлежит одной вполне определенной прямой  $N$ , инвариантной относительно  $\alpha$ . Поэтому пересечение прямых  $M$  и  $N$  — неподвижная точка, а, по предположению, все неподвижные точки лежат на прямой  $L$ . Следовательно, точка пересечения  $C$  прямых  $M$  и  $N$  принадлежит прямой  $L$ . Тогда каждая неподвижная относительно  $\alpha$  прямая проходит через точку  $C$ . Произвольная прямая  $K$ , проходящая через  $C$  и отличная от  $L$ , содержит точку, скажем,  $R$  вне прямой  $L$ . С другой стороны,  $R$  лежит на некоторой неподвижной относительно  $\alpha$  прямой,

проходящей через точку  $C$ , и, следовательно, эта неподвижная прямая совпадает с  $RC = K$ . Таким образом, любая прямая, проходящая через точку  $C$ , при отображении  $\alpha$  остается неподвижной. Если бы при этом опять-таки существовали неподвижные элементы, отличные от прямой  $L$ , ее точек, точки  $C$  и проходящих через нее прямых, то в силу лемм 20.4.1 и 20.4.2 коллинеация  $\alpha$  была бы тождественной. Остальные утверждения теоремы справедливы в силу принципа двойственности.

Коллинеации, о которых шла речь в этой теореме, — это перспективные коллинеации, рассмотренные в § 20.2. Они называются иногда *центральными коллинеациями*. Если хотят подчеркнуть, что коллинеация имеет центр  $C$  и ось  $L$ , то говорят о *C-L коллинеации*. Очевидно, что все коллинеации с центром  $C$  и осью  $L$  образуют группу. Как и в § 20.2, мы называем коллинеацию *элацией*, если центр  $C$  лежит на оси  $L$ , и *гомологией*, если центр  $C$  не лежит на  $L$ .

**Лемма 20.4.3.** *Центральная коллинеация  $\alpha$  полностью определяется ее центром  $C$ , осью  $L$  и парой соответственных точек  $P$  и  $P\alpha$ , причем точка  $P$  лежит вне  $L$  и отлична от  $C$ , а точки  $P$ ,  $P\alpha$  и  $C$  должны лежать на одной прямой.*

**Доказательство.** Если бы существовали две коллинеации  $\alpha_1$  и  $\alpha_2$  с центром  $C$ , осью  $L$  и такие, что  $P\alpha_1 = P\alpha_2$ , то коллинеация  $\alpha_1\alpha_2^{-1}$  оставляла бы неподвижными точки прямой  $L$ , центр  $C$  и точку  $P$ , откуда, согласно теореме 20.4.1,  $\alpha_1\alpha_2^{-1} = 1$ , т. е.  $\alpha_1 = \alpha_2$ . Лемма доказана.

**Теорема 20.4.2.** *Произведение двух элаций с общей осью  $L$ , но различными центрами  $C_1$  и  $C_2$  является элацией с осью  $L$  и центром  $C_3$ , отличным как от  $C_1$ , так и от  $C_2$ .*

**Доказательство.** Пусть  $\alpha_1$  — элация, имеющая центр  $C_1$  на оси  $L$ , а  $\alpha_2$  — элация, имеющая центр  $C_2 \neq C_1$  также на оси  $L$ . Тогда  $\alpha_1\alpha_2$  — коллинеация, оставляющая неподвижными все точки прямой  $L$ . По теореме 20.4.1  $\alpha_1\alpha_2 = \alpha_3$  — центральная коллинеация с осью  $L$ . Чтобы убедиться в том, что  $\alpha_3$  — элация, мы должны показать, что  $\alpha_3$  не оставляет на месте ни одной точки плоскости, лежащей вне  $L$ . Если  $P\alpha_3 = P$ , где  $P$  — точка, лежащая вне  $L$ , то  $P\alpha_1 = P\alpha_2^{-1}$ , причем точки  $C_1$ ,  $P$ ,  $P\alpha_1$  лежат на одной прямой, также как и точки  $C_2$ ,  $P$ ,  $P\alpha_2^{-1}$ . Но в силу равенства  $P\alpha_1 = P\alpha_2^{-1}$  эти две прямые совпадают, значит, и их пересечения с прямой  $L$  совпадают, т. е.  $C_1 = C_2$ , а это противоречит условию. Следовательно, коллинеация  $\alpha_3 = \alpha_1\alpha_2$  оставляет неподвижными только точки прямой  $L$ , значит, это элация, центр которой  $C_3$  лежит на оси  $L$ . Если бы  $C_3 = C_1$ , то элация  $\alpha_2 = \alpha_1^{-1}\alpha_3$  имела бы центр  $C_1$ , что противоречит условию. Поэтому  $C_3 \neq C_1$ , и аналогично  $C_3 \neq C_2$ .

Рассмотрим группу  $G = G(C, L)$   $C$ - $L$  центральных коллинеаций. Если  $P \neq C$  и  $P \notin L$ , то для любого  $\alpha \in G$  точки  $C, P, P\alpha$  лежат на одной прямой. Если для любой точки  $Q$  прямой  $CP$  при  $Q \neq C, Q \notin L$ , существует такой элемент  $\alpha \in G$ , что  $P\alpha = Q$ , то мы говорим, что плоскость  $\pi$   $C$ - $L$  транзитивна. Это означает, что все возможные  $C$ - $L$  коллинеации действительно существуют. Утверждение, что плоскость  $\pi$   $C$ - $L$  транзитивна, означает также, что для некоторой прямой  $M$ , отличной от  $L$  и проходящей через  $C$ ,  $C$ - $L$  коллинеации переставляют транзитивно все точки прямой  $M$ , кроме точки  $C$  и точки пересечения прямых  $M$  и  $L$ . Это утверждение справедливо для произвольной прямой  $M$ , отличной от  $L$  и содержащей точку  $C$ .

Согласно теореме 20.4.2, все элации, имеющие общую ось  $L$ , образуют группу  $G(L)$ , называемую группой трансляций с осью  $L$ .

**Теорема 20.4.3.** (Бэр [10].) *Если для двух различных центров  $C_1$  и  $C_2$  на оси  $L$  группы элаций  $G(C_1, L)$  и  $G(C_2, L)$  не являются единичными, то полная группа трансляций  $G(L)$  абелева. Кроме того, все отличные от единичного элементы группы  $G(L)$  имеют или (1) бесконечный порядок, или (2) один и тот же простой порядок  $p$ .*

*Доказательство.* Пусть  $\alpha_1$  и  $\alpha_2$  — элементы, отличные от единичных, из групп  $G(C_1, L)$  и  $G(C_2, L)$  соответственно. Пусть  $P$  — произвольная точка вне прямой  $L$ . Тогда в нашем распоряжении следующие прямые:

$$\begin{aligned} L_1 &: C_1 P P \alpha_1, \quad L_2 : C_2 P P \alpha_2, \\ L_1 \alpha_2 &: C_1 P \alpha_2 P (\alpha_1 \alpha_2), \quad L_2 \alpha_1 : C_2 P \alpha_1 P (\alpha_2 \alpha_1)^1. \end{aligned}$$

Точки  $C_2, P\alpha_1$  и  $(P\alpha_1)\alpha_2 = P(\alpha_1\alpha_2)$  лежат на одной прямой, и точки  $C_1, P\alpha_2, (P\alpha_2)\alpha_1 = P(\alpha_2\alpha_1)$  также лежат на одной прямой. Следовательно, пересечением различных прямых  $C_2 P \alpha_1$  и  $C_1 P \alpha_2$  является точка  $P(\alpha_1\alpha_2)$ , а также точка  $P(\alpha_2\alpha_1)$ . Отсюда  $P(\alpha_1\alpha_2) = P(\alpha_2\alpha_1)$  для произвольной точки  $P \notin L$ . Поэтому  $\alpha_1\alpha_2 = \alpha_2\alpha_1$ , т. е. произвольный элемент  $\alpha_1 \in G(C_1, L)$  перестановочен с любым элементом  $\alpha_2$  каждой группы  $G(C_2, L)$  при  $C_2 \neq C_1$ . Пусть  $\beta_1 \neq 1$  — другой элемент группы  $G(C_1, L)$ . Тогда  $\beta_1\alpha_2$  — элация, имеющая центр  $C_3 \neq C_1, C_2$ . Поэтому элемент  $\alpha_1$  перестановочен с элементом  $\beta_1\alpha_2$ , а так как элемент  $\alpha_1$  перестановочен с  $\alpha_2$ , то  $\alpha_1$  перестановочен с  $\beta_1$ . Итак, любой элемент  $\alpha_1 \neq 1$  группы  $G(C_1, L)$  перестановочен с любым элементом группы  $G(L)$ . Поэтому  $G(L)$  — абелева группа. Как показывают примеры, группа  $G(C_1, L)$  может и

<sup>1)</sup> Здесь  $P\alpha_1, P\alpha_2, P(\alpha_1\alpha_2), P(\alpha_2\alpha_1)$  — образы точки  $P$  при  $\alpha_1, \alpha_2, \alpha_1\alpha_2, \alpha_2\alpha_1$  соответственно. — Прим. ред.

не быть абелевой, если любая другая группа  $G(C_i, L)$  является единичной группой при  $C_i \in L$ .

Если порядок каждого элемента группы  $G(L)$  бесконечен, имеем случай (1). Если же группа  $G(L)$  содержит элементы конечного порядка, то существует элемент простого порядка, скажем  $\alpha_1 \in G(C_1, L)$ ,  $\alpha_1^p = 1$ . Теперь при  $\alpha_2 \neq 1 \in G(C_2, L)$ ,  $C_2 \neq C_1$ , имеем  $\alpha_1\alpha_2 = \alpha_3 \in G(C_3, L)$ ,  $C_3 \neq C_1, C_2$ . Тогда элемент  $(\alpha_1\alpha_2)^p = \alpha_2^p = \alpha_3^p$  принадлежит группам  $G(C_2, L)$  и  $G(C_3, L)$ , а значит, равен единице. Поэтому  $\alpha_2^p = 1$ . Аналогично из  $\alpha_2^p = 1$  следует равенство  $\beta_1^p = 1$  для любого  $\beta_1 \in G(C_1, L)$ . Итак, любой элемент группы  $G(L)$ , кроме единицы, в этом случае имеет порядок  $p$ .

**Теорема 20.4.4.** *Если плоскость  $\pi$   $C_1$ - $L$  транзитивна и  $C_2$ - $L$  транзитивна, где  $C_1 \neq C_2$  — центры на оси  $L$ , то плоскость  $\pi$   $C$ - $L$  транзитивна при любом центре  $C \in L$ .*

**Доказательство.** Выберем прямую  $M \neq L$ , проходящую через точку  $C \neq C_1, C_2$ . Пусть  $P$  и  $Q$  — две произвольные точки этой прямой, отличные от  $C$ . Пусть прямые  $PC_1$  и  $QC_2$  пересекаются в точке  $S$ . Выбираем теперь такой элемент  $\alpha_1 \in G(C_1, L)$ , что  $P\alpha_1 = S$ , и такой элемент  $\alpha_2 \in G(C_2, L)$ , что  $S\alpha_2 = Q$ . В силу  $C_1$ - $L$  и  $C_2$ - $L$  транзитивности такие  $\alpha_1$  и  $\alpha_2$  существуют. Тогда  $\alpha_1\alpha_2 = \alpha_3$  — элация, имеющая ось  $L$  и такая, что точки  $P, P\alpha_3 = Q$  и  $C$  лежат на одной прямой. Следовательно,  $\alpha_3 \in G(C, L)$  и плоскость  $\pi$   $C$ - $L$  транзитивна.

**Следствие 20.4.1.** *Если плоскость  $\pi$   $C_1$ - $L$  и  $C_2$ - $L$  транзитивна, причем  $C_1 \neq C_2$  — точки на  $L$ , то группа  $G(L)$  содержит все возможные элации, центры которых лежат на оси  $L$ .*

Если плоскость  $\pi$   $C$ - $L$  транзитивна при любом центре  $C \in L$ , то  $\pi$  называется *плоскостью трансляций* относительно оси  $L$ .

Каков смысл элаций в терминах свойств тернарного кольца, определяющего систему координат плоскости  $\pi$ ? Рассмотрим сначала случай, когда плоскость  $\pi$   $C$ - $L$  транзитивна при любом выборе точки  $C$  на оси  $L$ . Выберем ось  $L$  в качестве прямой  $L_\infty$ , а центр  $C$  — в качестве точки  $Y = (\infty)$ .

**Теорема 20.4.5.** *Плоскость  $Y$ - $L_\infty$  транзитивна тогда и только тогда, когда для соответствующего тернарного кольца  $R$ , определяющего систему координат, имеем*

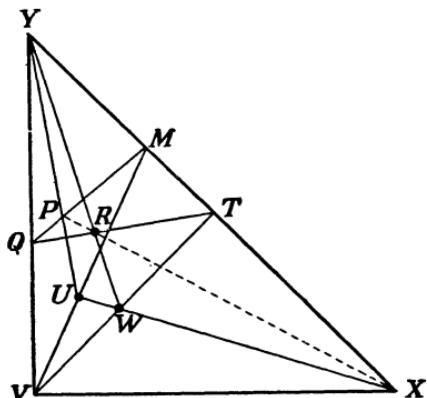


Рис. 12. Теорема линейности.

$$1) a \cdot m \circ b = am + b,$$

2) по сложению тернарное кольцо  $R$  образует группу.

*Доказательство.* Предположим, что плоскость  $\pi Y\text{-}L_\infty$  транзитивна. Выберем  $YQV$  (см. рис. 12) в качестве прямой  $x = 0$ ,  $V = (0, 0)$ ,  $Q = (0, b)$ ,  $X = (0)$ ,  $T = (1)$ ,  $M = (m)$ . При этом прямая  $MQ$  задается уравнением  $y = x \cdot m \circ b$ . Выбираем точку  $P = (a, a \cdot m \circ b)$  на прямой  $MQ$ . Тогда  $VM$  — прямая  $y = xm$ ,  $TQ$  — прямая  $y = x + b$ , а прямая  $YP$  определяется равенством  $x = a$ . В таком случае точка  $U$  пересечения прямых  $YP$  и  $VM$  имеет координаты  $U = (a, am)$ . Проводим прямую  $UX$ , заданную уравнением  $y = am$ .  $UX$  пересекает прямую  $VT$ , определяемую равенством  $y = x$ , в точке  $W = (am, am)$ . Тогда прямая  $YW$  с уравнением  $x = am$  пересекает прямую  $QT$  с уравнением  $y = x + b$  в точке  $R = (am, am + b)$ . Если теперь верно, что точки  $P, R, X$  лежат на одной прямой, то из того, что  $y = am + b$  — уравнение прямой  $RX$ , и из того, что  $P = (a, a \cdot m \circ b)$ , мы получаем  $a \cdot m \circ b = am + b$ . Следовательно, мы должны теперь показать, что точки  $P, R, X$  лежат на одной прямой. По условию плоскость  $\pi Y\text{-}L_\infty$  транзитивна. Пусть  $\beta = Y\text{-}L_\infty$  коллинеация, оставляющая неподвижными все точки прямой  $L_\infty$ , все прямые, проходящие через точку  $Y$ , и действующая на прямой  $x = 0$ , проходящей через точку  $Y$ , так что  $V\beta = Q$ , т. е.  $(0, 0)\beta = (0, b)$ . Тогда  $\beta$  оставляет неподвижными прямые  $YPU$  ( $x = a$ ),  $YRW$  ( $x = am$ ). Более того,  $(VM)\beta = QM$ ,  $(VT)\beta = QT$ . Поэтому  $U\beta = P$ ,  $W\beta = R$  и, конечно,  $X\beta = X$ . Но точки  $U, W, X$  лежат на прямой  $y = am$ . Следовательно, точки  $U\beta, W\beta, X\beta$ , т. е. точки  $P, R, X$  лежат на прямой  $y = xm + b$ . Отсюда  $P$  — это точка  $(a, am + b)$  и  $a \cdot m \circ b = am + b$ . Этим первая часть теоремы доказана.

Каково действие коллинеации  $\beta$ , определяемой равенством  $(0, 0)\beta = (0, b)$ , на произвольную точку  $(a, c)$ ? Это нетрудно выяснить из следующих соотношений:

$$\begin{aligned} y = x &\rightarrow y = x + b, \\ x = c &\rightarrow x = c, \\ (c, c) &\rightarrow (c, c + b), \\ y = c &\rightarrow y = c + b, \\ x = a &\rightarrow x = a, \\ (a, c) &\rightarrow (a, c + b). \end{aligned}$$

Итак, если  $(0, 0)\beta = (0, b)$ , то

$$(a, c)\beta = (a, c + b).$$

Если теперь  $\delta = Y\text{-}L_\infty$  коллинеация, определяемая равенством

$$(0, 0)\delta = (0, d),$$

то находим, что

$$(u, v)\delta = (u, v+d).$$

Для произведения  $\beta\delta$  вычисляем

$$(0, 0)(\beta\delta) = [(0, 0)\beta]\delta = (0, b)\delta = (0, b+d).$$

Следовательно, в общем случае  $(a, c)(\beta\delta) = [a, c + (b + d)]$ . Но  $[(a, c)\beta]\delta = (a, c+b)\delta = [a, (c+b)+d]$ . Поэтому сложение подчиняется ассоциативному закону

$$c + (b + d) = (c + b) + d.$$

Поскольку сложение на плоскости всегда обладает нулем и удовлетворяет аксиомам лупы, отсюда следует, что сложение подчиняется аксиомам группы. Этим доказано свойство (2).

Обратно, предположим, что тернарное кольцо  $R$  плоскости  $\pi$  удовлетворяет требованиям:

$$1) a \cdot m \circ b = am + b,$$

2) по сложению тернарное кольцо является группой.

Для произвольного  $b \in R$  определяем отображение  $\beta = \beta(b)$  для точек:

$$(\infty) \rightarrow (\infty),$$

$$(m) \rightarrow (m),$$

$$(a, c) \rightarrow (a, c + b)$$

и для прямых:

$$L_\infty \rightarrow L_\infty,$$

$$x = a \rightarrow x = a,$$

$$y = xm + t \rightarrow y = xm + (t + b).$$

Это коллинеация, так как если точка  $(a, c)$  лежит на прямой  $y = xm + t$ , то  $c = am + t$ ; откуда

$$c + b = (am + t) + b = am + (t + b),$$

т. е. точка  $(a, c + b)$  лежит на прямой  $y = xm + (t + b)$ . Легко проверить, что остальные определяющие свойства коллинеации имеют место для отображения  $\beta$ . Но это  $Y$ - $L_\infty$  коллинеация, отображающая  $(0, 0)$  в  $(0, b)$ , причем элемент  $b$  выбран произвольно. Следовательно, плоскость  $\pi$   $Y$ - $L_\infty$  транзитивна.

Докажем соответствующую теорему для плоскостей трансляций.

**Теорема 20.4.6.** Плоскость  $\pi$  является плоскостью трансляций относительно прямой  $L_\infty$  тогда и только тогда, когда соответствующее тернарное кольцо образует систему Веблена — Веддербарна. Это означает следующее:

- 1) по сложению это тернарное кольцо — абелева группа,
- 2) по умножению отличные от нуля элементы образуют лупу,
- 3)  $(a + b)m = am + bm$ ,
- 4) если  $r \neq s$ , уравнение  $xr = xs + t$  имеет единственное решение  $x$ ,
- 5)  $a \cdot m \circ b = am + b$ .

*Доказательство.* По теореме 20.4.4 плоскость  $\pi$  является плоскостью трансляций относительно оси  $L_\infty$ , если она  $Y$ - $L_\infty$  транзитивна и  $X$ - $L_\infty$  транзитивна. Как нам уже известно из теоремы 20.4.5,  $a \cdot m \circ b = am + b$ , а по сложению тернарное кольцо образует группу. При доказательстве теоремы 20.4.5 мы показали существование элации  $\beta(b)$  для любого  $b \in R$ , отображающего произвольную точку  $(a, c)$  в точку  $(a, c + b)$ . Согласно теореме 20.4.3, полная группа трансляций абелева, откуда

$$\beta(b)\beta(d) = \beta(d)\beta(b),$$

и поэтому  $(a, c + b + d) = (a, c + d + b)$ , откуда  $b + d = d + b$ , т. е. сложение в кольце  $R$  абелево, и свойство (1) установлено.

Пусть  $b$  — произвольный элемент из  $R$ . Рассмотрим элацию с центром  $X$ , отображающую  $(0, 0)$  в  $(b, 0)$ . Тогда последовательно находим:

$$\begin{aligned} (0, 0) &\rightarrow (b, 0), \\ y = x &\rightarrow y = x - b, \\ y = a &\rightarrow y = a, \\ (a, a) &\rightarrow (a + b, a), \\ x = a &\rightarrow x = a + b, \\ y = am &\rightarrow y = am, \\ (a, am) &\rightarrow (a + b, am). \end{aligned}$$

Далее, так как  $(0, 0) \rightarrow (b, 0)$ , то

$$y = xm \rightarrow y = xm - bm.$$

Но теперь, поскольку точка  $(a, am)$  лежит на прямой  $y = xm$ , точка  $(a + b, am)$  лежит на прямой  $y = xm - bm$ , откуда

$$am = (a + b)m - bm,$$

т. е.  $am + bm = (a + b)m$ . Этим доказано дистрибутивное свойство (3).

Плоскость по умножению — всегда лупа, а свойство (4) означает, что при  $r \neq s$  прямые  $y = xr$  и  $y = xs + t$  пересекаются в одной-единственной конечной точке.

Система элементов с бинарными операциями сложения и умножения, подчиненными требованиям (1), (2), (3) и (4), называется системой Веблена — Веддербарна, так как впервые была рассмотрена в работе [1] этих авторов.

Докажем обратное утверждение, что любая система Веблена — Веддербарна  $R$  может служить системой координат плоскости трансляций с осью  $L_\infty$ . В качестве точек выбираем (1) конечные точки  $(a, b)$ , где  $a$  и  $b$  — произвольные элементы из  $R$ , (2) бесконечные точки  $(m)$ , где  $m \in R$ , и (3) точку  $Y = (\infty)$ . В качестве прямых выбираем (1)  $L_\infty$ , состоящую из точек  $(m)$  и  $(\infty)$ , (2) прямые  $x = c$ , содержащие точку  $(\infty)$  и все точки вида  $(c, d)$ , и (3) прямые  $y = xm + b$ , содержащие точки  $(m)$  и все точки вида  $(a, am + b)$ , где  $a \in R$ . Теперь непосредственно проверяется, что существует одна-единственная прямая, соединяющая две любые различные точки, существует одна-единственная точка, лежащая на двух различных прямых, и что никакие три из четырех точек  $(0, 0)$ ,  $(1, 1)$ ,  $(\infty)$  и  $(0)$  не лежат на одной прямой. Эта проверка состоит в рассмотрении нескольких случаев, причем условие (4) нам необходимо, чтобы показать, что прямые  $y = xr + b$  и  $y = xs + c$  при  $r \neq s$  пересекаются в одной конечной точке.

Для плоскости Веблена — Веддербарна легко проверить, что отображение  $(x, y) \rightarrow (x + r, y + s)$  для конечных точек является коллинеацией при любых  $r$  и  $s$ , оставляющей на месте все точки прямой  $L_\infty$ , а для конечных прямых оно определяет следующее отображение:  $x = c \rightarrow x = r + c$ ,  $y = xm + b \rightarrow y = xm - rm + s + b$ . Если  $s = rt$ , то эта коллинеация является элацией с осью  $L_\infty$  и центром  $(t)$ . Следовательно, плоскость Веблена — Веддербарна есть плоскость трансляций относительно оси  $L_\infty$ .

Произвольное тело является, конечно, системой Веблена — Веддербарна, даже если не требовать, чтобы оно было ассоциативным. Система Веблена — Веддербарна, в которой умножение ассоциативно, называется *почти-полем*. Оно будет рассмотрено позднее. Следует отметить, что неизоморфные системы Веблена — Веддербарна могут быть системами координат одной и той же проективной плоскости. Это будет показано в § 20.9. Действительно, если изменить выбор точек  $X$  и  $Y$  на прямой  $L_\infty$ , для которой  $\pi$  — плоскость трансляций, то соответствующее тернарное кольцо снова будет в силу теоремы 20.4.6 системой Веблена — Веддербарна, но не все такие системы должны быть изоморфными.

Легко построить класс систем Веблена — Веддербарна, известных как системы Холла [2]. Рассмотрим такое поле  $F$ , что существует полином  $x^2 - rx - s$ , неприводимый над полем  $F$ . Тогда мы можем построить систему Веблена — Веддербарна  $J$  над полем  $F$ .

**Теорема 20.4.7.** Пусть  $F$  — поле, над которым квадратный полином  $f(x) = x^2 - rx - s$  неприводим. Тогда множество

элементов  $a + ub$ ,  $a, b \in F$ , составляет систему  $J$  Веблена — Веддербарна относительно следующих операций:

- 1)  $(a_1 + ub_1) + (a_2 + ub_2) = (a_1 + a_2) + u(b_1 + b_2)$ ,
- 2) при  $c \in F$  полагаем  $(a + ub)c = ac + u(bc)$ ,
- 3) для  $z = a + ub$ , где  $a, b \in F$ ,  $b \neq 0$ , и  $w = c + zd$ ,  $c, d \in F$ , полагаем

$$wz = ds + z(c + dr) = ac + adr + ds + u(bc + bdr).$$

При так определенных операциях  $J$  — система Веблена — Веддербарна, удовлетворяющая закону дистрибутивности  $(x + y)z = xz + yz$ . Элементы  $c \in F$  обладают свойством  $cx = xc$ ,  $c(xy) = (cx)y = (xc)y$ . Кроме того, любой элемент  $z \notin F$  является корнем уравнения  $z^2 - rz - s = 0$ .

*Доказательство.* Сложение вполне определено, причем по сложению  $J$  — абелева группа. Умножение также вполне определено, однако есть два существенно различных правила умножения  $xy$ : правило (2) для  $y = c \in F$  и правило (3) для  $y = z \notin F$ . Дистрибутивный закон  $(x + y)z = xz + yz$  выполняется, так как умножение производится по правилу (2), если  $z \in F$ , и по правилу (3), если  $z \notin F$ , но дистрибутивность имеет место в обоих этих случаях.

Заметим, что из правила (3) при  $z \notin F$  получается равенство  $z^2 = rz + s$ , а при  $c \in F$  получается  $cz = zc$ . Очевидно, что  $cx = xc$  при  $c, x \in F$ . Единица 1 поля  $F$  является единицей системы  $J$ . Чтобы убедиться в том, что система по умножению — лупа, мы должны показать, что в соотношении  $xy = v$  любая пара элементов  $x, y, v$ , из которых все отличны от нулевого, однозначно определяет третий. Элементы  $x$  и  $y$  определяют элемент  $v = xy$  однозначно, что следует из правила (2), если  $y \in F$ , и из правила (3), если  $y \notin F$ , причем, если  $x \neq 0$ ,  $y \neq 0$ , то и  $v \neq 0$ , что сразу вытекает из правила (3) при  $b \neq 0$  и  $s \neq 0$ . При данных  $y \neq 0$  и  $v \neq 0$  или правило (2), или правило (3) однозначно определяет такой элемент  $x \neq 0$ , что  $xy = v$ .

Положение немного усложняется, если заданы элементы  $x \neq 0$  и  $v \neq 0$ . Пусть  $x = a + ub$ ,  $v = c + ud$  при  $a, b, c, d \in F$ . Если  $ad - bc = 0$ , то существует один-единственный элемент  $f \neq 0$ ,  $f \in F$ , такой, что  $af = c$  и  $bf = d$ , откуда  $xf = v$ . Это и есть единственный элемент из поля  $F$ , удовлетворяющий этому соотношению. Предположим теперь, что  $ad - bc \neq 0$ . Если бы удалось представить  $y$  в виде  $y = y_1 + uy_2$ , где  $y_1, y_2 \in F$ ,  $y_2 \neq 0$ , то мы бы имели  $x = (a - by_1y_2^{-1}) + y(by_2^{-1})$ ,  $xy = sb y_2^{-1} + y(a - by_1y_2^{-1} + rb y_2^{-1})$  и  $v = (c - dy_1y_2^{-1}) + y(dy_2^{-1})$ . Требование  $xy = v$  дает

следующие соотношения:

$$\begin{aligned} ay_2 - by_1 &= d - rb, \\ cy_2 - dy_1 &= sb. \end{aligned}$$

Так как  $ad - bc \neq 0$ , эта система относительно  $y_1$  и  $y_2$  имеет единственное решение, причем  $y_2 = (d^2 - rbd - sb^2)/(ad - bc)$ . Здесь  $y_2 \neq 0$ , так как в силу неприводимости полинома  $x^2 - rx - s$  над полем  $F$  мы не можем получить равенство  $d^2 - rbd - sb^2 = 0$  при  $d$  и  $b$  из поля  $F$ , отличных от нуля. Полученные значения для  $y_1$  и  $y_2$  определяют такой элемент  $y \notin F$ , что  $xy = v$ . Таким образом, отличные от нуля элементы системы  $J$  образуют лупу.

Чтобы показать, что при  $m \neq n$  уравнение  $xm = xn + v$  имеет единственное решение, достаточно найти одно решение, так как если бы существовало два решения  $x_1$  и  $x_2$ , то мы получили бы равенство  $(x_1 - x_2)m = (x_1 - x_2)n$ , противоречащее свойству лупы. Найти же такое решение при  $m, n \in F$  нетрудно. Предположим поэтому, что  $m \notin F$ . (Если  $m \in F$ , но  $n \notin F$ , то вместо уравнения  $xm = xn + v$  рассматриваем уравнение  $xn = xm - v$ .) Тогда можно выразить  $n$  и  $v$  через  $m$ . Пусть  $n = c \in F$ ,  $v = v_1 + mv_2$  ( $v_1, v_2 \in F$ ). Если  $x = x_1 + mx_2$ , то находим систему уравнений

$$\begin{aligned} -cx_1 + sx_2 &= v_1, \\ x_1 + (r - c)x_2 &= v_2, \end{aligned}$$

являющуюся разрешимой, так как в силу неприводимости полинома  $x^2 - rx - s$  определитель  $c^2 - rc - s$  не равен нулю. Наконец, если  $n = a + mb$ ,  $v = v_1 + mv_2$  и если мы положим  $x = x_1 + mx_2$ , то  $-ax_1 + (a^2b^{-1} - ab^{-1}r - b^{-1}s + s)x_2 = v_1(1 - b)x_1 + ax_2 = v_2$ .

При этом определитель равен  $-b^{-1}[a^2 - ra(1 - b) - s(1 - b)^2]$ , он отличен от нуля, так как  $b \neq 0$ , а полином  $x^2 - rx - s$  неприводим. Следовательно, одно решение существует, и уравнение  $xm = xn + v$  имеет единственное решение  $x$ . Таким образом,  $J$  — система Веблена — Веддербарна.

## 20.5. Муфанговы и дезарговы плоскости

В предыдущем параграфе было показано, что для произвольной плоскости системы Веблена — Веддербарна может быть выбрана в качестве системы координат в том и только в том случае, когда она является плоскостью трансляций по отношению к некоторой прямой, обозначенной через  $L_\infty$ . Но что можно сказать о плоскости и о ее системе координат, если эта плоскость является плоскостью трансляций по отношению к нескольким прямым? В этом параграфе мы дадим ответ на этот вопрос.

**Теорема 20.5.1.** *Если  $\pi$  — плоскость трансляций относительно двух прямых, пересекающихся в точке  $Q$ , то эта плоскость является плоскостью трансляций относительно любой прямой пучка прямых, проходящих через точку  $Q$ .*

**Следствие 20.5.1.** *Если  $\pi$  — плоскость трансляций относительно трех прямых, не пересекающихся в одной точке, то она является плоскостью трансляций относительно каждой прямой.*

**Доказательство.** Следствие непосредственно вытекает из теоремы, так как множество прямых, содержащее вместе с любой парой прямых пучок с центром в точке их пересечения, состоит из всех прямых плоскости, если оно содержит три прямые, не пересекающиеся в одной точке.

Предположим, что  $L_1$  и  $L_2$  — две прямые, пересекающиеся в точке  $Y$ , и что  $\pi$  — плоскость трансляций относительно прямых  $L_1$  и  $L_2$ . Пусть  $L_3$  — третья прямая, проходящая через точку  $Y$ , и пусть  $C$  — произвольная точка прямой  $L_3$ , отличная от  $Y$ . Пусть, далее,  $RCS$  — произвольная прямая, содержащая точку  $C$  и пересекающая  $L_1$  в точке  $R$ , а  $L_2$  в точке  $S$ . Тогда существует элация  $\alpha$ , имеющая ось  $L_1$  и центр  $R$  и отображающая  $S$  в  $C$ , а  $L_2$  в  $L_3$ . Так как плоскость  $\pi$  обладает всеми элациями, осью которых является  $L_2$ , а центром — точка  $S$ , то построение, использованное при доказательстве теоремы линейности (рис. 12), верно во всех случаях, когда точка  $S$  является центром, а прямая  $L_2$  — осью. Коллинеация  $\alpha$  отображает все эти построения на такие же построения с центром  $C$  и осью  $L_3$ . Поэтому плоскость  $\pi$  обладает всевозможными элациями, имеющими центр  $C$  и ось  $L_3$ . Так как это рассуждение справедливо для любой точки прямой  $L_3$ , отличной от  $Y$ , то, в силу следствия из теоремы 20.4.4,  $\pi$  есть плоскость трансляций с осью  $L_3$ .

**Теорема 20.5.2.** *Плоскость  $\pi$  является плоскостью трансляций для любой прямой, проходящей через точку  $Y = (\infty)$ , в том и только в том случае, если (1) ее конечные прямые задаются линейными уравнениями  $x = c$  и  $y = xm + b$  и (2) координаты подчиняются следующим требованиям:*

- 2.1) по сложению они образуют абелеву группу,
- 2.2)  $(a+b)m = am + bm$ ,
- 2.3)  $a(s+t) = as + at$ ,
- 2.4) каждый элемент  $a \neq 0$  обладает таким обратным элементом  $a^{-1}$ , что  $aa^{-1} = 1 = a^{-1}a$ ,
- 2.5)  $a^{-1}(ab) = b$ .

**Доказательство.** Предположим, что  $\pi$  — плоскость трансляций для любой прямой, проходящей через точку  $Y = (\infty)$ . Среди этих прямых находится прямая  $L_\infty$ . Поэтому, согласно теореме

20.4.6, условия линейности (1) выполняются и координаты образуют систему Веблена — Веддербарна. Значит, и условия (2.1) и (2.2) выполняются. Докажем остальные три свойства.

Рассмотрим элацию, центр которой — точка  $Y = (\infty)$ , а ось — прямая  $x = 0$  и которая отображает точку  $(0)$  в точку  $(m)$ . При этом все точки  $(0, b)$  остаются неподвижными так же, как и прямые  $L_\infty$  и  $x = c$ . Последовательно находим:

$$\begin{aligned} (0) &\rightarrow (m), \\ (0, b) &\rightarrow (0, b), \\ y = b &\rightarrow y = xm + b, \\ x = a &\rightarrow x = a, \\ (a, b) &\rightarrow (a, am + b). \end{aligned}$$

Этим определяется отображение для любой конечной точки. В частности,  $(1, t) \rightarrow (1, m+t)$  и  $(0, 0) \rightarrow (0, 0)$ , откуда  $y = xt \rightarrow y = x(m+t)$ . Но  $(a, at) \rightarrow (a, am+at)$ , а точка  $(a, at)$  лежит на прямой  $y = xt$ . Поэтому точка  $(a, am+at)$  лежит на прямой  $y = x(m+t)$ , откуда следует дистрибутивный закон (2.3):

$$am + at = a(m + t).$$

Теперь рассмотрим элацию, имеющую центр  $(0, 0)$ , ось  $x = 0$  и отображающую  $(0)$  в точку  $(-1 - a, 0)$ . Для нее получаем, что  $(0, 1+a) \rightarrow (0, 1+a)$ , откуда  $y = 1+a \rightarrow y = x + 1+a$ . Далее,

$$\begin{aligned} (0) &\rightarrow (-1 - a, 0), \\ (0, b+ab) &\rightarrow (0, b+ab), \end{aligned}$$

откуда  $y = b+ab \rightarrow y = xb+b+ab$ . Теперь имеем

$$\begin{aligned} y = 1+a &\rightarrow y = x + 1 + a, \\ y = x(1+a) &\rightarrow y = x(1+a), \end{aligned}$$

откуда  $(1, 1+a) \rightarrow (d, d+1+a)$ , если  $a \neq 0$ ; при этом

$$d(1+a) = d + 1 + a.$$

Далее,

$$\begin{aligned} (\infty) &\rightarrow (\infty), \\ (1, 1+a) &\rightarrow (d, d+1+a), \end{aligned}$$

откуда  $x = 1 \rightarrow x = d$ .

Теперь получаем

$$\begin{aligned} y = x(b+ab) &\rightarrow y = x(b+ab), \\ y = b+ab &\rightarrow y = xb+b+ab, \end{aligned}$$

откуда  $(1, b+ab) \rightarrow (d, d[b+ab])$ , где  $d(b+ab) = db + b + ab$ .

Предположим теперь, что не только  $a \neq 0$ , но и  $(-1 - a, 0) \neq (0, 0)$ , т. е. что  $a \neq -1$ . Для такого элемента  $a$  существует такой элемент  $d$ , что  $d(1 + a) = d + 1 + a$  и  $d(b + ab) = db + b + ab$  для произвольного  $b$ . Полагая  $d = u + 1$  и применяя дистрибутивные законы, находим, что  $ua = 1$  и  $u(ab) = b$ . Непосредственно из дистрибутивных законов находим, что при  $a = -1$  эти соотношения сохраняются, когда  $u = -1$ . Так как для  $u \neq 0$  существует такой элемент  $v$ , что  $vu = 1$  и  $v(ua) = a$ , то находим, что  $v = a$ . Следовательно,  $u = a^{-1}$ , и мы получаем свойство (2.4)  $aa^{-1} = a^{-1}a = 1$  и свойство (2.5)  $a^{-1}(ab) = b$ .

Обратно, предположим, что условия (1) и (2) для координат плоскости  $\pi$  выполняются. Согласно теореме 20.4.6,  $\pi$  — плоскость трансляций относительно прямой  $L_\infty$ . Так как справедлива теорема 20.5.1, достаточно показать, что плоскость  $\pi$  обладает коллинеацией, отображающей прямую  $L_\infty$  на некоторую другую прямую, проходящую через точку  $Y = (\infty)$ . Такой коллинеацией является следующее отображение:

$$\begin{aligned} (\infty) &\rightarrow (\infty), \\ (m) &\rightarrow (1, m), \\ (-1, m) &\rightarrow (-m), \\ (0, b) &\rightarrow (0, b), \\ (c, d) &\rightarrow [(1 + c^{-1})^{-1}, (1 + c)^{-1}d], c \neq 0, -1, \\ L_\infty &\rightarrow x = 1, \\ x = -1 &\rightarrow L_\infty, \\ x = 0 &\rightarrow x = 0, \\ x = c &\rightarrow x = (1 + c^{-1})^{-1}, c \neq 0, -1, \\ y = xm + b &\rightarrow y = x(m - b) + b. \end{aligned}$$

Чтобы это доказать, необходимо установить сохранение отношений инцидентности при этом отображении и, в частности, надо доказать, что если точка  $(c, d)$  лежит на прямой  $y = xm + b$ , то образ этой точки принадлежит образу этой прямой. Доказательство последнего факта сводится к доказательству тождества

$$(1 + c)^{-1}(cm + b) = (1 + c^{-1})^{-1}(m - b) + b.$$

Оно следует из условий теоремы и из следующих тождеств:

$$\begin{aligned} (1 + c)^{-1}(cm) &= (1 + c^{-1})^{-1}m, \\ (1 + c)^{-1}b &= (1 + c^{-1})^{-1}(-b) + b. \end{aligned}$$

Докажем, следуя Бруку [1], еще одно тождество, вытекающее из условий теоремы. Пусть

$$[y^{-1} - (y + z^{-1})^{-1}] [y(zy) + y] = t,$$

где  $y \neq 0$ ,  $y \neq -z^{-1}$ . Умножив это равенство на  $y + z^{-1}$ , получим

$$(y + z^{-1})t = (y + z^{-1})[zy + 1 - (y + z^{-1})^{-1}(y(zy)) - (y + z^{-1})^{-1}y] = \\ = y(zy) + y + y + z^{-1} - y(zy) - y = y + z^{-1}.$$

Значит,  $t = 1$ , а элементы  $y^{-1} - (y + z^{-1})^{-1}$  и  $y(zy) + y$  взаимно обратны. Тогда для любого  $x$  имеем

$$[y^{-1} - (y + z^{-1})^{-1}] [(y(zy))x + yx] = x.$$

Положим

$$[y^{-1} - (y + z^{-1})^{-1}] [y(z(yx)) + yx] = w.$$

Тогда

$$(y + z^{-1})w = (y + z^{-1})[z(yx) + x] - y[z(yx)] - yx = \\ = yx + z^{-1}x = (y + z^{-1})x.$$

Следовательно,  $w = x$ . Сравнивая выражения для  $w$  и  $x$ , получаем тождество Муфанг [1]:

$$[y(zy)]x = y[z(yx)]. \quad (\text{M})$$

Это тождество, очевидно, сохраняется и для исключенных значений  $y = 0$ ,  $y = -z^{-1}$  и, следовательно, верно без ограничений для переменных. В частности, тождество Муфанг при  $z = 1$  дает левый альтернативный закон:

$$(uy)x = y(ux). \quad (\text{LA})$$

Если плоскость является плоскостью трансляций относительно любой прямой, то она называется *плоскостью Муфанг*, по имени Руффа Муфанг [1], впервые изучавшей ее.

**Теорема 20.5.3.** *Плоскость муфангова в том и только в том случае, если любое тернарное кольцо (1) линейно и (2) является альтернативным телом, т. е. обладает следующими свойствами:*

- 2.1) по сложению тернарное кольцо — абелева группа,
  - 2.2)  $(a + b)m = am + bm$ ,
  - 2.3)  $a(s + t) = as + at$ ,
  - 2.4) любой элемент  $a \neq 0$  имеет обратный  $a^{-1}$ , такой, что  $a^{-1}a = aa^{-1} = 1$ ,
  - 2.5)  $a^{-1}(ab) = b$ ,
  - 2.6)  $(ba)a^{-1} = b$ ;
- кроме того, выполняются альтернативные законы:
- 2.7)  $a(ab) = (aa)b$ ,  $(ba)a = b(aa)$ .

*Доказательство.* Из теоремы 20.5.2 получаем свойство (1), а также свойства (2.1) — (2.5). Достаточно доказать свойство (2.6), так как очевидно, что правый альтернативный закон  $(ba)a = b(aa)$  вытекает из (2.6) точно так же, как левый альтернативный закон — из свойства (2.5).

Рассмотрим элацию, осью которой служит прямая  $x = 0$ , а центром — точка  $(0, 0)$  и которая переводит точку  $Y = (\infty)$  в точку  $(0; -1)$ . Последовательно получаем

$$(\infty) \rightarrow (0, -1),$$

$$(1, 0) \rightarrow (1, 0),$$

откуда

$$x = 1 \rightarrow y = x - 1.$$

$$(\infty) \rightarrow (0, -1),$$

$$(a, 0) \rightarrow (a, 0);$$

отсюда

$$x = a \rightarrow y = xa^{-1} - 1,$$

$$x = 1 \rightarrow y = x - 1,$$

$$y = x(1 - ab) \rightarrow y = x(1 - ab).$$

Поэтому

$$(1, 1 - ab) \rightarrow [(ab)^{-1}, (ab)^{-1} - 1].$$

Кроме того,

$$0 \rightarrow 0,$$

откуда

$$y = 1 - ab \rightarrow y = (ab)^{-1} - 1,$$

$$x = a \rightarrow y = xa^{-1} - 1.$$

$$y = x(a^{-1} - b) \rightarrow y = x(a^{-1} - b),$$

и потому

$$(a, 1 - ab) \rightarrow (b^{-1}, b^{-1}a^{-1} - 1).$$

Так как  $(0) \rightarrow (0)$ , мы получаем  $y = 1 - ab \rightarrow y = b^{-1}a^{-1} - 1$ . Сравнивая образы прямой  $y = 1 - ab$ , мы находим, что  $(ab)^{-1} = b^{-1}a^{-1}$ . Отсюда, учитывая равенство  $b^{-1} = a(a^{-1}b^{-1})$ , получаем

$$b = (b^{-1})^{-1} = [a(a^{-1}b^{-1})]^{-1} = (a^{-1}b^{-1})^{-1}a^{-1} = (ba)a^{-1}.$$

Этим доказано свойство (2.6).

Мы сейчас показали, что в муфанговой плоскости координаты удовлетворяют аксиомам альтернативного тела. Обратно, пусть нам дано альтернативное тело. Строим плоскость с соответствующей ему системой координат. В силу теоремы 20.5.2, получается

плоскость трансляций относительно любой прямой, проходящей через точку  $Y = (\infty)$ . Поэтому, согласно теореме 20.5.1 и следствию из нее, отсюда будет вытекать, что эта плоскость является плоскостью трансляций относительно любой прямой, если мы сможем указать коллинеацию, не оставляющую неподвижной точку  $Y = (\infty)$ . Такой коллинеацией является следующее отображение:

$$(a, b) \xleftrightarrow{} (b, a),$$

$$(0) \xleftrightarrow{} (\infty),$$

$$(m) \xleftrightarrow{} (m^{-1}), m \neq 0,$$

$$x = c \xleftrightarrow{} y = c,$$

$$y = xm + b \xleftrightarrow{} y = xm^{-1} - bm^{-1}, m \neq 0.$$

Этим завершается доказательство теоремы. Здесь уместно сделать несколько замечаний.

Справедливы более сильные утверждения, чем только что доказанные, однако их доказательство требует более глубоких результатов об альтернативных кольцах, чем те, которые здесь можно изложить. Установлено, что плоскость трансляций относительно двух различных прямых является плоскостью Муфанг, т. е. плоскостью трансляций относительно любой прямой. На алгебраическом языке это означает, что свойство  $(2.6)(ba)a^{-1} = b$  является следствием предыдущих. Ни одно простое доказательство этого факта автору не известно. Как мы видели, левый альтернативный закон  $x(xy) = (xx)y$  следует из свойства (2.5). Клейнфельд [2] и Л. А. Скорняков [2] показали, что для альтернативного тела характеристики, отличной от 2, из этого закона следует также и правый альтернативный закон  $(yx)x = y(xx)$ . Это вообще неверно для тела характеристики 2, однако, налагая более сильное условие Муфанг  $[y(zy)]x = y[z(yx)]$ , которое, как мы показали, следует из (2.5). Сан Суси [1] показал, что и при характеристике, равной 2, правый альтернативный закон вытекает из левого. Брук и Клейнфельд [1] изучали альтернативные тела  $R$  и пришли к замечательному результату, что такое кольцо  $R$  или ассоциативно, или является алгеброй особого вида над своим центром, являющимся полем  $F$ . А именно  $R$  является алгеброй Кэли—Диксона (Cayley—Dickson) над  $F$  с восемью базисными элементами, причем каждый элемент, не принадлежащий полю  $F$ , порождает квадратичное поле над  $F$ , а любая пара элементов (не содержащихся в одном и том же квадратичном расширении поля  $F$ ) порождает алгебру кватернионов. Эти тонкие результаты помогли им показать, что в муфанговой плоскости любое тернарное кольцо не только является альтернативным телом, но и является одним и тем же альтернативным телом. Для полного ознакомления со

всеми этими результатами, кроме результата Сан Суси, отсылаем читателя к книге Пиккерта [1].

**Теорема 20.5.4.** *Следующие свойства плоскости  $\pi$  эквивалентны:*

1) плоскость  $\pi$   $X\text{-}OY$  транзитивна, т. е.  $\pi$  обладает всеми гомологиями, центром которых служит точка  $X = (0)$ , а осью — прямая  $x = 0$ ;

2) для тернарного кольца плоскости  $\pi$ , определенной четырьмя точками  $X, Y, O, I$ , имеем

$$2.1) x \cdot m \circ b = xm + b,$$

$$2.2) \text{умножение удовлетворяет аксиомам группы.}$$

**Доказательство.** Пусть для плоскости  $\pi$  справедливо свойство (1). Рассмотрим гомологию, ось которой — прямая  $x = 0$ , а центр — точка  $X = (0)$  и на прямой  $L_\infty(m) \rightarrow (1)$ . Тогда имеем

$$(0, 0) \rightarrow (0, 0),$$

$$(m) \rightarrow (1),$$

откуда

$$y = xm \rightarrow y = x.$$

Но

$$y = am \rightarrow y = am,$$

$$(a, am) \rightarrow (am, am).$$

откуда

$$(\infty) \rightarrow (\infty),$$

так как

$$x = a \rightarrow x = am$$

то

$$y = c \rightarrow y = c,$$

и

$$(a, c) \rightarrow (am, c).$$

откуда

$$(0, b) \rightarrow (0, b), (m) \rightarrow (1),$$

получаем

$$y = x \cdot m \circ b \rightarrow y = x + b.$$

Следовательно, если точка  $(a, c)$  лежит на прямой  $y = x \cdot m \circ b$ , то точка  $(am, c)$  лежит на прямой  $y = x + b$ . Таким образом, из равенства  $c = a \cdot m \circ b$  следует, что  $c = am + b$ , откуда получается условие линейности (2.1)  $a \cdot m \circ b = am + b$ .

Гомология, заданная отображением  $(m) \rightarrow (1)$ , переводит точку  $(a, 1)$  в точку  $(am, 1)$  и, в частности,  $(1, 1) \rightarrow (m, 1)$ . Если умножить эту гомологию на другую, определенную условием  $(n) \rightarrow (1)$ , то получим отображения  $(1, 1) \rightarrow (m, 1) \rightarrow (mn, 1)$  и  $(a, 1) \rightarrow (am, 1) \rightarrow ((am)n, 1)$ .

Но произведение должно быть гомологией, для которой  $(mn) \rightarrow (1)$ , откуда  $(a, 1) \rightarrow (a(mn), 1)$ , и поэтому  $(am)n = a(mn)$ , т. е. для умножения справедлив ассоциативный закон. Но так как по умножению тернарное кольцо есть лупа, отсюда следует, что оно является даже группой.

Предположим теперь, что выполняется условие (2). Следующее отображение при фиксированном  $m \neq 0$  является гомологией плоскости  $\pi$ :

$$\begin{aligned}(\infty) &\rightarrow (\infty), \\(0) &\rightarrow (0), \\(n) &\rightarrow (m^{-1}n), \\(a, b) &\rightarrow (am, b), \\L_\infty &\rightarrow L_\infty, \\x = a &\rightarrow x = am, \\y = xn + b &\rightarrow y = x(m^{-1}n) + b.\end{aligned}$$

Заставляя параметр  $m$  пробегать все отличные от нуля значения, мы получаем все гомологии с центром  $X = (0)$  и осью  $x = 0$ . Поэтому из условия (2) следует условие (1).

**Теорема 20.5.5.** *Если в плоскости  $\pi$  справедливы следующие утверждения, являющиеся частными случаями теоремы Дезарга:*

1) *теорема линейности для всякой тройки осей, не пересекающихся в одной точке,*

2) *общая теорема для одной оси и одного центра, не лежащего на этой оси,*

*то в качестве системы координат для плоскости  $\pi$  можно выбрать ассоциативное тело. В этом случае теорема Дезарга справедлива на всей плоскости  $\pi$ . Группа коллинеаций плоскости  $\pi$  транзитивна на четырехугольниках, а любое тернарное кольцо плоскости  $\pi$  изоморфно одному и тому же телу.*

**Доказательство.** Согласно условию, мы можем применить теоремы 20.5.3 и 20.5.4 и находим, что для некоторого четырехугольника  $XYOI$ , определяющего тернарное кольцо плоскости  $\pi$ , имеет место равенство  $x \cdot m \circ b = xm + b$  и координаты образуют ассоциативное тело. Очевидно, что если существует коллинеация плоскости  $\pi$ , отображающая точки  $X_1, Y_1, O_1, I_1$  одного четырехугольника в соответствующие точки  $X_2, Y_2, O_2, I_2$  другого, то соответствующие им тернарные кольца изоморфны. Докажем сначала, что если в качестве координат плоскости  $\pi$  относительно четырехугольника  $X_1Y_1O_1I_1$  выбраны элементы ассоциативного тела  $D$ , то коллинеации плоскости  $\pi$  транзитивны на четырехугольниках, откуда следует, что любому четырехугольнику соответствует координатное кольцо, изоморфное  $D$ . В силу теоремы 20.5.3,  $\pi$  — плоскость трансляций относительно любой прямой, лежащей в этой плоскости. Если  $ABC$  — произвольный треугольник, то существует элация с осью  $AB$ , оставляющая

неподвижными точками  $A$ ,  $B$  и отображающая  $C$  в произвольную точку  $C'$ , которая не лежит на прямой  $AB$ . Сначала применим это утверждение к произвольному четырехугольнику  $X_2Y_2O_2I_2$ . При подходящем выборе таких элаций мы находим коллинеацию, отображающую  $X_2$  в  $X_1$ ,  $Y_2$  в  $Y_1$  и  $O_2$  в  $O_1$ . Точка  $I_2$  не лежит ни на одной из сторон треугольника  $X_2Y_2O_2$ , и поэтому относительно системы координат  $X_1Y_1O_1I_1$  она является конечной точкой  $I_2 = (a, b)$ , причем  $a \neq 0$  и  $b \neq 0$ . Следующая коллинеация оставляет неподвижными точки  $X$ ,  $Y$ ,  $O$  и отображает  $I_2$  в  $I_1$ :

$$\begin{aligned} (x, y) &\rightarrow (xa^{-1}, yb^{-1}), \\ (m) &\rightarrow (amb^{-1}), \\ (\infty) &\rightarrow (\infty), \\ y = xm + s &\rightarrow y = x(amb^{-1}) + sb^{-1}, \\ x = c &\rightarrow x = ca^{-1}, \\ L_\infty &\rightarrow L_\infty. \end{aligned}$$

Таким образом, все тернарные кольца изоморфны некоторому ассоциативному телу  $D$ , а плоскость  $\pi$  на четырехугольниках транзитивна.

Осталось только показать, что на всей плоскости  $\pi$  справедлива теорема Дезарга. Если центр лежит на оси, эта теорема, конечно, верна, так как в этом случае плоскость  $\pi$  обладает всеми возможными элациями. Предположим теперь, что центр  $O$  не лежит на оси, которую мы обозначим через  $L_\infty$ . Покажем, что плоскость  $\pi$  обладает всеми гомологиями с центром  $O$  и осью  $L_\infty$ . При фиксированном элементе  $a \neq 0$  следующее отображение является такой гомологией:

$$\begin{aligned} (\infty) &\rightarrow (\infty), \\ (m) &\rightarrow (m), \\ (c, d) &\rightarrow (ac, ad), \\ L_\infty &\rightarrow L_\infty, \\ x = c &\rightarrow x = ac, \\ y = xm + b &\rightarrow y = xm + ab. \end{aligned}$$

Если параметр  $a$  пробегает все отличные от нуля значения, мы получаем всевозможные соответствия, имеющие центр  $O$  и ось  $L_\infty$ .

## 20.6. Теорема Веддербарна и теорема Артина — Цорна

Напомним те свойства конечных полей (поля Галуа), которые нам понадобятся. Доказательства этих свойств можно найти в книге Ван дер Вардена [1] (ч. 1, гл. V, § 37).

1) Число элементов конечного поля равно степени простого числа. Для каждой степени  $p^r$  существует конечное поле  $GF(p^r)$ , состоящее из  $p^r$  элементов, причем оно единственno с точностью до изоморфизма.

2) Любой элемент  $x$  поля  $GF(p^r)$  удовлетворяет уравнению  $x^{p^r} = x$ . Мультиликативная группа  $F^*(p^r)$ , состоящая из  $p^r - 1$  элементов поля  $GF(p^r)$ , отличных от нуля, циклична. Всякий образующий элемент этой циклической группы называется *первобазовым корнем*.

3) Поле  $GF(p^r)$  можно представить как поле классов вычетов полиномов  $P(x)$  с коэффициентами из простого поля  $F_p$  характеристики  $p$  по модулю неприводимого полинома  $f(x)$  степени  $r$  над полем  $F_p$  или как поле классов вычетов кольца целочисленных полиномов по модулю идеала  $(p, f(x))$ .

4) Автоморфизмы поля  $GF(p^r)$  образуют циклическую группу порядка  $r$ , порожденную автоморфизмом  $z \rightarrow \alpha(z) = z^p$ .

**Теорема 20.6.1.** (Теорема Веддербарна.) *Конечное тело  $R$  коммутативно и поэтому является конечным полем  $GF(p^r)$ .*

**Доказательство.** Излагаемое здесь доказательство принадлежит Витту [1]. Единица тела  $R$  порождает простое подполе тела  $R$ , которое должно быть конечным полем  $F_p$ , где  $p$  — некоторое простое число. Пусть тело  $R$  обладает базисом  $x_1 = 1, x_2, \dots, x_r$  из  $r$  элементов над  $F_p$ . Тогда  $R$  состоит точно из  $p^r$  элементов. Центр  $Z$  тела  $R$  состоит из всех таких элементов  $z \in R$ , что  $zx = xz$  для любого  $x \in R$ . Центр  $Z$  — коммутативное подтело тела  $R$ , и поэтому  $Z$  — конечное поле. Пусть  $Z$  состоит из  $q = p^s$  элементов. Покажем, что центр  $Z$  совпадает со всем  $R$ . Тело  $R$  является векторным пространством над  $Z$ ; если базис  $R$  над  $Z$  состоит из  $t$  элементов, то тело  $R$  состоит из  $q^t = p^{st} = p^r$  элементов. При этом  $t = 1$ , если  $R = Z$ . Нормализатор  $N_x$  произвольного элемента  $x \in R$  есть подтело, содержащее центр  $Z$ . Поэтому тело  $N_x$  состоит из  $q^d$  элементов, но так как  $R$  — векторное пространство над  $N_x$ , то  $d/t$ . Следовательно, в мультиликативной группе  $R^*$ , состоящей из  $p^r - 1 = q^t - 1$  отличных от нуля элементов тела  $R$ , произвольный элемент  $x \notin Z$  обладает нормализатором порядка  $q^d - 1$ , где  $d$  делит  $t$  и  $d < t$ . Исходя из этого, для порядка группы  $R^*$  получаем

$$q^t - 1 = q - 1 + \sum (q^t - 1)/(q^d - 1), \quad (20.6.1)$$

где  $q - 1$  — число элементов центра, а каждое из последующих слагаемых  $(q^t - 1)/(q^d - 1)$ , где  $d/t$ ,  $d < t$ , — это число элементов в соответствующем классе сопряженных элементов.

В § 16.8 мы показали, что полином  $f(x) = x^t - 1$  обладает сомножителем  $k(x)$  с целыми коэффициентами, а именно  $k(x) =$

$\Rightarrow \prod_{(j,t)=1} (x - w^j)$ , где  $w$  — некоторый первообразный корень степени  $t$  из единицы, а  $w^j$  при  $j = 1, \dots, t$ , где  $(j, t) = 1$ , — все первообразные корни степени  $t$  из единицы. Поэтому если  $d/t$ ,  $d < t$ , то  $x^t - 1 = k(x)(x^d - 1)r(x)$ , так как  $k(x)$  не содержит ни одного сомножителя полинома  $x^d - 1$ . При этом  $r(x)$  содержит все остальные сомножители полинома  $x^t - 1$ , если они имеются. Поэтому  $(x^t - 1)/(x^d - 1) = k(x)r(x)$ . При  $x = q$  имеем  $k(q) = \prod_{(j,t)=1} (q - w^j)$ , а так как  $w^j \neq 1$  — комплексный корень из единицы, то  $|q - w^j| > q - 1$ . Следовательно,  $k(q)$  — целое число, абсолютная величина которого больше  $q - 1$ . Поэтому если  $t > 1$ , то целое число  $k(q)$  делит каждое слагаемое из (20.6.1), кроме  $q - 1$ . Но тогда  $k(q)$  делит и  $q - 1$ , что невозможно, так как  $|k(q)| > q - 1$ . Поэтому  $t = 1$ , т. е.  $Z = R$ . Значит, тело  $R$  коммутативно и является конечным полем.

**Теорема 20.6.2.** (Артин — Цорн.)<sup>1)</sup> *Конечное альтернативное тело является полем Галуа  $GF(p^r)$ .*

**Доказательство.** Изложим сначала элементы теории альтернативных колец. Альтернативным кольцом  $R$  называется система с двумя бинарными операциями — сложением и умножением со следующими свойствами: (1) по сложению эта система — абелева группа, (2) выполняются оба дистрибутивных закона и (3) умножение подчиняется двум ослабленным ассоциативным законам:

$$(xx)y = x(xy), \quad y(xx) = (yx)x. \quad (20.6.2)$$

Кольцо (альтернативное)  $R$  называется телом (альтернативным), если все его ненулевые элементы образуют лупу по умножению. Как отмечалось в предыдущем параграфе, координатная система муфгановой плоскости образует альтернативное тело, в котором вместо (20.6.2) выполняются свойства

$$\begin{aligned} aa^{-1} &= a^{-1}a = 1, \\ a^{-1}(ab) &= b = (ba)a^{-1}, \end{aligned} \quad (20.6.3)$$

причем, как мы показали, из свойств (20.6.3) вытекают свойства (20.6.2).

Для произвольного кольца со свойствами дистрибутивности определим два объекта, а именно *ассоциатор*  $(x, y, z)$  и *коммутатор*  $(x, y)$ , следующим образом:

$$\begin{aligned} (x, y, z) &= (xy)z - x(yz), \\ (xy) &= xy - yx. \end{aligned} \quad (20.6.4)$$

<sup>1)</sup> См. Цорн [1].

Очевидно, ассоциатор тождественно равен нулю в любом ассоциативном кольце, а коммутатор тождественно равен нулю в коммутативном кольце. И ассоциатор, и коммутатор линейны по каждому аргументу. Соотношения (20.6.2) можно теперь переписать в виде

$$(x, x, y) = 0, \quad (y, x, x) = 0. \quad (20.6.5)$$

Из линейности ассоциатора получаем

$$\begin{aligned} 0 &= (x, y + z, y + z) = \\ &= (x, y, y) + (x, y, z) + (x, z, y) + (x, z, z) = \\ &= (x, y, z) + (x, z, y) \end{aligned} \quad (20.6.6)$$

и

$$\begin{aligned} 0 &= (x + y, x + y, z) = \\ &= (x, x, z) + (x, y, z) + (y, x, z) + (y, y, z) = \\ &= (x, y, z) + (y, x, z). \end{aligned}$$

Отсюда получается, что

$$\begin{aligned} (x, y, z) &= -(x, z, y) = (z, x, y) = -(z, y, x) = \\ &= (y, z, x) = -(y, x, z), \end{aligned} \quad (20.6.7)$$

т. е. ассоциатор  $(x, y, z)$  под действием четных подстановок симметрической группы подстановок букв  $x, y, z$  не изменяется, а под действием нечетных подстановок меняет знак на обратный. Именно благодаря этому свойству эти кольца названы *альтернативными* (знакопеременными). Из (20.6.7) немедленно получаем  $(x, y, x) = -(x, x, y) = 0$ , откуда

$$(xy)x = x(yx). \quad (20.6.8)$$

Закон (20.6.8) называется *рефлексивным законом*.

Функция  $h(x_1, \dots, x_n)$  от элементов кольца и со значениями в нем называется *кососимметрической*, если (1) она линейна по всем своим аргументам и (2) обращается в нуль, как только значения какой-нибудь пары аргументов совпадают. Заметим, что из кососимметричности следует свойство альтернативности и что ассоциатор и коммутатор кососимметричны в альтернативном кольце.

Сейчас мы выведем несколько соотношений для альтернативного кольца, причем для доказательства теоремы нам понадобятся лишь некоторые из них, однако и остальные представляют некоторый интерес. Следующее тождество справедливо в любом дистрибутивном кольце:

$$(wx, y, z) - (w, xy, z) + (w, x, yz) = w(x, y, z) + (w, x, y)z. \quad (20.6.9)$$

Определим функцию  $f(w, x, y, z)$  следующим образом:

$$f(w, x, y, z) = (wx, y, z) - x(w, y, z) - (x, y, z)w. \quad (20.6.10)$$

**Лемма 20.6.1.** В любом альтернативном кольце  $R$  функция  $f(w, x, y, z)$ , определенная равенством (20.6.10), кососимметрична и удовлетворяет следующим тождествам:

$$\begin{aligned} 3f(w, x, y, z) &= (w, (x, y, z)) - (x, (y, z, w)) + \\ &\quad + (y, (z, w, x)) - (z, (w, x, y)). \end{aligned} \quad (20.6.11)$$

$$f(w, x, y, z) = ((w, x), y, z) + ((y, z), w, x). \quad (20.6.12)$$

*Доказательство.* Применяя соотношения (20.6.7), перепишем тождество (20.6.9) в виде

$$(wx, y, z) - (xy, z, w) + (yz, w, x) = w(x, y, z) + (w, x, y)z. \quad (20.6.13)$$

Вместо члена  $(wx, y, z)$  подставляем его выражение через функцию  $f$ , получаемое из (20.6.10), и аналогично поступаем с остальными слагаемыми левой части равенства (20.6.13). Тогда

$$f(w, x, y, z) - f(x, y, z, w) + f(y, z, w, x) = F(x, y, z, w), \quad (20.6.14)$$

где  $F(x, y, z, w)$  — правая часть равенства (20.6.11), меняющая поэтому знак при циклической перестановке аргументов. Поэтому из (20.6.14) имеем

$$0 = F(w, x, y, z) + F(x, y, z, w) = f(w, x, y, z) + f(z, w, x, y)$$

и, следовательно,

$$f(w, x, y, z) = -f(z, w, x, y). \quad (20.6.15)$$

Следовательно, функция  $f$  меняет знак при циклической перестановке ее аргументов и, согласно (20.6.10), при перестановке двух ее последних аргументов, а значит, и при перестановке двух любых аргументов. Так как  $f(x, x, y, z) = 0$ , функция  $f$  кососимметрична. В частности, соотношение (20.6.14) сводится к тождеству (20.6.11). Вычитая из (20.6.9) результат перемены местами аргументов  $w$  и  $x$ , получаем

$$((w, x), y, z) = -(\omega, (x, y, z)) + (x, (y, z, w)) + 2f(w, x, y, z).$$

Аналогичными преобразованиями правая часть равенства (20.6.12) при помощи тождества (20.6.11) сводится к левой части.

Лемма 20.6.2. Для любых элементов  $x, y, z$  альтернативного кольца имеем тождества

$$(x^2, y, z) = x(x, y, z) + (x, y, z)x, \quad (20.6.16)$$

$$(x, xy, z) = (x, y, xz) = (x, y, z)x, \quad (20.6.17)$$

$$(x, yx, z) = (x, y, zx) = x(x, y, z) \quad (20.6.18)$$

и так называемые тождества Муффанг:

$$(xy)(zx) = x((yz)x) = (x(yz))x, \quad (20.6.19)$$

$$x(y(xz)) = ((xy)x)z, ((zx)y)x = z(x(yx)). \quad (20.6.20)$$

*Доказательство.* Тождество (20.6.16) получаем из равенства  $f(x, x, y, z) = 0$ . Соотношения (20.6.17) вытекают из того, что  $f(x, y, z, x) = 0$  и  $f(x, z, x, y) = 0$ , а (20.6.18) — из равенств  $f(y, x, x, z) = 0$  и  $f(z, x, x, y) = 0$ . Докажем (20.6.19), применяя тождество (20.6.18):

$$\begin{aligned} (xy)(zx) &= x(y(zx)) + (x, y, zx) = \\ &= x(y(zx)) + x(y, z, x) = x((yz)x). \end{aligned}$$

Первое из равенств (20.6.20) с помощью свойств (20.6.17) получается следующим образом:

$$\begin{aligned} ((xy)x)z &= (xy)(xz) + (xy, x, z) = \\ &= x(y(xz)) + (x, y, xz) - (x, xy, z) = x(y(xz)); \end{aligned}$$

второе же получается аналогично с помощью соотношений (20.6.18).

Теперь мы сможем показать, что для тела законы (20.6.3) следуют из соотношений (20.6.2). Пусть дан элемент  $a \neq 0$ . Тогда существует такой элемент  $u$ , что  $au = 1$ . Отсюда  $a = (au)a = a(ua)$ , и, значит,  $ua = 1$ . Поэтому мы можем записать  $u = a^{-1}$ , причем  $a^{-1}a = aa^{-1} = 1$ . Для произвольных ненулевых элементов  $a$  и  $b$  определим третий элемент  $c$  из соотношения  $b = a^{-1}c$ . Тогда, применяя первое равенство (20.6.20), получаем

$$a^{-1}(ab) = a^{-1}(a(a^{-1}c)) = ((a^{-1}a)a^{-1})c = (1a^{-1})c = a^{-1}c = b.$$

Аналогично равенство  $(ba)a^{-1} = b$  получается из второго соотношения (20.6.20).

Теперь мы имеем более чем достаточно сведений об альтернативных кольцах, чтобы доказать теорему Артина — Цорна. Пусть  $R$  — конечное альтернативное кольцо. Достаточно показать, что конечное альтернативное тело  $R_1$ , порожданное двумя элементами  $b$  и  $c$ , ассоциативно. В самом деле, если это так, то, согласно теореме Веддербарна,  $R_1$  — конечное поле, порожданное одним единственным элементом  $d$ . Поэтому если  $R$  порождается элемен-

тами  $b_1, b_2, \dots, b_s$ , то пара образующих  $b_1, b_2$  порождает конечное поле, обладающее единственным образующим  $c_1$ . Тогда  $R$  порождается элементами  $c_1, b_3, \dots, b_s$ . Повторяя этот процесс несколько раз, мы сведем число образующих кольца  $R$  до единицы, а, значит, кольцо  $R$  ассоциативно и является полем  $GF(p^r)$ .

Рассмотрим подкольцо  $R_1$ , порожденное элементами  $b$  и  $c$ . Оно конечно и не содержит делителей нуля. Пусть  $a_1, \dots, a_t$  — элементы подкольца  $R_1$ , отличные от нуля. Тогда для произвольного элемента  $x \in R_1$  произведения  $xa_1, \dots, xa_t$  все различны, так как  $R_1$  не содержит делителей нуля. Поэтому эти произведения — не что иное, как элементы  $a_1, a_2, \dots, a_t$ , взятые в некотором порядке. Следовательно, для некоторого элемента, скажем  $a_1$ , имеем  $xa_1 = x$ , откуда  $a_1 = 1$  — единица кольца  $R$ . Далее, для некоторого  $a_i$  имеем  $xa_i = 1$ , откуда  $a_i = x^{-1}$ . Следовательно,  $R_1$  — тело. Каждый элемент из  $R_1$  есть сумма одночленов вида  $(x_1 \dots x_r)(x_{r+1} \dots x_n)$ , где каждый сомножитель  $x_i$  равен или  $b$ , или  $c$ , причем скобки могут расставляться всеми возможными способами. Так как справедливы оба дистрибутивных закона, умножение ассоциативно в  $R_1$  тогда и только тогда, когда ассоциативно умножение одночленов. Чтобы это показать, определим рекуррентно одночлен с нормальной расстановкой скобок:

$$\begin{aligned}[x_1 x_2] &= x_1 x_2, \\ &\dots \dots \dots \dots \dots \dots \dots \\ [x_1 \dots x_n] &= [x_1 \dots x_{n-1}] x_n.\end{aligned}\tag{20.6.21}$$

Если удастся показать, что одночлен с произвольной расстановкой скобок равен некоторому одночлену с нормальной расстановкой скобок, то отсюда сразу будет следовать ассоциативность, так как тогда

$$\begin{aligned}([x_1 \dots x_r][y_1 \dots y_s])[z_1 \dots z_t] &= [x_1 \dots x_r y_1 \dots y_s z_1 \dots z_t] = \\ &= [x_1 \dots x_r]([y_1 \dots y_s][z_1 \dots z_t]).\end{aligned}$$

Тот факт, что всякий одночлен равен одночлену с нормальной расстановкой скобок с теми же сомножителями, следующими друг за другом в том же порядке, мы докажем методом полной индукции по длине одночлена. Из соотношений (20.6.5) и (20.6.7) следует, что это верно для одночленов от элементов  $b$  и  $c$  длины 3, так как один из этих двух элементов должен повториться. Поэтому

$$x_1(x_2 x_3) = (x_1 x_2) x_3 = [x_1 x_2 x_3].\tag{20.6.22}$$

Мы должны теперь показать, что

$$[u_1 \dots u_r][v_1 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s],\tag{20.6.23}$$

применяя индукцию по числу  $n = r + s$ , а при фиксированном  $n$  — по  $s$ . При  $s = 1$  утверждение справедливо в силу определения (20.6.21). Предположим, что  $s > 1$ ,  $v_1 = v_s = b$  или  $v_1 = \dots = v_s = c$ . Тогда во втором тождестве (20.6.20)  $z[x(yx)] = [(zx)y]x$  полагаем  $z = [u_1 \dots u_r]$ ,  $v_1 = v_s = x$  и  $[v_2 \dots v_{s-1}] = y$  и, применяя предположение индукции, получаем

$$\begin{aligned} [u_1 \dots u_r][xv_2 \dots v_{s-1}x] &= \{([u_1 \dots u_r]x)[v_2 \dots v_{s-1}]\}x = \\ &= [u_1 \dots u_r v_1 v_2 \dots v_{s-1}]v_s = [u_1 \dots u_r v_1 v_2 \dots v_{s-1} v_s], \end{aligned} \quad (20.6.24)$$

и утверждение (20.6.23) доказано при  $v_1 = v_s$ . Предположим теперь, что  $v_1 \neq v_s$ ; пусть, например,  $v_1 = b$ ,  $v_s = c$ ;  $u_r$  равно либо  $b$ , либо  $c$ . Если  $u_r = b$ , то полагаем

$$x = [u_1 \dots u_{r-1}], \quad u_r = b, \quad v_1 = b, \quad [v_2 \dots v_s] = y.$$

Тогда  $f(x, b, b, y) = 0 = (xb, b, y) - b(x, b, y) - (x, b, b)y$ . Здесь  $(x, b, b) = 0$ , а, по предположению индукции, элементы  $x$ ,  $b$ ,  $y$  ассоциативны, откуда  $(x, b, y) = 0$ . Следовательно,  $(xb, b, y) = 0$ , т. е.  $(xb)(by) = [(xb)b]y$ , откуда

$$\begin{aligned} [u_1 \dots u_{r-1}b][bv_2 \dots v_s] &= ([u_1 \dots u_{r-1}]bb)[v_2 \dots v_s] = \\ &= [u_1 \dots u_{r-1}bb][v_2 \dots v_s] = [u_1 \dots u_r v_1 \dots v_s], \end{aligned} \quad (20.6.25)$$

где последнее равенство получено в силу предположения индукции по  $s$ .

Аналогично, если  $u_r = c$ , полагаем

$$x = [u_1 \dots u_{r-1}], \quad u_r = c, \quad [v_1 \dots v_{s-1}] = z, \quad v_s = c.$$

Теперь  $f(x, c, z, c) = 0 = (xc, z, c) - c(x, z, c) - (c, z, c)x$ . Здесь  $(c, z, c) = 0$ , а  $(x, z, c) = 0$ , по предположению индукции. Отсюда  $(xc, z, c) = 0$ , а это дает  $(xc)(zc) = [(xc)z]c$ , откуда

$$\begin{aligned} [u_1 \dots u_{r-1}c][v_1 \dots v_{s-1}c] &= \\ &= ([u_1 \dots u_{r-1}c][v_1 \dots v_{s-1}])c = \\ &= [u_1 \dots u_{r-1}u_r v_1 \dots v_{s-1}]c = \\ &= [u_1 \dots u_{r-1}u_r v_1 \dots v_{s-1}v_s]. \end{aligned} \quad (20.6.26)$$

Равенствами (20.6.24) — (20.6.26) доказано для всех случаев равенство (20.6.23). Этим доказана ассоциативность кольца  $R_1$  и закончено доказательство теоремы.

## 20.7. Дважды транзитивные группы и почти-поля

Определенный класс групп тесно связан с проективными плоскостями. Это класс дважды транзитивных групп подстановок, в которых только тождественная подстановка оставляет на месте два

символа. Мы будем налагать на эти группы добавочное условие, которое, вообще говоря, не является необходимым, но которое понадобится для нашего доказательства. Это условие составляет пункт (3) или (3') следующей теоремы.

**Теорема 20.7.1.** Пусть  $G$  — такая группа подстановок символов  $c_0, c_1, \dots, c_{n-1}$ , что

- 1) она дважды транзитивна,
  - 2) только единица оставляет неподвижными два символа,
  - 3) существует не более одной подстановки, отображающей элемент  $c_i$  в  $c_j$  и переставляющей все символы, или
- 3') число  $n$  конечно.

Тогда единичная подстановка и подстановки группы  $G$ , переставляющие все символы, образуют транзитивную инвариантную абелеву подгруппу  $A$ . Группа  $G$  изоморфна группе линейных преобразований  $x \rightarrow xt + b$  некоторого почти-поля  $K$ . Обратно, группа линейных преобразований  $x \rightarrow xt + b$ ,  $t \neq 0$ , почти-поля  $K$  изоморфна группе, обладающей свойствами (1), (2), причем линейные преобразования можно рассматривать как подстановки элементов почти-поля  $K$ . Если при  $t \neq 0, 1$  уравнение  $xt + b = x$  всегда имеет решение, то выполняется условие (3), и прямые  $x = c$  и  $y = xt + b$  являются конечными прямыми плоскостями, координатами которой служат элементы почти-поля  $K$ . Подстановка  $\begin{pmatrix} c_0 & c_1 & \dots & c_{n-1} \\ d_0 & d_1 & \dots & d_{n-1} \end{pmatrix}$  из группы  $G$ , рассматриваемая как подстановка элементов из  $K$ , соответствует прямой плоскости  $\pi$ , состоящей из точек  $(c_i, d_i)$ ,  $i = 0, 1, \dots, n - 1$ .

**Доказательство.** Докажем сначала чисто теоретико-групповую часть теоремы, т. е. что подстановки группы  $G$ , переставляющие все символы, вместе с единичной подстановкой образуют транзитивную инвариантную абелеву подгруппу. Для этого докажем ряд лемм.

**Лемма 20.7.1.** В группе  $G$  существует один и только один элемент порядка 2, отображающий друг в друга два определенных символа  $i$  и  $j$ .

Так как группа  $G$  дважды транзитивна, то один такой элемент  $g$  должен найтись. Элемент  $g^2$ , оставляя на месте два символа, равен единице. Если  $h$  — другой элемент с такими же свойствами, как и  $g$ , то элемент  $gh^{-1}$  оставляет неподвижными два символа, откуда  $gh^{-1} = 1$ , т. е.  $g = h$ .

**Лемма 20.7.2.** Все элементы порядка 2 лежат в одном и том же классе сопряженных элементов.

Любой элемент порядка 2 оставляет на месте не более одного символа. Если  $n = 2$ , то такой элемент только один. При  $n \geq 3$

элементы  $g$  и  $h$  порядка 2 должны переставлять некоторый символ  $i$ ,  $g = (i, j) \dots$ ,  $h = (i, k) \dots$ . Для элемента  $x$  вида  $x = \begin{pmatrix} i & j & \dots \\ i & k & \dots \end{pmatrix}$  группы  $G$  имеем  $x^{-1}gx = (i, k) \dots = h$ . Если некоторый элемент порядка 2 оставляет на месте некоторый символ, то и все другие элементы порядка 2 обладают этим свойством.

Теперь мы можем выделить два случая:

Случай 1. Элементы порядка 2 переставляют все символы.

Случай 2. Любой элемент порядка 2 оставляет неподвижным один символ.

**Лемма 20.7.3.** В случае 2 существует один-единственный элемент порядка 2, оставляющий данный символ на месте.

Пусть, как и прежде, элемент  $g = (i, j) \dots$  трансформируется в  $h = (i, k) \dots$  элементом  $x = \begin{pmatrix} i & j & \dots \\ i & k & \dots \end{pmatrix}$ . Если оба элемента  $g$  и  $h$  действуют тождественно на один и тот же символ  $s$ , то элемент  $x$  также должен действовать тождественно на  $s$ , т. е. элемент  $x \neq 1$  оставляет неподвижными два символа  $i$  и  $s$ , что противоречит условию (2). Если элемент  $g$  оставляет на месте символ  $s$ , то путем трансформирования элемента  $g$  произвольным элементом, отображающим  $s$  в  $t$ , можно найти элемент порядка 2, оставляющий неподвижным символ  $t$ .

Заметим, что из этой леммы следует, что элемент  $g = (i, j)(s) \dots$  лежит в центре подгруппы  $H_s$  элементов, оставляющих на месте символ  $s$ .

**Лемма 20.7.4.** Произведение двух различных элементов порядка 2 группы  $G$  есть подстановка, переставляющая все символы.

Пусть  $g^2 = 1$ ,  $h^2 = 1$  и  $g \neq h$ . Предположим, что произведение  $gh$  оставляет на месте символ  $i$ . В силу леммы 20.7.3 элементы  $g$  и  $h$  не могут оба оставлять на месте символ  $i$ , а значит, ни один из них не обладает этим свойством. Но тогда  $g = (i, j) \dots$ ,  $h = (j, i) \dots$  и  $gh = (i)(j) \dots = 1$ , откуда  $g = h$ , что противоречит условию. Значит, элемент  $gh$  перемещает все символы.

**Лемма 20.7.5.** В группе  $G$  существует один-единственный элемент, переставляющий все символы и отображающий некоторый данный символ  $i$  в другой данный символ  $j \neq i$ .

В случае 1 таким элементом является элемент  $g = (i, j) \dots$ . В случае 2 выберем два элемента:  $g = (i) \dots$  порядка 2 и  $h = (i, j) \dots$ . Тогда, согласно лемме 20.7.4, подстановка  $gh$  отображает  $i$  в  $j$  и перемещает все символы. Значит, по крайней мере один такой элемент существует. Но в силу условия (3) найдется не более одного такого элемента. Заметим, что лемма 20.7.5 вытекает из условия (3'). Так как группа  $G$  дважды транзитивна

относительно  $n$  символов, индекс подгруппы, оставляющей на месте символ  $c_0$ , равен  $n$ , причем эта подгруппа  $H_0$  транзитивна относительно остальных  $n - 1$  символов, а так как только единица оставляет на месте два символа, порядок подгруппы  $H_0$  равен  $n - 1$ . Таким образом, порядок группы  $G$  равен  $n(n - 1)$ . Тогда элементы, отображающие  $i$  в  $j$ , образуют левый смежный класс по подгруппе  $H_i$  всех элементов, действующих тождественно на символ  $i$ . Поэтому существует точно  $n - 1$  элементов, отображающих  $i$  в  $j$ . Для данной тройки символов  $i, j, k$  в группе  $G$  существует благодаря свойству двукратной транзитивности элемент  $g = \begin{pmatrix} i & k & \dots \\ j & k & \dots \end{pmatrix}$ , причем такой элемент единственен, так как только единица группы  $G$  оставляет неподвижными два символа. Для данных  $i$  и  $j$  существуют точно  $n - 2$  возможности выбора символа  $k$ , а элементов, отображающих  $i$  в  $j$ , всего  $n - 1$ . Следовательно, один-единственный элемент отображает  $i$  в  $j$  и перемещает все символы.

**Лемма 20.7.6.** В случае 1 любой элемент, переставляющий все символы, имеет порядок 2, причем все такие элементы вместе с единицей образуют инвариантную абелеву подгруппу.

Понятно, что  $g = (i, j) \dots$  — один и, следовательно, единственный элемент, переставляющий все символы и отображающий  $i$  в  $j$ . Если  $g^2 = 1$ ,  $h^2 = 1$ , то при  $g = h$  имеем  $gh = 1$ , в то время как при  $g \neq h$  элемент  $gh$  порядка 2,  $(gh)^2 = 1$ , переставляет все символы, откуда  $hg = gh$ . Поэтому элементы порядка 2 вместе с единицей образуют абелеву группу  $A$ . В силу леммы 20.7.2 подгруппа  $A$  инвариантна. Этим лемма доказана.

**Лемма 20.7.7.** В случае 2 данный элемент  $g$ , переставляющий все символы, можно представить в виде произведения  $g = ab$  двух элементов порядка 2, причем один из сомножителей можно выбрать произвольно.

Пусть  $a^2 = 1$ , где  $a$  — элемент, оставляющий на месте символ  $i$ , и  $g$  — элемент, отображающий  $i$  в  $j$ . Выбираем элемент  $b = (i, j) \dots$ , тогда  $b^2 = 1$  и  $g = ab$ , так как элемент  $ab$  переставляет все символы и отображает  $i$  в  $j$ . Аналогично предположим, что заданы элементы  $g$  и  $b$ , причем  $b$  имеет порядок 2 и оставляет неподвижным символ  $k$ . Если элемент  $g$  отображает  $i$  в  $k$ , то при  $a = (i, k) \dots$  мы имеем  $g = ab$ .

**Лемма 20.7.8.** В случае 2 произведение  $abc$  трех элементов порядка 2 имеет снова порядок 2, при этом  $abc = cba$ .

Если  $a = b$ , лемма очевидна. Если  $b \neq a$ , то  $ab = g = dc$ , где в силу леммы 20.7.7  $d^2 = 1$ . Тогда  $abc = dc^2 = d$ . Так как  $d = d^{-1}$ , то  $abc = c^{-1}b^{-1}a^{-1} = cba$ .

**ЛЕММА 20.7.9.** В случае 2 элементы, переставляющие все символы, вместе с единицей образуют инвариантную абелеву подгруппу.

Пусть элементы  $g$  и  $h$  переставляют все символы. Согласно леммам 20.7.4 и 20.7.7,  $g = ab$ ,  $h = cd$ , где  $a, b, c, d$  — элементы порядка 2. Полагая  $h = eb$  при  $e^2 = 1$ , получаем  $gh^{-1} = ae$ , откуда при  $e = a$  имеем  $gh^{-1} = 1$ , а при  $a \neq e$  элемент  $gh^{-1}$  переставляет все символы. Следовательно, элементы, переставляющие все символы, вместе с единицей образуют подгруппу  $A$ . Применяя лемму 20.7.8, получаем  $gh = (abc)d = (cba)d = c(bad) = c(dab) = hg$ . Это значит, что подгруппа  $A$  абелева. Так как элемент, сопряженный с элементом, переставляющим все символы, также обладает этим свойством, подгруппа  $A$  инвариантна.

Мы сейчас построим алгебраическую систему  $S$ , состоящую из символов  $c_0, c_1, \dots, c_{n-1}$ , переставляемых подстановками из группы  $G$ . Один символ этой системы назовем нулем, а другой — единицей. Пусть, например,  $c_0 = 0$ ,  $c_1 = 1$ . В системе  $S$  определим сложение:

$$y = x + b \quad (20.7.1)$$

тогда и только тогда, когда в подгруппе  $A$  содержится подстановка

$$A_b = \begin{pmatrix} 0 & \dots & x & \dots \\ b & \dots & y & \dots \end{pmatrix}. \quad (20.7.2)$$

В системе  $S$  определим умножение:

$$y = xm \quad (20.7.3)$$

тогда и только тогда, когда в подгруппе  $H_0$ , оставляющей на месте 0, содержится подстановка

$$M_m = \begin{pmatrix} 0 & 1, & \dots & x & \dots \\ 0 & m, & \dots & y & \dots \end{pmatrix}. \quad (20.7.4)$$

Определение сложения правомерно, так как в подгруппе  $A$  есть только один элемент, отображающий 0 в  $b$ . Умножение на  $m \neq 0$  также вполне определено, так как в подгруппе  $H_0$  есть только один элемент, отображающий 1 в  $m$ . Если в подгруппе  $A$  содержатся подстановки

$$\begin{aligned} A_a &= \begin{pmatrix} 0, & \dots, & x \\ a, & \dots, & y \end{pmatrix}, \\ A_b &= \begin{pmatrix} 0, & \dots, & a, & \dots, & y \\ b, & \dots, & c, & \dots, & z \end{pmatrix}, \end{aligned} \quad (20.7.5)$$

то

$$A_a A_b = A_c = \begin{pmatrix} 0 & \dots & x & \dots \\ c & \dots & z & \dots \end{pmatrix}. \quad (20.7.6)$$

Из определения сложения получаем

$$c = a + b, \quad y = x + a, \quad z = y + b, \quad z = x + c, \quad (20.7.7)$$

откуда

$$(x + a) + b = x + (a + b), \quad (20.7.8)$$

т. е. имеет место ассоциативный закон сложения. Очевидно, нейтральным элементом для сложения является подстановка

$$A_0 = \begin{pmatrix} 0 & \dots & 1 & \dots & x & \dots \\ 0 & \dots & 1 & \dots & x & \dots \end{pmatrix};$$

при этом выполняются равенства

$$x + 0 = 0 + x = x. \quad (20.7.9)$$

Кроме того, если для символа  $u$   $A_u = \begin{pmatrix} 0 & \dots & a & \dots \\ u & \dots & 0 & \dots \end{pmatrix}$ , то  $a + u = 0$  и  $u = -a$ . Далее, так как  $A$  — абелева группа, пусть  $A_a A_b = A_b A_a = A_c$ , тогда

$$c = a + b = b + a, \quad (20.7.10)$$

т. е. сложение коммутативно. Таким образом, сложение подчиняется аксиомам абелевой группы. Более того, соответствие  $a \rightarrow A_a$  является изоморфизмом абелевых групп  $S$  и  $A$ .

Аналогичным образом можно показать, рассматривая подстановки из подгруппы  $H_0$ , что ненулевые элементы системы  $S$  образуют мультиликативную группу. Для нуля имеем  $0 \cdot m = 0$ ; кроме этого, положим  $m \cdot 0 = 0$  и  $0 \cdot 0 = 0$ . Пусть теперь  $g$  — произвольная подстановка из группы  $G$ . Если  $(0)g = b$ , то положим  $g_1 = gA_b^{-1}$ . Тогда элемент  $g_1$  оставляет 0 на месте и, значит, принадлежит подгруппе  $H_0$ , скажем  $g_1 = M_m$ . Теперь

$$g = M_m A_b. \quad (20.7.11)$$

Если  $(x)g = y$ , то

$$(x)g = y = xm + b, \quad m \neq 0. \quad (20.7.12)$$

Представление (20.7.11) единственno, так как единица — единственный элемент, принадлежащий подгруппам  $A$  и  $H_0$ , поэтому подстановки из группы  $G$  должны быть линейными преобразованиями (20.7.12) системы  $S$ :

$$x \rightarrow xm + b, \quad m \neq 0. \quad (20.7.13)$$

Отметим следующие соотношения:

$$\begin{aligned} M_m M_t &= M_{mt}, \\ M_m^{-1} A_1 M_m &= A_m. \end{aligned} \quad (20.7.14)$$

Первое соотношение очевидно, а второе вытекает из того, что подстановка  $M_m^{-1} A_1 M_m$  переставляет все символы и 0 отображает в  $m$ , т. е. совпадает с  $A_m$ . Далее получаем

$$M_t^{-1} A_m M_t = A_{mt}, \quad (20.7.15)$$

или, в терминах преобразований системы  $S$ ,

$$(xt^{-1} + m)t = x + mt. \quad (20.7.16)$$

Полагая в последнем равенстве  $x = yt$ , получим дистрибутивный закон

$$(y + m)t = yt + mt. \quad (20.7.17)$$

Итак, система  $S$  по сложению — абелева группа, ее элементы, отличные от нуля, образуют мультиликативную группу, и выполняется правый дистрибутивный закон (20.7.17). Поэтому система  $S$  — почти-поле, а элементы группы  $G$  — линейные преобразования  $S$ . Согласно законам почти-поля, отображения

$$x \rightarrow xm + b, \quad m \neq 0, \quad (20.7.18)$$

обладают тем свойством, что последовательное выполнение двух отображений  $\alpha : x \rightarrow xm_1 + b_1$  и  $\beta : x \rightarrow xm_2 + b_2$  совпадает с отображением

$$\alpha\beta : x \rightarrow x(m_1m_2) + b_1m_2 + b_2. \quad (20.7.19)$$

Обратно, предположим, что задано некоторое почти-поле  $S$ . Линейные преобразования (20.7.18) почти-поля  $S$  образуют мультиликативную группу  $G$  с законом умножения (20.7.19). Пусть  $r$  и  $s$  ( $r \neq s$ ) — два различных элемента из  $S$ . Тогда отображение

$$g : x \rightarrow x(r - s) + s \quad (20.7.20)$$

— такой элемент группы  $G$ , что (0)  $g = s$  и (1)  $g = r$ . Следовательно, группа  $G$  дважды транзитивна. Элемент из  $G$ , оставляющий на месте какие-либо два символа, сопряжен с элементом, оставляющим на месте символы 0 и 1. Но если отображение  $x \rightarrow xm + b$  тождественно в нуле и в единице, то мы последовательно находим, что  $b = 0$ ,  $m = 1$ , т. е. что это отображение тождественно. Следовательно, тождественное отображение является единственным отображением, оставляющим на месте два символа. Преобразование  $x \rightarrow x + (c - b)$  переставляет все символы и отображает данный элемент  $b$  в данный элемент  $c$ . Если уравнение

$xm + b = x$  при  $m \neq 0, 1$  всегда имеет решение, то единственными преобразованиями, переставляющими все символы, являются преобразования вида  $x \rightarrow x + t$ , а среди последних только преобразование  $x \rightarrow x + (c - b)$  отображает заданный элемент  $b$  в заданный элемент  $c$ , т. е. условие (3) теоремы 20.7.1 выполнено. Но тогда одно из уравнений  $(xm + b)r = xr$ ,  $xs + t = xr$  всегда имеет решение (причем единственное), а это и означает, что система  $S$ , рассматриваемая как система Веблена—Веддербарна, является системой координат плоскости, конечными прямыми которой являются прямые  $x = c$  и  $y = xm + b$ . Этим завершается доказательство теоремы.

Как уже отмечалось, условие (3) автоматически выполняется, если  $G$  — конечная группа подстановок. Поэтому нахождение всех конечных дважды транзитивных групп подстановок, в которых только единичная подстановка оставляет на месте два символа, эквивалентно нахождению всех конечных почти-полей. Последняя задача была решена Цассенхаузом [2]. Рассмотрим ее решение.

Пусть  $K$  — конечное почти-поле. Если мультиплекативная группа почти-поля  $K$  абелева, то в  $K$  выполняются оба дистрибутивных закона, т. е.  $K$  — поле Галуа  $GF(p^r)$ . Поэтому этот случай в дальнейшем мы исключаем и будем предполагать, что умножение в  $K$  некоммутативно. Тогда левый дистрибутивный закон в  $K$  не может иметь места, так как в противном случае, согласно теореме Веддербарна, почти-поле  $K$  было бы конечным ассоциативным телом, а значит, и конечным полем  $GF(p^r)$ . В дальнейшем мы будем пользоваться следующими обозначениями предыдущей теоремы:  $K$  — конечное почти-поле, состоящее из  $n$  элементов,  $G$  — дважды транзитивная группа степени  $n$ , в которой только единичная подстановка оставляет на месте два символа.  $G$  является группой линейных преобразований

$$g : x \rightarrow xm + b, \quad m \neq 0. \quad (20.7.21)$$

$A$  — инвариантная абелева подгруппа группы  $G$ , состоящая из единицы и всех подстановок, переставляющих все  $n$  символов.  $H_0 = M$  — подгруппа всех подстановок, оставляющих на месте символ 0. Подгруппа  $A$  изоморфна аддитивной группе почти-поля  $K$ , а подгруппа  $M$  — мультиплекативной группе  $K^*$ , состоящей из  $n - 1$  ненулевых элементов почти-поля  $K$ .

Лемма 20.7.K1. Пусть  $A$  — элементарная абелева группа и  $n = p^r$ , где  $p$  — простое число. Отличные от 1 элементы группы  $A$  сопряжены между собой при помощи элементов из  $M$ .

$A$  — абелева группа, причем, согласно (20.7.14),  $A_m = M_m^{-1} A_1 M_m$ . Значит, все элементы группы  $A$ , за исключением единицы, сопряжены между собой при помощи элементов из  $M$ .

Но так как группа  $A$  должна содержать элемент простого порядка, например  $p$ , то порядок всех отличных от единицы элементов группы  $A$  равен  $p$ . Поэтому группа  $A$  — элементарная абелева. Так как она регулярна и ее порядок равен  $n$ , то  $n = p^r$ .

**Лемма 20.7.К2.** Элементы группы  $M$  являются автоморфизмами группы  $A$ , и каждый автоморфизм из  $M$ , отличный от тождественного, оставляет на месте только элемент 0 почти-поля  $K$ .

Элементы из  $M$  — это подстановки вида  $a \rightarrow am$  элементов из  $K$ , а каждая из них, кроме тождественной, является автоморфизмом аддитивной группы  $A$ , действующим тождественно только на элемент 0.

**Лемма 20.7.К3.** Если числа  $q$  и  $s$  простые, то подгруппы группы  $M$  порядков  $q^2$  и  $qs$  цикличны.

Заметим сначала следующее: если  $(x_1, \dots, x_k)$  — цикл подстановки  $M_m$ , то  $x_1m = x_2, x_2m = x_3, \dots, x_km = x_1$ , откуда  $(x_1 + \dots + x_k)m = x_1 + \dots + x_k$ , т. е. если  $m \neq 1$ , то  $x_1 + \dots + x_k = 0$ . Предположим теперь, что группа  $M$  обладает нециклической подгруппой  $W$  порядка  $q^2$ . Тогда  $W$  — прямое произведение двух групп порядка  $q$ . Пусть  $W$  порождается элементами  $x$  и  $y$ . Рассмотрим некоторую область транзитивности группы  $W$ , состоящую, конечно, из  $q^2$  символов. Тогда элементы  $x$  и  $y$  имеют вид

$$x = (a_1 a_2 \dots a_q) (a_{q+1} \dots a_{2q}) \dots (a_{q^2-q+1} \dots a_{q^2}),$$

$$y = (a_1 a_{q+1} a_{2q+1} \dots a_{q^2-q+1}) \dots (a_l a_{q+l} \dots a_{q^2-q+l}) \dots$$

Элемент  $xy^j$  обладает следующей областью транзитивности, содержащей  $a_1$ :

$$(a_1 a_{2+jq} a_{3+2jq} \dots a_{q+j(q-1)q}).$$

Учитывая замечание о циклах, получаем

$$a_1 + a_{2+jq} + \dots + a_{q+j(q-1)q} = 0, \quad (20.7.22)$$

$$a_1 + a_{q+1} + a_{2q+1} + \dots + a_{q^2-q+1} = 0. \quad (20.7.23)$$

Суммируя равенства (20.7.22) по  $j = 0, 1, \dots, q-1$  и прибавляя равенство (20.7.23), замечаем, что каждое  $a_i \neq a_1$  встречается в точности один раз, а  $a_1$  встречается  $(q+1)$  раз. Следовательно,

$$qa_1 + (a_1 + a_2 + \dots + a_{q^2}) = 0. \quad (20.7.24)$$

Суммируя элементы всех циклов подстановки  $x$ , получаем

$$a_1 + a_2 + \dots + a_{q^2} = 0, \quad (20.7.25)$$

откуда

$$qa_1 = 0. \quad (20.7.26)$$

Но порядок группы  $M$  равен  $n - 1 = p^r - 1$ , значит, числа  $q$  и  $p$  взаимно просты. Поэтому из (20.7.26) получаем  $a_1 = 0$ , что невозможно. Следовательно, группа  $M$  не может содержать нециклической подгруппы порядка  $q^2$ .

Аналогично если  $M$  содержит нециклическую группу  $W$  порядка  $qs$ , где  $q < s$ , то последняя порождается элементами  $x$  и  $y$ , удовлетворяющими соотношениям

$$\begin{aligned} x^s &= 1, \quad y^q = 1, \quad q/s = 1, \\ y^{-1}xy &= x^t, \quad t^q \equiv 1 \pmod{s}. \end{aligned} \quad (20.7.27)$$

Так как  $M$  — регулярная группа, подгруппа  $W$  обладает областью транзитивности, содержащей  $qs$  символов.  $W$  содержит одну подгруппу порядка  $s$  и  $s$  подгруппы порядка  $q$ . Выберем в каждой из этих подгрупп по одному циклу, содержащему данный символ  $a_1$ :

$$(a_1, a_2, \dots, a_s),$$

$$(a_1, b_{11}, \dots, b_{1,q-1}),$$

$$(a_1, b_{21}, \dots, b_{2,q-1}),$$

...

$$(a_1, b_{s1}, \dots, b_{s,q-1}).$$

Каждый из  $qs$  символов, кроме  $a_1$ , встречается в этих циклах только один раз, а символ  $a_1$  встречается  $s+1$  раз. Но сумма всех  $qs$  букв равна нулю, так как эти циклы, взятые вместе, образуют некоторую подстановку  $x$ . Отсюда следует, что  $sa_1 = 0$ , а так как  $s/p^r = 1$ , то  $a_1 = 0$ , что противоречит условию. Значит, группа  $M$  не содержит нециклической подгруппы порядка  $qs$ .

**Лемма 20.7.К4.** *Силовская подгруппа группы  $M$  нечетного порядка циклична. Силовская 2-подгруппа группы  $M$  циклична или же является обобщенной группой кватернионов.*

Как было показано (теорема 12.5.2),  $p$ -группа  $P$  циклична, если  $p \neq 2$  и если группа  $P$  не содержит нециклических подгрупп порядка  $p^2$ . При  $p = 2$  группа  $P$  или циклична, или является обобщенной группой кватернионов.

Предположим, что группа  $M$  содержит такую циклическую подгруппу  $C$ , что фактор-группа  $M/C$  также циклична. Согласно лемме 20.7.К4 и теореме 9.4.3, группа  $M$  обладает этим свойством, если она не содержит силовской 2-подгруппы, изоморфной обобщенной группе кватернионов; группа  $M$  обладает этим свойством, даже если она является прямым произведением обобщенной группы кватернионов и группы нечетного порядка. Теорема 20.7.2 указывает все конечные почти-поля  $K$ , группа  $M$  которых обладает этим свойством. Цассенхауз показал, что существует еще

точно семь других конечных почти-полей; ниже мы их перечислим. Доказательство этого факта читатель может найти в статье Цассенхауза [2].

**Теорема 20.7.2.** Пусть  $q = p^h$ , где  $p$  — простое число, и пусть  $v$  — такое целое число, что все его простые делители делят число  $q - 1$  и  $v \not\equiv 0 \pmod{4}$ , если  $q \equiv 3 \pmod{4}$ . Тогда для  $r = hv$  мы можем следующим образом построить почти-поле  $K$ , состоящее из  $n = p^r$  элементов, исходя из поля Галуа  $GF(p^r)$ .

1) Элементами почти-поля  $K$  являются элементы поля  $GF(p^r)$ :

2) Сложение в  $K$  производится по тому же правилу, что и в поле  $GF(p^r)$ .

3) Произведение  $w \circ u$  в почти-поле  $K$  определяется в терминах произведения  $x \cdot y$  поля  $GF(p^r)$  следующим образом:

пусть  $z$  — фиксированный первообразный корень поля  $GF(p^r)$ ; если  $u = z^{rv+j}$ , то сравнением  $q^i \equiv 1 + j(q - 1) \pmod{v(q - 1)}$  однозначно определяется натуральное число  $i$  по модулю  $v$ . Тогда произведение  $w \circ u$  определяем так:

$$w \circ u = u \cdot w^{q^i}.$$

4) Центром почти-поля  $K$  является подполе  $GF(q)$ . Любое почти-поле  $K$  из  $n = p^r$  элементов можно построить описанным выше способом из поля  $GF(p^r)$ , если почти-поле  $K$  обладает тем свойством, что его мультипликативная группа  $M$  содержит такую инвариантную циклическую подгруппу  $C$ , что фактор-группа  $M/C$  также циклична.

Кроме описанных в этой теореме конечных почти-полей, как показал Цассенхауз, существует еще ровно семь других. Все они состоят из  $p^2$  элементов. Чтобы их определить, достаточно задать образующие элементы мультипликативной группы  $M$  как матричные преобразования аддитивной группы с двумя образующими. Выпишем их в таком же порядке, как они выписаны у Цассенхауза:

$$\text{I. } n = 5^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -2 \\ -1 & -2 \end{pmatrix},$$

$$M \cong M(2, 3);$$

$$\text{II. } n = 11^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 5 \\ -5 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix},$$

$$M \cong M(2, 3) \times (C);$$

$$\text{III. } n = 7^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 3 \\ -1 & -2 \end{pmatrix}, \\ M \cong G_3;$$

$$\text{IV. } n = 23^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -6 \\ 12 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \\ M \cong G_3 \times (C);$$

$$\text{V. } n = 11^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 2 & 4 \\ 1 & -3 \end{pmatrix}, \\ M \cong M(2, 5);$$

$$\text{VI. } n = 29^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & -7 \\ -12 & -2 \end{pmatrix}, \quad C = \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}, \\ M \cong M(2, 5) \times (C);$$

$$\text{VII. } n = 59^2, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 9 & 15 \\ -10 & -10 \end{pmatrix}, \quad C = \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \\ M \cong M(2, 5) \times (C).$$

Здесь группа  $M(2, 3)$  в случае I имеет порядок 24; группа  $M(2, 5)$  в случае V имеет порядок 120, а группа  $G_3$  в случае III имеет порядок 48. Группа  $M(2, 5)$  обладает центром  $Z$  порядка 2, а фактор-группа  $M(2, 5)/Z$  является простой группой порядка 60.

## 20.8. Конечные плоскости.

### Теорема Брука — Райзера

Как мы показали выше, конечная проективная плоскость порядка <sup>1)</sup>  $n$  обладает следующими свойствами:

- 1) она содержит всего  $n^2 + n + 1$  прямых,
- 2) она содержит  $n^2 + n + 1$  точек,
- 3) каждая из ее прямых состоит из  $(n + 1)$  точек,
- 4) каждая точка принадлежит  $(n + 1)$  прямым,
- 5) через две различные точки проходит одна и только одна прямая,
- 6) две различные прямые пересекаются в одной и только одной точке.

<sup>1)</sup> Под порядком конечной проективной плоскости автор понимает число точек каждой прямой плоскости (двойственное понятие — число прямых, пересекающихся в одной точке), уменьшенное на единицу. — Прим. перев.

При доказательстве того факта, что некоторая система является конечной проективной плоскостью, полезно помнить, что некоторая система „точек“ и „прямых“, удовлетворяющая части из перечисленных выше свойств, есть конечная плоскость порядка  $n$ , удовлетворяющая также и остальным свойствам.

**Теорема 20.8.1.** *Система точек и прямых, удовлетворяющая условиям (1), (3), (5), или, двойственно, условиям (2), (4), (6), является конечной плоскостью порядка  $n$ , обладающей и остальными тремя свойствами.*

**Доказательство.** Предположим, что система удовлетворяет условиям (1), (3), (5). Пусть точка  $P_i$  лежит на  $m_i$  прямых. Тогда точка  $P_i$  соединена с  $n$  другими точками на каждой из  $m_i$  прямых. С другой стороны, в силу свойства (5) других точек в этой системе нет. Значит, она состоит из  $1 + nm_i$  точек. Отсюда следует, что число  $m = m_i$  не зависит от выбора точки  $P_i$ . Учитывая инцидентности точек и прямых, находим

$$(n+1)(n^2+n+1) = m(1+mn),$$

так как, с одной стороны, на каждой из  $n^2+n+1$  прямых содержится по  $n+1$  точек, а, с другой стороны, через каждую из  $1+mn$  точек проходят  $m$  прямых. Отсюда  $m = n+1$ , и свойства (2), (4) установлены. В силу свойства (5) не существует двух различных прямых, пересекающихся более чем в одной точке. Чтобы убедиться в справедливости утверждения (6), достаточно показать, что точка пересечения двух прямых существует всегда. Точка  $P$  данной прямой  $L$  лежит на  $n$  других прямых, и это справедливо для каждой из  $n+1$  точек прямой  $L$ . Таким образом, прямая  $L$  пересекается с  $n(n+1) = n^2+n$  другими прямыми, но, кроме них, других прямых не существует. Следовательно, свойство (6) справедливо. Итак, из свойств (1), (3), (5) следуют остальные. В силу принципа двойственности, наоборот, из свойств (2), (4), (6) получаются свойства (1), (3), (5).

**Следствие 20.8.1.** *Для конечной системы Веблена — Веддербарна условие (4) теоремы 20.4.6, т. е. что при  $r \neq s$  уравнение  $xr = xs + t$  имеет единственное решение, является следствием остальных условий.*

Действительно, не пользуясь условием (4), мы убеждаемся, что для такой системы свойства (1), (3), (5) имеют место.

Оказывается, что не для любого натурального  $n$  существуют конечные плоскости порядка  $n$ . Если верна одна гипотеза, высказанная Эйлером, то не существует плоскостей порядка  $n$ , где  $n \equiv 2 \pmod{4}$ ,  $n \neq 2$ . В 1900 году Тарри [1] методом проб и ошибок показал, что плоскости порядка 6 не существует. Для любой степени  $n = p^r$  простого числа  $p$  существует поле  $GF(p^r)$  и, значит, по теореме 20.5.5 существует дезаргова плоскость

порядка  $p^r$ . Существуют системы Холла порядков  $p^{2r}$ , и при  $p^{2r} \neq 4$  им соответствуют недезарговы плоскости. Почти-полям также соответствуют недезарговы плоскости. Альберт [1] указал, как строить неассоциативные тела, состоящие из  $p^r$  элементов при  $p \neq 2$  и  $r > 2$ . Им, конечно, в силу теоремы 20.4.6 соответствуют недезарговы плоскости таких же порядков. Мы дадим простое построение Альберта для степеней  $p^r$ , где  $p \neq 2$ ,  $r$  нечетно и больше единицы.

**Теорема 20.8.2.** (АЛЬБЕРТ.) *Пусть  $p$  — нечетное простое число,  $r$  — нечетное число, большее единицы. Тогда, исходя из поля Галуа  $GF(p^r)$ , можно построить неассоциативное тело  $N$ , состоящее из  $p^r$  элементов.*

**Доказательство.** Сначала определим новое произведение  $(x, y)$  элементов поля  $GF(p^r)$ , где  $p \neq 2$  и число  $r \geq 1$  нечетно, по правилу

$$(x, y) = \frac{1}{2}(xy^p + x^py). \quad (20.8.1)$$

Так как отображение  $x \rightarrow x^p$  является автоморфизмом поля  $GF(p^r)$ , нетрудно убедиться в том, что так определенное умножение удовлетворяет дистрибутивным законам. Покажем, что если  $x \neq 0$  и  $y \neq 0$ , то  $(x, y) \neq 0$ . Предположим противное, т. е. что  $(x, y) = 0$  при  $x \neq 0$ ,  $y \neq 0$ . Тогда находим, что

$$xy^p = -x^py, \quad (20.8.2)$$

откуда

$$y^{p-1} = -x^{p-1}. \quad (20.8.3)$$

Так как числа  $p$  и  $r$  нечетны, число  $m = (p^r - 1)/(p - 1)$  также нечетно. Возводя обе части равенства (20.8.3) в степень  $m$ , получаем

$$1 = y^{p^r-1} = -x^{p^r-1} = -1, \quad (20.8.4)$$

что противоречит условию  $p \neq 2$ . Итак, если  $x \neq 0$ ,  $y \neq 0$ , то  $(x, y) \neq 0$ . Так как наша система конечна и не содержит делителей нуля, она должна быть квазигруппой. При этом для данного элемента  $x \neq 0$  существует единственный элемент  $u \neq 0$ , такой, что

$$x = (u, 1) = \frac{1}{2}(u + u^p). \quad (20.8.5)$$

Теперь определим взаимно однозначное отображение  $\alpha$ :

$$x \rightarrow x\alpha = u, \quad (20.8.6)$$

если  $u$  и  $x$  удовлетворяют условию (20.8.5).

Определим, далее, систему  $D$ , элементами которой являются элементы поля Галуа  $GF(p^r)$ . Сложение в ней определяется сло-

жением в этом поле, а умножение  $x \circ y$  определяется следующим образом:

$$x \circ y = (x\alpha, y\alpha); \quad (20.8.7)$$

здесь произведение в правой части определяется формулой (20.8.1), а отображение  $\alpha$  — (20.8.6). Единица 1 поля  $GF(p^r)$  остается единицей и в системе  $D$ , так как проверка показывает, что

$$x \circ 1 = 1 \circ x = x. \quad (20.8.8)$$

Умножение в системе  $D$  коммутативно, но неассоциативно. Альберт показал, что умножение степеней элемента, не принадлежащего простому полю  $F_p$ , неассоциативно.

Изложенные методы позволяют построить недезарговы плоскости порядков  $p^r$  для всех  $r \geq 2$  и  $p \neq 2$ , а также порядков  $2^r$ , где  $r$  — четное число и  $r \geq 4$ . Было доказано, что существует только одна дезаргова плоскость каждого из порядков 2, 3, 4, 5, 7, 8. Известны другие конечные плоскости, в частности плоскости Хьюгеса, которые будут рассмотрены ниже. Однако не было построено ни одной конечной плоскости, порядок которой отличен от простого числа или его степени.

Кроме изолированного результата Тарри о несуществовании плоскости порядка 6, не было известно никаких ограничений на порядки плоскостей до 1949 года, когда Брук и Райзер [1] доказали следующую основную теорему.

**Теорема 20.8.3.** *Если  $n \equiv 1, 2 \pmod{4}$  и  $n$  нельзя представить в виде суммы квадратов двух целых чисел, т. е. в виде  $n = a^2 + b^2$ , то плоскостей порядка  $n$  не существует.*

**Доказательство.** Здесь приводится упрощенное доказательство этой теоремы, полученное из первоначального благодаря использованию методов Чоула и Райзера [1]. Пусть  $N = n^2 + n + 1$ . Сопоставим символам  $x_i$  ( $i = 1, \dots, N$ ) точки  $P_i$  ( $i = 1, \dots, N$ ) плоскости  $\pi$  порядка  $n$ . Пусть  $L_j$  ( $j = 1, \dots, N$ ) — прямые плоскости  $\pi$ . Определим числа инцидентности  $a_{ij}$  следующим образом:

$$\begin{aligned} a_{ij} &= 1, \text{ если } P_i \in L_j, \\ a_{ij} &= 0, \text{ если } P_i \notin L_j, \quad i, j = 1, \dots, N. \end{aligned} \quad (20.8.9)$$

Матрица  $A$  инцидентности плоскости  $\pi$  определяется как матрица

$$A = (a_{ij}), \quad i, j = 1, \dots, N. \quad (20.8.10)$$

Матрица инцидентности  $A$  подчиняется следующим основным соотношениям:

$$AA^T = A^TA = nI + S, \quad (20.8.11)$$

где  $I$  — единичная матрица, а  $S$  — матрица, состоящая только из единиц.

Пусть  $AA^T = C$ . Если  $C = (c_{rs})$ , то

$$c_{rs} = \sum_{j=1}^N a_{rj} a_{sj}. \quad (20.8.12)$$

Здесь  $c_{rr} = n + 1$ , так как точка  $P_r$  лежит точно на  $n + 1$  прямой и так как из чисел  $a_{rj}$  ( $j = 1, \dots, N$ ) точно  $n + 1$  равны 1, а остальные равны 0. Далее, при  $r \neq s$  имеем  $c_{rs} = 1$ , так как  $a_{rj} a_{sj} = 0$ , если только оба сомножителя  $a_{rj}$  и  $a_{sj}$  не равны единице. Но равенство  $a_{rj} = a_{sj} = 1$  означает, что прямая  $L_j$  содержит как точку  $P_r$ , так и точку  $P_s$ . Но данные точки  $P_r$  и  $P_s$  определяют одну-единственную прямую  $L_j$ , проходящую через них. Значит,  $c_{rr} = n + 1$ ,  $c_{rs} = 1$  при  $r \neq s$ . Поэтому  $AA^T = nI + S$ . Аналогичные рассуждения показывают, что  $A^T A = nI + S$ .

Соотношение  $AA^T = nI + S$  можно истолковать в терминах квадратичных форм. Прямой  $L_j$  сопоставляем линейную форму, которую также обозначим через  $L_j$ :

$$L_j = \sum_{i=1}^N a_{ij} x_i, \quad j = 1, \dots, N. \quad (20.8.13)$$

Тогда

$$\begin{aligned} L_1^2 + \dots + L_N^2 &= \\ &= n(x_1^2 + \dots + x_N^2) + (x_1 + \dots + x_N)^2. \end{aligned} \quad (20.8.14)$$

Это тождество действительно имеет место, так как в сумме  $L_j$ ,  $j = 1, \dots, N$ , каждое слагаемое  $x_r$  встречается с коэффициентом 1 точно  $n + 1$  раз, вследствие того что каждая точка лежит точно на  $n + 1$  прямых. Каждое слагаемое вида  $2x_r x_s$  встречается в сумме  $L_1^2 + \dots + L_N^2$  только один раз, так как существует ровно одна прямая  $L_j$ , содержащая точки  $P_r$  и  $P_s$ . Этим доказано тождество (20.8.14). Предположим теперь, что  $n \equiv 1, 2 \pmod{4}$ . Тогда  $N = n^2 + n + 1 \equiv 3 \pmod{4}$ . Заметим, что равенство (20.8.14) можно переписать в виде

$$\begin{aligned} L_1^2 + \dots + L_N^2 &= n \left( x_2 + \frac{x_1}{n} \right)^2 + \dots \\ &\quad \dots + n \left( x_N + \frac{x_1}{n} \right)^2 + (x_2 + \dots + x_N)^2. \end{aligned} \quad (20.8.15)$$

В этом легко убедиться, заметив, что коэффициент при  $x_1^2$  в правой части равенства (20.8.15) равен  $(N - 1)/n = n + 1$ . Произведем замену переменных в равенстве (20.8.15), положив

$$y_1 = x_2 + \dots + x_N, \quad y_2 = x_2 + \frac{x_1}{n}, \dots, \quad y_N = x_N + \frac{x_1}{n}. \quad (20.8.16)$$

При этом переменные  $x_i$  можно рационально выразить через  $y_i$ . Теперь перепишем (20.8.15) в виде

$$L_1^2 + \dots + L_N^2 = y_1^2 + ny_2^2 + ny_3^2 + \dots + ny_N^2. \quad (20.8.17)$$

Применяем теорему Лагранжа о том, что любое натуральное число можно представить в виде суммы квадратов четырех целых чисел<sup>1)</sup>. Имеем

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2, \quad (20.8.18)$$

а также знаменитое тождество Лагранжа:

$$\begin{aligned} (a_1^2 + a_2^2 + a_3^2 + a_4^2)(y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2) &= \\ &= (a_1 y_i + a_2 y_{i+1} + a_3 y_{i+2} + a_4 y_{i+3})^2 + \\ &+ (a_1 y_{i+1} - a_2 y_i + a_3 y_{i+3} - a_4 y_{i+2})^2 + \\ &+ (a_1 y_{i+2} - a_3 y_i + a_4 y_{i+1} - a_2 y_{i+3})^2 + \\ &+ (a_1 y_{i+3} - a_4 y_i + a_2 y_{i+2} - a_3 y_{i+1})^2 = \\ &= z_i^2 + z_{i+1}^2 + z_{i+2}^2 + z_{i+3}^2. \end{aligned} \quad (20.8.19)$$

Как видно из преобразований (20.8.19), величины  $z_i, z_{i+1}, z_{i+2}, z_{i+3}$  рационально выражаются через  $y_i, y_{i+1}, y_{i+2}, y_{i+3}$ . Учитывая, что  $N \equiv 3 \pmod{4}$ , и применяя тождества (20.8.18) и (20.8.19) к равенству (20.8.17), получаем

$$L_1^2 + \dots + L_N^2 = z_1^2 + z_2^2 + \dots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2). \quad (20.8.20)$$

Заметим, что первоначально каждое из выражений  $L_j, j = 1, \dots, N$ , было линейной формой от переменных  $x_i$  с рациональными (фактически с целыми) коэффициентами, а поэтому они являются линейными формами с рациональными коэффициентами от переменных  $y_i$ , а значит, и от независимых переменных  $z_1, \dots, z_N$ . Так как равенство (20.8.20) является тождеством относительно переменных  $z_i$ , оно останется справедливым, если некоторые из переменных  $z_i$  специализировать как линейные комбинации остальных. Пусть

$$L_1 = b_1 z_1 + \dots + b_N z_N. \quad (20.8.21)$$

Пложим  $L_1 = z_1$ , если  $b_1 \neq 1$  и  $L_1 = -z_1$ , если  $b_1 = 1$ . При такой специализации  $z_1$  можно представить в виде линейной комбинации от  $z_2, \dots, z_N$  с рациональными коэффициентами. Тогда  $L_1^2 = z_1^2$ , и при нашей специализации  $z_1$  получаем

$$L_2^2 + \dots + L_N^2 = z_2^2 + \dots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2). \quad (20.8.22)$$

<sup>1)</sup> Доказательство этой теоремы можно найти, например, в книге И. В. Арнольда „Теория чисел“, Госучпедгиз, М., 1939.—Прим. перев.

Продолжая таким образом, получаем последовательно  $L_2 = \pm z_2, \dots, L_{N-2} = \pm z_{N-2}$  и выражаем линейно переменные  $z_2, \dots, z_{N-2}$  через последующие переменные. Наконец, получим

$$L_{N-1}^2 + L_N^2 = n(z_{N-1}^2 + z_N^2), \quad (20.8.23)$$

где  $L_{N-1}$  и  $L_N$  — линейные формы от независимых переменных  $z_{N-1}$  и  $z_N$  с рациональными коэффициентами. Придадим переменным  $z_{N-1}$  и  $z_N$  значения, равные целым положительным числам, кратным общему знаменателю коэффициентов формы  $L_{N-1}$  и формы  $L_N$ . Тогда в равенстве (20.8.23) будут фигурировать только целые числа. Целое число  $n$ , являясь частным двух целых чисел, каждое из которых есть сумма двух квадратов в силу известного результата из теории чисел<sup>1)</sup>, само представимо в виде суммы двух квадратов. Теперь мы имеем

$$n = a^2 + b^2, \quad (20.8.24)$$

и теорема доказана. Существует частичное обращение этой теоремы.

**Теорема 20.8.4.** *Если  $n \equiv 0, 3 \pmod{4}$  или  $n \equiv 1, 2 \pmod{4}$  и  $n = a^2 + b^2$ , то существуют линейные формы  $L_j, j = 1, \dots, N$ , от  $x_1, \dots, x_N$  с рациональными коэффициентами, такие, что*

$$L_1^2 + \dots + L_N^2 = n(x_1^2 + \dots + x_N^2) + (x_1 + \dots + x_N)^2.$$

Существует также квадратная рациональная матрица  $A$  порядка  $N$ , обладающая свойством  $AA^T = A^TA = nI + S$ .

*Доказательство.* Если  $n \equiv 0, 3 \pmod{4}$ , мы можем, используя равенства (20.8.18) и (20.8.19), привести соотношение (20.8.17) к виду

$$L_1^2 + \dots + L_N^2 = z_1^2 + \dots + z_N^2, \quad (20.8.25)$$

откуда видно, что линейные формы  $L_i = z_i$ , конечно, удовлетворяют теореме. Если  $n \equiv 1, 2 \pmod{4}$  и  $n = a^2 + b^2$ , мы можем использовать тождество

$$(a^2 + b^2)(y_i^2 + y_{i+1}^2) = (ay_i + by_{i+1})^2 + (by_i - ay_{i+1})^2 = z_i^2 + z_{i+1}^2 \quad (20.8.26)$$

вместо тождества (20.8.19), чтобы привести соотношение (20.8.17) к виду (20.8.25). Если

$$L_j = \sum_i b_{ij} x_i, \quad j = 1, \dots, N, \quad (20.8.27)$$

<sup>2)</sup> См., например, Арнольд И. В., Теория чисел, Госучпедгиз, М., 1939. — Прим. перев.

— найденные линейные формы, то, полагая  $A = (b_{ij})$ ,  $i, j = 1, \dots, N$ , мы получаем

$$AA^T = nI + S, \quad (20.8.28)$$

однако, вообще говоря,  $A^TA \neq nI + S$ . Труднее показать, что при условиях этой теоремы существует рациональная матрица  $A$ , удовлетворяющая обоим соотношениям  $AA^T = nI + S = A^TA$ . Это и даже несколько большее было показано Холлом и Райзером [1].

## 20.9. Коллинеации в конечных плоскостях

Если коллинеация  $\alpha$  плоскости  $\pi$  оставляет на месте две точки, то она оставляет, также на месте прямую, соединяющую их; аналогично если коллинеация  $\alpha$  не двигает две прямые, то она оставляет неподвижной также точку их пересечения. Следовательно, если коллинеация  $\alpha$  оставляет на месте некоторый четырехугольник, то  $\alpha$  отображает на себя некоторую собственную подплоскость плоскости  $\pi$ . Следующая теорема дает некоторые сведения о возможных порядках подплоскостей.

**Теорема 20.9.1.** (Брук.) *Если плоскость  $\pi$  порядка  $n$  обладает подплоскостью  $\pi^*$  порядка  $m$ , то  $n = m^2$  или  $n \geq m^2 + m$ .*

**Доказательство.** Пусть  $L$  — прямая подплоскости  $\pi^*$ , а  $P$  — точка прямой  $L$ , не принадлежащая  $\pi^*$ . Тогда  $m+1$  точек плоскости  $\pi^*$  лежат на прямой  $L$ , а  $m^2$  точек этой же плоскости не лежат на прямой  $L$ . Соединяя точку  $P$  с каждой из этих  $m^2$  точек плоскости  $\pi^*$ , не принадлежащих  $L$ , мы получаем  $m^2$  прямых, проходящих через точку  $P$ , причем все они различны, так как если бы две такие прямые совпадали, то эта прямая  $K$  содержала бы две различные точки подплоскости  $\pi^*$  и, значит, принадлежала бы подплоскости  $\pi^*$ . Но тогда точка  $P$  как точка пересечения прямых  $K$  и  $L$  была бы точкой подплоскости  $\pi^*$ , что противоречит предположению. Итак, через точку  $P$  проходит не менее  $m^2 + 1$  прямых, а именно прямая  $L$  и  $m^2$  других прямых, соединяющих точку  $P$  с точками плоскости  $\pi^*$ . Следовательно, так как через точку  $P$  проходит  $n+1$  прямая,  $n \geq m^2$ . Если  $n \neq m^2$ , должна существовать по крайней мере еще одна прямая  $L_1$ , проходящая через точку  $P$ , но не проходящая ни через одну точку подплоскости  $\pi^*$ . Рассмотрим теперь точки пересечения прямой  $L_1$  с  $m^2 + m + 1$  прямыми плоскости  $\pi^*$ . Если бы какие-нибудь две из этих точек пересечения совпали, то эта точка принадлежала бы подплоскости  $\pi^*$ , что невозможно. Следовательно, прямая  $L_1$  содержит не менее  $m^2 + m + 1$  точек. Поэтому  $n \geq m^2 + m$ .

Нетрудно перечислить все подмножества  $S$  плоскости, которые вместе с любой парой точек содержат соединяющую их прямую и которые вместе с любой парой прямых содержат их пересечение.

Во-первых, если множество  $S$  содержит четыре точки, никакие три из которых не лежат на одной прямой, то множество  $S$  является подплоскостью. Остальные такие подмножества называются *вырожденными подплоскостями*. Вот они:

- 1) пустое множество;
- 2) единственная точка  $P$  и, возможно, одна или несколько прямых, проходящих через точку  $P$ ;
- 3) единственная прямая  $L$  и, возможно, одна или несколько точек, лежащих на прямой  $L$ ;
- 4) единственная точка  $P$  и единственная прямая  $L$ , не проходящая через точку  $P$ ;
- 5) вершины и стороны треугольника;
- 6) прямая  $L$ , точка  $P$  на ней, одна или несколько точек на прямой  $L$  и одна или несколько прямых, проходящих через точку  $P$ ;
- 7) прямая  $L$ , содержащая три или более точек, отдельная точка  $P$ , не лежащая на прямой  $L$ , и прямые, соединяющие точку  $P$  с точками прямой  $L$ .

Коллинеация  $\alpha$  является подстановкой множества точек и подстановкой множества прямых плоскости  $\pi$ . Пусть  $P$  — подстановка множества точек, а  $Q$  — подстановка множества прямых. Обе эти подстановки запишем как квадратные матрицы порядка  $N$ . Здесь, как обычно,  $N = n^2 + n + 1$ . Обозначим

$$\begin{aligned} P &= (p_{ij}), \\ Q &= (q_{ij}), \end{aligned} \tag{20.9.1}$$

где  $p_{ij} = 1$ , если  $P_i\alpha = P_j$ , и  $q_{ij} = 1$ , если  $Q_i\alpha = Q_j$ , а в остальных случаях  $p_{ij} = 0$ ,  $q_{ij} = 0$ . Тогда

$$P^{-1}AQ = A, \tag{20.9.2}$$

где  $A = (a_{ij})$  — матрица инцидентности плоскости  $\pi$ . Обратно, если существуют мономиальные матрицы  $P$  и  $Q$ , состоящие из нулей и единиц, подчиненные условию (20.9.2), то они определяют коллинеацию плоскости  $\pi$ .

**Теорема 20.9.2.** (ПАРКЕР [1].) *Подстановки  $P$  множества точек и подстановки  $Q$  множества прямых для произвольной коллинеации подобны как подстановки.*

**Следствие 20.9.1.** (БЭР.) *Коллинеация оставляет на месте равное число точек и прямых.*

*Доказательство.* Так как

$$AA^T = A^TA = nI + S, \tag{20.9.3}$$

то

$$(\det A)^2 = \det(nI + S) = (n + 1)^2 n^{N-1}, \tag{20.9.4}$$

откуда видно, что матрица  $A$  невырожденная. Теперь равенство (20.9.2) принимает вид

$$Q = A^{-1}PA, \quad (20.9.5)$$

т. е. матрицы  $P$  и  $Q$  подобны. Поэтому матрицы  $P$  и  $Q$ , рассматриваемые как представления некоторой циклической группы, обладают одними и теми же неприводимыми составляющими. Однако, приводя цикл  $(x_1, \dots, x_r)$  длины  $r$  любой из этих подстановок, мы находим, что характерами этих неприводимых составляющих являются  $1, \zeta, \zeta^2, \dots, \zeta^{r-1}$ , где  $\zeta$  — первообразный корень степени  $r$  из единицы. Но это означает, что корень степени  $m$  из единицы является характером подстановки  $P$  кратности  $a_m$ , где  $a_m$  — число циклов подстановки  $P$ , длина которых кратна  $m$ . Так как эти кратности  $a_m$  одинаковы для подстановок  $P$  и  $Q$ , отсюда следует, что подстановки  $P$  и  $Q$  имеют одинаковое число циклов каждой длины  $m$ . Поэтому  $P$  и  $Q$  подобны как подстановки. В частности, отсюда получается следствие, в котором утверждается, что подстановки  $P$  и  $Q$  имеют одинаковое число циклов длины 1, т. е. имеют одинаковое число элементов, оставляемых ими на месте.

**Теорема 20.9.3.** (ПАРКЕР.) Группа коллинеаций  $G$  плоскости  $\pi$ , рассматриваемая как группа подстановок множества точек плоскости  $\pi$  и как группа подстановок множества прямых плоскости  $\pi$ , обладает одним и тем же числом областей транзитивности.

**Доказательство.** Пусть группа  $G$  имеет порядок  $g$ . Она представляется группой подстановок  $G_1$  множества точек и группой подстановок  $G_2$  множества прямых, причем, согласно равенству (20.9.5), эти представления эквивалентны. Пусть  $\chi_1, \chi_2$  — характеристики этих представлений, тогда

$$\sum_{x \in G} \chi_1(x) = \sum_{x \in G} \chi_2(x). \quad (20.9.6)$$

Но, согласно теореме 16.6.13,

$$\sum_{x \in G} \chi_1(x) = k_1 g, \quad \sum_{x \in G} \chi_2(x) = k_2 g, \quad (20.9.7)$$

где  $k_1$  — число областей транзитивности группы  $G_1$  и  $k_2$  — число областей транзитивности группы  $G_2$ . Поэтому  $k_1 = k_2$ , и теорема доказана. Хотя, как видно из предыдущей теоремы, каждая отдельно взятая подстановка группы  $G_1$  подобна соответствующей подстановке из группы  $G_2$ , в целом неверно, что группы  $G_1$  и  $G_2$  подобны как группы подстановок. Например, в дезарговой плоскости группа всех коллинеаций, отображающих точку  $P_0$  в себя, не оставляет неподвижной ни одной прямой.

**Теорема 20.9.4.** Группа коллинеаций дезарговой плоскости  $\pi$  порядка  $n = p^r$  имеет порядок

$$r(n^2 + n + 1)(n^2 + n)n^2(n - 1)^2.$$

**Доказательство.** В плоскости  $\pi$  число упорядоченных четверок точек  $P_1, P_2, P_3, P_4$  равно  $(n^2 + n + 1)(n^2 + n)n^2(n - 1)^2$ , так как в качестве точки  $P_1$  можно выбрать любую из  $n^2 + n + 1$  точек, в качестве  $P_2$  — любую из оставшихся точек, в качестве  $P_3$  — любую из  $n^2$  точек, не принадлежащих прямой  $P_1P_2$ , и в качестве  $P_4$  — любую из  $(n - 1)^2$  точек, не лежащих ни на одной из прямых  $P_1P_2, P_1P_3, P_2P_3$ . В силу теоремы 20.5.5 группа коллинеаций  $G$  плоскости  $\pi$  транзитивна на четырехугольниках. Подгруппа группы  $G$ , отображающая в себя четырехугольник  $XYOI$ , является группой автоморфизмов поля Галуа  $GF(p^r)$ , служащего системой координат плоскости  $\pi$ , а она, как отмечалось в § 20.6, имеет порядок  $r$ .

**Теорема 20.9.5.** (Зингер [1].) Дезаргова плоскость  $\pi$  порядка  $n$  обладает коллинеацией  $\alpha$  порядка  $N = n^2 + n + 1$ , циклической и на множестве точек, и на множестве прямых.

**Доказательство.** Пусть  $n = p^r$ . Тогда на плоскости  $\pi$  можно ввести координаты при помощи поля  $GF(p^r) = F$ . Плоскость  $\pi$  удобно представить в однородных координатах. Точка  $P$  задается координатами

$$P = (\lambda x_1, \lambda x_2, \lambda x_3), \quad (20.9.8)$$

где  $x_1, x_2, x_3$  — фиксированные элементы из поля  $F$ , не все равные нулю, а  $\lambda$  пробегает все ненулевые элементы из поля  $F$ . Аналогично прямая  $L$  задается координатами

$$L = [u_1\mu, u_2\mu, u_3\mu], \quad (20.9.9)$$

где  $u_1, u_2, u_3$  — фиксированные элементы из  $F$ , не все равные нулю, а  $\mu$  пробегает все ненулевые элементы поля  $F$ .  $P \in L$  тогда и только тогда, когда

$$x_1u_1 + x_2u_2 + x_3u_3 = 0. \quad (20.9.10)$$

Так как  $F$  — поле, отношение инцидентности (20.9.10) не зависит от выбора значения  $\lambda$  в (20.9.8) и значения  $\mu$  в (20.9.9). Однородные координаты отождествляются с неоднородными следующим образом:

$$\begin{aligned} (\infty) &= (0, \lambda, 0), \\ (m) &= (\lambda, \lambda m, 0), \\ (a, b) &= (\lambda a, \lambda b, \lambda), \\ L_\infty &= [0, 0, \mu], \\ (x = c) &= [\mu, 0, -c\mu], \\ (y = xm + b) &= [m\mu, -\mu, b\mu]. \end{aligned} \quad (20.9.11)$$

Без труда проверяется, что представление плоскости  $\pi$  однородными координатами согласуется с представлением неоднородными координатами. Поле  $GF(p^{3r}) = F_1$  можно рассматривать как кубическое расширение поля  $F = GF(p^r)$ , и если  $w$ —первообразный корень поля  $F_1$ , то любой элемент  $x$  поля  $F_1$  обладает единственным представлением в виде

$$x = x_1 + x_2w + x_3w^2, \quad x_i \in F. \quad (20.9.12)$$

Следовательно, если  $x \neq 0$ ,  $\lambda \in F$ ,  $\lambda \neq 0$ , то элементы  $\lambda x$  поля  $F_1$  соответствуют точкам  $(\lambda x_1, \lambda x_2, \lambda x_3)$  плоскости  $\pi$ . Но в поле  $F_1$  порядок элемента  $w$  равен  $p^{3r} - 1 = n^3 - 1$ . Элементами поля  $F$  являются решения в поле  $F_1$  уравнения

$$x^{p^r} = x, \quad (20.9.13)$$

откуда для  $x \in F$ ,  $x \neq 0$ , учитывая, что  $p^r = n$ , получаем

$$x^{n-1} = 1. \quad (20.9.14)$$

Таким образом, множество  $F^*$  (ненулевых элементов поля  $F$ ) состоит из элементов единственной подгруппы порядка  $n - 1$  циклической группы  $\{w\}$  порядка  $n^3 - 1$ . Следовательно, группа  $F^*$  состоит из элементов

$$w^{Ni}, \quad N = n^2 + n + 1. \quad (20.9.15)$$

Поэтому элементы  $w^u$  и  $w^v$  представляют одну и ту же точку плоскости  $\pi$  тогда и только тогда, когда

$$u \equiv v \pmod{N}. \quad (20.9.16)$$

Следовательно, отображение  $\alpha$

$$x \rightarrow xw, \quad (20.9.17)$$

определенное для элементов поля  $F_1$ , является циклической подстановкой степени  $N$  множества точек плоскости  $\pi$ . Если  $P_1 = (x_1, x_2, x_3)$  и  $P_2 = (y_1, y_2, y_3)$ —две различные точки, то, как нетрудно проверить, координаты точек прямой  $P_1P_2$  задаются следующим образом:

$$\begin{aligned} \lambda_1(x_1, x_2, x_3) + \lambda_2(y_1, y_2, y_3) = \\ = (\lambda_1 x_1 + \lambda_2 y_1, \lambda_1 x_2 + \lambda_2 y_2, \lambda_1 x_3 + \lambda_2 y_3), \end{aligned} \quad (20.9.18)$$

где  $\lambda_1$  и  $\lambda_2$ —произвольные элементы поля  $F$ , не равные одновременно нулю. Следовательно, если  $w^i = x_1 + x_2w + x_3w^2$ ,  $w^j = y_1 + y_2w + y_3w^2$ , то координаты точек прямой  $P_1P_2$  однозначно определяются величинами

$$\lambda_1 w^i + \lambda_2 w^j. \quad (20.9.19)$$

Тогда отображение  $x \rightarrow xw$  переводит точки (20.9.19) прямой в точки

$$\lambda_1 w^{i+1} + \lambda_2 w^{j+1}, \quad (20.9.20)$$

принадлежащие прямой, соединяющей точки  $P_1\alpha$  и  $P_2\alpha$ . Следовательно, отображение  $\alpha$  есть коллинеация плоскости  $\pi$ , действующая на множестве точек как цикл длины  $N$ . Нетрудно заметить (например, с помощью теоремы 20.9.2), что  $\alpha$  есть также цикл длины  $N$  на множестве прямых плоскости  $\pi$ .

Можно указать грубую верхнюю оценку порядка группы  $G$  коллинеаций плоскости  $\pi$  порядка  $n$ . Упорядоченная четверка точек  $P_1, P_2, P_3, P_4$  имеет не более  $M = (n^2+n+1)(n^2+n)n^2(n-1)^2$  образов. Подгруппа  $H_1$  индекса  $\leq M$ , отображающая четверку  $P_1, P_2, P_3, P_4$  в себя, отображает также на себя подплоскость  $\pi_1$ , порожденную этими точками. Если подплоскость  $\pi_1$  имеет порядок  $m_1$ , то подгруппа  $H_1$  переставляет  $n - m_1$  точек на каждой прямой плоскости  $\pi$ , не являющихся точками подплоскости  $\pi_1$ . Подгруппа  $H_2$  индекса  $\leq n - m_1$  группы  $H_1$ , оставляющая на месте одну из этих точек, отображает в себя большую подплоскость  $\pi_2$  порядка  $m_2$ , где в силу теоремы 20.9.2  $m_2 \geq m_1^2$ . Мы получаем, таким образом, убывающую цепочку подгрупп  $H_1 \supset H_2 \supset \dots \supset H_s = 1$ , в которой подгруппа  $H_i$  отображает на себя подплоскость порядка  $m_i$ , причем  $m_{i+1} \geq m_i^2$  и  $[H_i : H_{i+1}] < n$ . Отсюда  $s \leq \log_2 n$ , и порядок группы  $G$  не больше  $n^s M$ . Порядки групп коллинеаций известных недезарговых плоскостей не пре- восходят порядков групп коллинеаций дезарговых плоскостей того же порядка, и кажется, что это имеет место всегда.

Две следующие теоремы показывают, что если в некотором смысле группа коллинеаций конечной плоскости достаточно велика, то эта плоскость дезаргова.

**Теорема 20.9.6.** (Глисон [1].) *Если для любой пары  $P, L$  точки  $P$  и содержащей ее прямой  $L$  конечной плоскости  $\pi$  группа элаций  $G(P, L)$  нетривиальна, то плоскость  $\pi$  дезаргова.*

**Доказательство.** Согласно теореме 20.4.3, если две группы элаций  $G(P_1, L)$  и  $G(P_2, L)$ , где  $P_1$  и  $P_2$  — различные точки прямой  $L$ , нетривиальны, т. е. не являются единичными группами, то все элации с осью  $L$  образуют абелеву группу, в которой все элементы, отличные от 1, имеют один и тот же простой порядок  $p$ . В силу принципа двойственности, если группы  $G(P, L_1)$  и  $G(P, L_2)$  нетривиальны, где  $L_1$  и  $L_2$  — различные прямые, пересекающиеся в точке  $P$ , то все элации с центром  $P$  образуют абелеву группу, состоящую из элементов простого порядка  $p$ . Следовательно, при условиях настоящей теоремы любая группа элаций  $G(P, L)$  является элементарной абелевой группой, порядок которой равен простому числу  $p$  или его степени.

**Лемма 20.9.1.** Пусть  $H$  — группа подстановок некоторого конечного множества  $S$ , причем такая, что для некоторого простого числа  $p$  и каждого элемента  $x \in S$  существует элемент порядка  $p$  из группы  $H$ , оставляющий на месте только этот элемент  $x$  множества  $S$ . Тогда группа  $H$  транзитивна.

**Доказательство.** Рассмотрим область транзитивности  $S_1$  множества  $S$  относительно группы  $H$ . Для  $x \in S_1$  существует элемент группы  $H$  порядка  $p$ , оставляющий неподвижным  $x$  и разбивающий все остальные символы на циклы длины  $p$ . Следовательно, число элементов в области  $S_1$  сравнимо с 1 по модулю  $p$ , а число элементов в другой области транзитивности  $S_2$  (если она существует) кратно  $p$ . Но тогда, выбрав некоторый элемент  $y \in S_2$ , аналогичными рассуждениями получаем, что число элементов области транзитивности  $S_1$  кратно  $p$ . Полученное противоречие показывает, что множество  $S$  содержит одну область транзитивности, т. е. что группа  $H$  транзитивна.

**Лемма 20.9.2.** Пусть для прямой  $L$  конечной плоскости  $\pi$  и для всех точек  $P_i$  прямой  $L$  группы элаций  $G(P_i, L)$  имеют один и тот же порядок  $h > 1$ . Тогда  $\pi$  — плоскость трансляций относительно прямой  $L$ .

**Доказательство.** Пусть плоскость  $\pi$  имеет порядок  $n$ . Пересечение любых двух из  $n+1$  групп  $G(P_i, L)$ , каждая из которых имеет порядок  $h$ , состоит из единичной подгруппы, а объединение этих  $n+1$  групп образует группу трансляций  $T(L)$ . Следовательно, порядок группы  $T(L)$  равен  $t = (n+1)(h-1)+1$ . Так как только единица группы  $T(L)$  может оставлять неподвижной точку, не принадлежащую прямой  $L$ , группа  $T(L)$  переставляет  $n^2$  точек таким образом, что каждая область транзитивности состоит из  $t$  точек, откуда  $t$  делит  $n^2$ , т. е.

$$n^2 = tm = [(n+1)(h-1)+1]m. \quad (20.9.21)$$

Но  $h > 1$ , поэтому  $m < n$ . С другой стороны, рассматривая равенство (20.9.21) по модулю  $n+1$ , имеем

$$n^2 \equiv 1 \equiv m \pmod{n+1}. \quad (20.9.22)$$

Но из соотношений  $m \equiv 1 \pmod{n+1}$  и  $m < n$  следует, что  $m = 1$ ,  $t = n^2$ , т. е. группа  $T(L)$  транзитивна на  $n^2$  точках плоскости  $\pi$ , не принадлежащих прямой  $L$ , и поэтому  $\pi$  — плоскость трансляций относительно прямой  $L$ .

Теперь мы в состоянии доказать нашу теорему. Зафиксируем прямую  $L$  плоскости  $\pi$ . Для каждой точки  $P \in L$  группа элаций  $G(P, M)$ , где  $M \neq L$  — другая прямая, проходящая через точку  $P$ , содержит элемент порядка  $p$ , оставляющий на месте точку  $P$  и отображающий прямую  $L$  на себя, причем так, что  $P$  —

единственная точка прямой  $L$ , остающаяся неподвижной. Следовательно, в силу леммы 20.9.1 группа  $G(L)$  всех коллинеаций, оставляющих прямую  $L$  инвариантной, транзитивна на множестве точек прямой  $L$ . Отсюда теперь следует, что для  $n+1$  точек  $P_i$  прямой  $L$  все группы элаций  $G(P_i, L)$ , являясь сопряженными относительно группы  $G(L)$ , имеют один и тот же порядок  $h$ . Согласно лемме 20.9.2, отсюда следует, что  $\pi$  — плоскость трансляций относительно прямой  $L$ . Но  $L$  — произвольная прямая плоскости  $\pi$ . Значит,  $\pi$  — плоскость трансляций относительно любой прямой  $L$ . Поэтому, согласно теореме 20.5.3, системой координат плоскости  $\pi$  может служить альтернативное тело. По теореме 20.6.2 конечное альтернативное тело является полем. Поэтому плоскость  $\pi$  дезаргова.

Глисон [1] использовал эту теорему для изучения конечных плоскостей Фано (Fano). Конфигурация Фано состоит из семи точек и семи прямых, образующих конечную плоскость порядка 2. Под плоскостью Фано понимается плоскость, в которой диагональные точки любого четырехугольника лежат на одной прямой, или, что то же самое, плоскость, в которой любой четырехсторонник порождает конфигурацию Фано. Глисон показал, что любая конечная плоскость Фано дезаргова и является конечной плоскостью над полем  $GF(p^2)$ . Из-за недостатка места мы не можем доказать здесь этот очень интересный результат.

Будем называть коллинеацию порядка 2 *инволюцией*.

**Теорема 20.9.7.** (Бэр.) Пусть  $\alpha$  — инволюция проективной плоскости порядка  $n$ . Тогда или (1)  $n = m^2$  и точки и прямые, инвариантные относительно  $\alpha$ , образуют подплоскость порядка  $m$ , или (2)  $\alpha$  — центральная коллинеация. В случае (2), если  $n$  нечетно, то  $\alpha$  — гомология, а если  $n$  четно, то  $\alpha$  — элация.

**Доказательство.** Покажем сначала, что каждая точка лежит на некоторой прямой, инвариантной относительно  $\alpha$ . Если точка  $P$  не остается на месте под действием  $\alpha$ , то  $P\alpha \neq P$  и коллинеация  $\alpha$  оставляет неподвижной прямую  $PP\alpha$ , являющуюся поэтому искомой. Если же  $P$  — неподвижная точка, соединяем ее с другой точкой  $Q$ . Может случиться, что прямая  $L = PQ$  неподвижна. Если нет, предположим, что  $Q\alpha \neq Q$ ,  $Q\alpha \notin PQ$ , и пусть  $L\alpha = PQ\alpha$ . Если затем  $R$  — третья точка на прямой  $L$ , то  $R\alpha \in L\alpha$ . Тогда инволюция  $\alpha$  отображает прямые  $Q\alpha R$  и  $QR\alpha$  друг в друга. Значит, точка их пересечения  $S$  — вторая неподвижная точка, отличная от  $P$ . В этом случае  $PS$  — искомая неподвижная прямая, проходящая через точку  $P$ . В силу принципа двойственности любая прямая проходит через инвариантную относительно  $\alpha$  точку.

Прямая, соединяющая две инвариантные точки, также инвариантна относительно  $\alpha$ , а пересечение двух инвариантных прямых — инвариантная точка. Поэтому если существует четверка

инвариантных точек, никакие три из которых не лежат на одной прямой, то инвариантные относительно  $\alpha$  элементы плоскости  $\pi$  образуют собственную подплоскость  $\pi_1$ . Предположим, что мы имеем этот случай и что порядок подплоскости  $\pi_1$  равен  $m$ . Тогда, по теореме 20.9.1,  $n \geq m^2$ , однако из доказательства этой теоремы видно, что в случае  $n > m^2$  существует прямая плоскости  $\pi$ , не проходящая ни через одну точку подплоскости  $\pi_1$ . Но, как мы показали, любая прямая плоскости  $\pi$  содержит инвариантную относительно  $\alpha$  точку. Следовательно,  $n$  не больше  $m^2$ , откуда  $n = m^2$ . Этим завершается рассмотрение случая (1) нашей теоремы.

Предположим теперь, что не существует четверки инвариантных точек, никакие три из которых не лежат на одной прямой. Что представляет из себя тогда конфигурация точек, инвариантных относительно  $\alpha$ ? Покажем сначала, что существует прямая, содержащая три такие точки. Пусть прямая  $L_1$  содержит инвариантную точку  $P_1$ . Выберем прямую  $L_2$ , не проходящую через точку  $P_1$ . Прямая  $L_2$  содержит инвариантную точку  $P_2 \neq P_1$ . Мы имеем теперь две инвариантные точки  $P_1, P_2$  и соединяющую их инвариантную прямую  $L$ . Выберем на прямой  $L$  третью точку  $Q$ . Если  $Q$  — инвариантная точка, то  $L$  — искомая прямая. Если же  $Q$  — неинвариантная точка, то некоторая прямая  $L_3$ , проходящая через точку  $Q$ , содержит некоторую точку  $P_3$ , не принадлежащую прямой  $L$ . Мы имеем теперь треугольник с инвариантными вершинами  $P_1, P_2, P_3$ . Рассмотрим прямую  $L_4$ , не проходящую ни через одну из точек  $P_1, P_2, P_3$ . Прямая  $L_4$  содержит некоторую инвариантную точку  $P_4$ . Если точка  $P_4$  не лежит ни на одной из прямых  $P_1P_2, P_1P_3, P_2P_3$ , то  $P_1, P_2, P_3, P_4$  — четверка инвариантных точек, никакие три из которых не лежат на одной прямой, но эта ситуация относится к уже рассмотренному случаю (1). Следовательно, точка  $P_4$  лежит на одной из этих трех прямых, являющейся искомой прямой, содержащей три инвариантные точки.

Теперь в нашем распоряжении прямая  $L$ , содержащая три инвариантные точки  $P_1, P_2, P_3$ . Если бы имелось более одной неподвижной точки, не принадлежащей прямой  $L$ , то существовала бы четверка инвариантных точек, никакие три из которых не лежат на одной прямой, но эту возможность мы включили в случай (1). Поэтому вне прямой  $L$  или есть только одна неподвижная точка  $P$ , или нет ни одной. Рассмотрим теперь произвольную точку  $P_i \in L$ . Через точку  $P_i$  проходит некоторая прямая  $K$ , отличная от  $L$ , а если существует инвариантная точка  $P \notin L$ , то прямая  $K$  отлична от прямой  $PP_i$ . Прямая  $K$  содержит одну инвариантную точку, но по построению не содержит инвариантных точек, лежащих вне прямой  $L$ . Следовательно, неподвижной точкой прямой  $K$  является точка  $P_i$ , откуда следует, что любая точка  $P_i$  прямой  $L$  инвариантна. Так как инволюция  $\alpha$  оставляет на месте каждую точку

прямой  $L$ , то  $\alpha$  — центральная коллинеация с осью  $L$ , что и требовалось для доказательства утверждения (2). Вне прямой  $L$  лежат  $n^2$  точек плоскости  $\pi$ , а порядок коллинеации  $\alpha$  равен 2. Следовательно, если  $n$  нечетно, инволюция  $\alpha$  оставляет на месте некоторую точку вне прямой  $L$ , т. е. является гомологией. Если же  $n$  четно,  $\alpha$  оставляет на месте четное число точек, не лежащих на прямой  $L$ , и поэтому оставляет на месте не менее двух таких точек, если оставляет хоть одну. Следовательно, в этом случае инволюция  $\alpha$  не оставляет неподвижной ни одной точки вне прямой  $L$  и является поэтому элацией. Этим доказательство теоремы закончено.

Следующая теорема является небольшим уточнением теоремы Острома [1], дополнительно предполагавшего, что  $n$  нечетно.

**Теорема 20.9.8. (Остром.)** *Если группа коллинеаций конечной проективной плоскости  $\pi$ , порядок которой  $n$  не является квадратом, дважды транзитивна на множестве точек плоскости  $\pi$ , то плоскость  $\pi$  дезаргова.*

*Доказательство.* Пусть  $G$  — группа коллинеаций плоскости  $\pi$ . По условию группа  $G$  дважды транзитивна на множестве  $N = n^2 + n + 1$  точек плоскости  $\pi$ . Так как число  $N(N - 1)$  делит порядок группы  $G$ , эта группа содержит элемент порядка 2, т. е. инволюцию  $\alpha$ . Так как  $n$  не является квадратом некоторого числа, то в силу теоремы 20.9.7 отсюда следует, что  $\alpha$  — элация, если  $n$  четно, и что  $\alpha$  — гомология, если  $n$  нечетно.

**Лемма 20.9.3.** *Группа  $G$  содержит элацию.*

*Доказательство.* Если  $n$  четно, инволюция  $\alpha$  является элацией. Поэтому достаточно рассмотреть лишь случай, когда  $n$  нечетно. Рассмотрим инволюцию  $\alpha$ , являющуюся гомологией. Пусть точка  $P$  — ее центр, прямая  $L$  — ее ось. Пусть  $A$  — точка на прямой  $L$ ,  $A_1 \neq P$  — точка вне прямой  $L$ . Тогда в группе  $G$  существует элемент  $\sigma$ , отображающий  $P$  в  $P$ ,  $A$  в  $A_1$ . В таком случае  $\beta = \sigma^{-1}\alpha\sigma$  — инволюция с центром  $P$  и с осью  $K$ , проходящей через точку  $A_1$  и поэтому отличной от  $L$ . Поэтому  $\alpha\beta$  — центральная коллинеация, так как она оставляет неподвижными все прямые, проходящие через точку  $P$ . Если коллинеация  $\rho = \alpha\beta$  оставляет на месте некоторую прямую  $T$ , не содержащую точку  $P$ , положим  $T_1 = T\alpha$ . Тогда элемент  $\beta$  должен также отображать друг в друга прямые  $T$  и  $T_1$ , а если  $T \neq T_1$ , отображение  $\rho$  должно оставлять на месте прямые  $T$  и  $T_1$ , откуда, согласно теореме 20.4.1,  $\rho = 1$  и  $\alpha = \beta$ , что невозможно, так как  $\alpha$  и  $\beta$  — инволюции с разными осями. Но если  $T = T_1$ , то  $T$  — ось инволюции  $\alpha$ , а также инволюции  $\beta$ , что опять-таки невозможно, так как инволюции  $\alpha$  и  $\beta$  имеют разные оси. Итак, коллинеация  $\rho$  не оставляет на месте ни одной прямой, не проходящей через точку  $P$ , и является, следовательно, элацией. Этим лемма доказана.

Мы можем теперь рассмотреть элацию  $\rho$  с центром  $P$  и осью  $L$ . Пусть  $P_i$  — произвольная другая точка прямой  $L$ . Тогда в группе  $G$  существует элемент  $\sigma$ , отображающий друг в друга точки  $P$  и  $P_i$ , следовательно, отображающий прямую  $L$  на себя. Поэтому группа  $G(L)$  коллинеаций, оставляющих на месте прямую  $L$  транзитивна на множестве точек прямой  $L$ , и поэтому для всех точек  $P_i$  прямой  $L$  группы элаций  $G(P_i, L)$  имеют один и тот же порядок  $h$ , причем  $h \geq 1$ , так как  $\rho$  — элация, обладающая центром  $P$  и осью  $L$ . В силу леммы 20.9.2 к теореме 20.9.6,  $\pi$  — плоскость трансляций относительно оси  $L$ . Но так как группа  $G$  дважды транзитивна на множестве точек, то любые две точки прямой  $L$  могут быть отражены подходящим элементом из  $G$  в две точки любой другой прямой  $K$ . Следовательно,  $\pi$  — также плоскость трансляций относительно прямой  $K$  и потому — муфандова плоскость. Но, как было показано при доказательстве теоремы 20.9.6, это означает, что плоскость  $\pi$  дезаргова. В еще неопубликованной работе А. Вагнера (A. Wagner) показывается, что теорема 20.9.8 справедлива без всяких ограничений на  $n$ .

Хьюгес [3] обобщил понятие матрицы инцидентности плоскости. Если даны плоскость  $\pi$  и группа  $G$  коллинеаций этой плоскости, то элементами этой матрицы являются элементы группового кольца  $G^*$  группы  $G$ , причем групповое кольцо  $G^*$  берется над кольцом целых чисел или над полем, характеристика которого не делит порядок группы  $G$ . Для такой матрицы могут быть получены аналоги уравнений инцидентности (20.9.3). Напомним, что, согласно теореме 20.9.3, число областей транзитивности на множестве прямых относительно всех элементов группы  $G$  равно числу областей транзитивности на множестве точек. Обозначим это число через  $w$  и выпишем употребляемые нами обозначения:

$\pi$  — данная проективная плоскость порядка  $n$ ,  
 $G$  — группа коллинеаций плоскости  $\pi$ , порядок которой равен  $g$ ,

$P_i$ ,  $i = 1, \dots, w$ , — фиксированный представитель  $i$ -й области транзитивности множества точек,

$L_j$ ,  $j = 1, \dots, w$ , — фиксированный представитель  $j$ -й области транзитивности множества прямых,

$H_i$  — подгруппа группы  $G$ , оставляющая неподвижной точку  $P_i$  и имеющая порядок  $h_i$ ,

$T_j$  — подгруппа группы  $G$ , оставляющая неподвижной прямую  $L_j$  и имеющая порядок  $t_j$ ,

$D_{ij} = \{x \mid x \in G, P_i x \in L_j\}$  — множество элементов  $d_{ij}$  группы  $G$ ,

$$\begin{aligned}\delta_{ij} &= \sum x, \quad x \in D_{ij}, \\ \delta_{ij}^* &= \sum x^{-1}, \quad x \in D_{ij}, \\ D &= (\delta_{ij}), \quad i, j = 1, \dots, w, \text{ — матрица над } G^*, \\ D' &= (\delta_{ij}^*)^T, \quad i, j = 1, \dots, w, \text{ — матрица над } G^*, \\ \rho_i &= \sum x, \quad x \in H_i, \quad i = 1, \dots, w, \\ \tau_j &= \sum x, \quad x \in T_j, \quad j = 1, \dots, w, \\ \gamma &= \sum x, \quad x \in G, \\ S &— \text{матрица порядка } w, \text{ каждый элемент которой равен } \gamma.\end{aligned}\tag{20.9.23}$$

Нам понадобятся также следующие диагональные матрицы:

$$\begin{aligned}C_1 &= \text{диаг.}(h_1^{-1}, h_2^{-1}, \dots, h_w^{-1}), \\ C_2 &= \text{диаг.}(t_1^{-1}, t_2^{-1}, \dots, t_w^{-1}), \\ P &= \text{диаг.}(\rho_1, \rho_2, \dots, \rho_w), \\ L &= \text{диаг.}(\tau_1, \tau_2, \dots, \tau_w).\end{aligned}\tag{20.9.24}$$

Заметим, что знание множеств  $D_{ij}$  таких элементов  $x$  группы  $G$ , что  $P_i x \in L_j$ , полностью определяет отношения инцидентности плоскости  $\pi$ , так как любая точка плоскости  $\pi$  может быть записана как образ  $P_i u$  некоторой точки  $P_i$ ,  $i = 1, \dots, w$ , при отображении  $u \in G$  и аналогично любая прямая представима как образ  $L_j v$ . При этом  $P_i u \in L_j v$  тогда и только тогда, когда  $P_i u v^{-1} \in L_j$  или  $u v^{-1} \in D_{ij}$ . Следовательно, задание матрицы  $D$  полностью определяет плоскость  $\pi$ . Если  $G$  — единичная группа, то  $D$  — матрица инцидентности  $A$  плоскости  $\pi$ .

**Теорема 20.9.9.** *Если  $\pi$  — плоскость порядка  $n$  и  $G$  — группа коллинеаций плоскости  $\pi$  порядка  $g$ , то матрица коллинеации  $D$  обладает следующими свойствами:*

$$\begin{aligned}DC_2 D' &= nP + S, \\ D'C_1 D &= nL + S, \\ DC_2 S &= (n+1)S, \\ SC_1 D &= (n+1)S.\end{aligned}\tag{20.9.25}$$

**Доказательство.** Первое равенство мы докажем, вычисляя элементы матрицы  $U = DC_2 D'$ , причем вычислим сначала элементы главной диагонали, а затем — остальные. Если  $U = (u_{r,s})$ ,  $r, s = 1, \dots, w$ , то имеем

$$u_{rr} = \sum_{j=1}^w \frac{\delta_{rj} \delta_{rj}^*}{t_j}.\tag{20.9.26}$$

В сумме (20.9.26)  $j$ -е слагаемое равно

$$\sum \frac{xy^{-1}}{t_j}, x \in D_{rj}, y \in D_{rj}. \quad (20.9.27)$$

Заметим, что для  $x \in D_{rj}$  полный двойной смежный класс  $H_r x T_j$  содержится в  $D_{rj}$ . Рассмотрим левые смежные классы по подгруппе  $H_r$  группы  $G$ :

$$G = H_r + H_r x_2 + \dots + H_r x_{v_r}, v_r h_r = g. \quad (20.9.28)$$

Для произвольного элемента  $h \in H_r$  справедливо, в силу включения  $H_r y \subseteq D_{rj}$ , соотношение  $xy^{-1} = h$ , или  $x = hy$ , где элемент  $y \in D_{rj}$  произвольный, а  $x \in D_{rj}$  — подходящим образом выбранный элемент. Следовательно, для данного элемента  $h \in H_r$  существуют  $d_{rj}$  таких возможных пар  $x, y \in D_{rj}$ , что  $xy^{-1} = h$ . Поэтому в сумме (20.9.26) коэффициент при  $h$  равен  $\sum_j d_{rj}/t_j$ . Но  $d_{rj}$  — число таких элементов  $x$ , что  $P_r x \in L_j$ , или  $P_r \in L_j x^{-1}$ . Для  $x \in D_{rj}$  число различных прямых в множестве  $L_j x^{-1}$  равно  $d_{rj}/t_j$ . Но точка  $P_r$  принадлежит ровно  $n+1$  прямым, следовательно,

$$\sum_j \frac{d_{rj}}{t_j} = n+1. \quad (20.9.29)$$

Поэтому в сумме (20.9.26) коэффициент при  $h \in H_r$  равен  $n+1$ .

Рассмотрим теперь уравнение  $xy^{-1} = z$ ,  $z \in H_r$ . Далее  $P_r, P_r z$  — различные точки, лежащие, следовательно, на вполне определенной прямой  $L_m v$ , где индекс  $m$  и смежный класс  $T_m v$  однозначно определены. Если для некоторого  $j$   $x \in D_{rj}$  и  $y \in D_{rj}$ , то точки  $P_r y$  и  $P_r zy = P_r x$  лежат на прямой  $L_m vy$ . Но  $P_r y \in L_j$ ,  $P_r x \in L_j$  и  $P_r x \neq P_r y$ . Следовательно,  $L_m vy = L_j$ , откуда  $j = m$ ,  $vy \in T_m$ . Поэтому в сумме (20.9.26) элемент  $z$  возникает только в слагаемом с  $j = m$ , при этом если  $x, y \in D_{rm}$ , то  $xy^{-1} = z$  для любого элемента  $y \in D_{rm}$ , так что  $L_m y^{-1} = L_m v = P_r P_r z$  и элемент  $x \in D_{rm}$  определяется равенством  $x = zy$ . Но элементы  $y$  таковы, что  $y^{-1}$  принадлежит смежному классу  $T_m v$  и принимает ровно  $t_m$  значений. Следовательно, в сумме (20.9.26) коэффициент при  $z$  равен  $t_m/t_m = 1$ . Таким образом, в сумме (20.9.26) коэффициент при  $h \in H_r$  равен  $n+1$ , а при  $z \in H_r$  равен 1. Этим мы установили равенство элементов на главной диагонали у матриц  $DC_2 D'$  и  $nP + S$ . Для недиагональных элементов матрицы  $U = DC_2 D'$  мы имеем

$$u_{rs} = \sum_{j=1}^w \frac{\delta_{rj} \delta_{sj}^*}{t_j}, \quad (20.9.30)$$

причем  $j$ -е слагаемое имеет вид

$$\sum \frac{xy^{-1}}{t_j}, \quad x \in D_{rj}, \quad y \in D_{sj}. \quad (20.9.31)$$

Теперь для произвольного элемента  $z \in G$  точки  $P_r z$  и  $P_s$  различны и полностью определяют соединяющую их прямую  $L_m v$ , где индекс  $m$  и смежный класс  $T_m v$  определены однозначно. Если  $xy^{-1} = z$ , где для некоторого  $j$   $x \in D_{rj}$ ,  $y \in D_{sj}$ , то точки  $P_r x = P_r z y$  и  $P_s y$  лежат на прямой  $L_m v y$ . Но точки  $P_r x \neq P_s y$  лежат на прямой  $L_j$ . Следовательно,  $L_j = L_m v y$ , откуда  $j = m$  и  $L_j y^{-1} = L_m v = P_r P_s z$ . Но эти элементы у таковы, что  $y^{-1}$  принадлежит смежному классу  $T_m v$  и принимает ровно  $t_m$  значений. При этом для любого элемента  $y^{-1} \in T_m v$  имеем  $L_m v y = L_m$  и  $P_r z y \in L_m$ , откуда  $x = z y \in D_{rm}$ . Следовательно, в сумме  $u_{rs}$  коэффициент при любом  $z$  равен  $t_m/t_m = 1$ , и поэтому  $u_{rs} = \sum z, z \in G$ , т. е.  $u_{rs} = \gamma$ , что и требовалось для доказательства первого из соотношений (20.9.25).

Второе из соотношений (20.9.25) двойственno первому, и его доказательство можно провести аналогичным образом.

Вычисляя элементы матрицы  $DC_2S = V = (v_{rs})$ , находим

$$v_{rs} = \sum_j \frac{\delta_{rj}}{t_j} \gamma = \sum_j \frac{d_{rj}}{t_j} \gamma, \quad (20.9.32)$$

но, согласно равенству (20.9.29), это равно  $(n+1)\gamma$ . Этим проверено третье соотношение, четвертое же двойственno третьему и доказывается аналогично.

Исходя из соотношений (20.9.25), Хьюгес получил ограничения для возможных коллинеаций плоскости, аналогичные ограничениям теоремы Брука — Райзера. Доказательство их основано (как и оригинальное доказательство Брука — Райзера) на глубоких результатах Хассе — Минковского о рациональной эквивалентности квадратичных форм. В частности, он получил следующий результат.

**Теорема 20.9.10.** (Хьюгес.) Пусть  $\pi$  — плоскость порядка  $n$ , для которого выполнены условия Брука — Райзера,  $G$  — некоторая группа коллинеаций плоскости  $\pi$  нечетного простого порядка  $p$ , и пусть число  $n$  точек, инвариантных относительно  $G$ , четно. Тогда для существования такой коллинеации необходимо, чтобы уравнение

$$x^2 = ny^2 + (-1)^{(p-1)/2} pz^2$$

имело целочисленное ненулевое решение  $x, y, z$ .

Такой же результат справедлив для группы коллинеаций  $G$  нечетного порядка  $g$  (не обязательно простого), если все элементы группы  $G$ , кроме 1, представляют те же самые точки.

Теорема Хьюгеса, подобно теореме Брука — Райзера, отрицает существование определенных коллинеаций, но она, разумеется, не гарантирует существование коллинеаций, удовлетворяющих этим условиям.

Основное содержание следующей теоремы состоит в том, что если плоскость  $\pi$  обладает некоторой группой  $G$  коллинеаций, то эта плоскость должна обладать еще другими коллинеациями определенного типа. При этом предположим, что группа  $G$  имеет простое строение. Точнее, мы будем предполагать, что группа  $G$  транзитивна и регулярна на множестве всех  $N = n^2 + n + 1$  точек плоскости  $\pi$  и что группа  $G$  абелева. Этот результат был впервые получен Холлом [3] для группы  $G$  порядка  $N$ , переставляющей циклически  $N$  точек плоскости  $\pi$ . Брук [1] обобщил его на случай транзитивной и регулярной группы  $G$ , но должен был предположить вдобавок, что группа  $G$  абелева, для того чтобы получить тот же результат. Гофман [1] получил аналогичный результат, предположив, что группа  $G$  переставляет циклически  $n^2 - 1$  точек плоскости  $\pi$ , не принадлежащих прямой  $L_\infty$  и отличных от начала координат.

Предположим, что мы имеем абелеву группу  $G$  коллинеаций плоскости  $\pi$  порядка  $n$ , являющуюся транзитивной и регулярной на  $N$  точках плоскости  $\pi$ . Тогда, если  $P$  — инвариантная точка плоскости  $\pi$ , любая точка имеет единственное представление вида  $Px$ ,  $x \in G$ . Если целое число  $t$  взаимно просто с  $N$ , то отображение  $x \rightarrow x^t$  для всех  $x \in G$ , очевидно, является автоморфизмом группы  $G$ . Если, далее, для любого элемента  $x \in G$  отображение  $Px \rightarrow Px^t$  — коллинеация плоскости  $\pi$ , то число  $t$  назовем множителем плоскости  $\pi$ . Очевидно, что множители образуют мультиликативную группу по модулю  $N$ .

**Теорема 20.9.11.** *Если плоскость  $\pi$  порядка  $n$  обладает абелевой группой коллинеаций  $G$ , являющейся транзитивной и регулярной на множестве всех  $N$  точек плоскости  $\pi$ , то любое простое число  $p$ , делящее  $n$ , является множителем плоскости  $\pi$ .*

**Доказательство.** При наших предположениях множество точек, как и множество прямых, состоит из одной-единственной области транзитивности относительно коллинеаций группы  $G$ . Поэтому можно выбрать в множестве точек один представитель  $P = P_1$ , а в множестве прямых один представитель  $L = L_1$ , и если  $D_{11} = \{x_1, x_2, \dots, x_{n+1}\}$ ,  $x_i \in G$ , то  $Px_i$  ( $i = 1, \dots, n+1$ ) — точки прямой  $L_1$ . Тогда  $x_1u, \dots, x_{n+1}u$ ,  $u \in G$ , — элементы группы  $G$ . При этом  $D' = \delta_{11}$ ,  $D = \delta_{11}^*$ :

$$\begin{aligned} D &= x_1 + \dots + x_{n+1}, \\ D' &= x_1^{-1} + \dots + x_{n+1}^{-1}. \end{aligned} \tag{20.9.33}$$

Матрицы  $C_1$  и  $C_2$  в этом случае равны единичной. Первые два из соотношений (20.9.25) принимают вид

$$DD' = D'D = n \cdot 1 + \gamma. \quad (20.9.34)$$

Последние два из соотношений (20.9.25) указывают только на то, что суммы  $D$  и  $D'$  состоят из  $n+1$  слагаемых. Чтобы доказать, что отображение  $Px \rightarrow Px^p$  — коллинеация плоскости  $\pi$ , достаточно убедиться в том, что точки  $Px_1^p, Px_2^p, \dots, Px_{n+1}^p$  лежат на одной прямой. Для этого мы должны показать, что для некоторого элемента  $u \in G$

$$D^{(p)} = x_1^p + \dots + x_{n+1}^p = (x_1 + \dots + x_{n+1})u, \quad (20.9.35)$$

так как произвольная прямая  $Lu$  состоит из точек  $Px_1u, Px_2u, \dots, Px_{n+1}u$ . Обратно, если справедливо равенство (20.9.35), то  $Px_1^p, \dots, Px_{n+1}^p$  — точки прямой  $Lu$ , откуда вообще следует, что  $P(x_1v)^p, \dots, P(x_{n+1}v)^p$  — точки прямой  $Luv^p$ , и поэтому отображение  $Px \rightarrow Px^p$  — коллинеация, а простое число  $p$  — множитель плоскости  $\pi$ . Для доказательства этой теоремы мы будем рассматривать групповое кольцо  $G^*$  группы  $G$  над кольцом целых чисел. Тогда  $G^*$  по модулю  $p$  — это групповое кольцо  $G^*$  с коэффициентами по модулю  $p$ . Имеем

$$D^{(p)} = x_1^p + \dots + x_{n+1}^p \equiv (x_1 + \dots + x_{n+1})^p = D^p \pmod{p}, \quad (20.9.36)$$

так как мультиномиальные коэффициенты делятся на  $p$  и так как группа  $G$  абелева. Предположение абелевости группы  $G$  используется здесь, а также в соотношении  $(x_i v)^p = x_i^p v^p$ , и утверждении, что отображение  $x \rightarrow x^p$  является автоморфизмом группы  $G$ . Заметим, что так как  $p|n$  и  $N = n^2 + n + 1$ , справедливо равенство  $(p, N) = 1$ . Так как  $p|n$ , из равенства (20.9.34) получаем

$$DD' \equiv \gamma \pmod{p}. \quad (20.9.37)$$

Отсюда, умножая на  $D^{p-1}$ , получаем, что

$$D^{(p)} D' \equiv D^{p-1} \gamma \equiv (n+1)^{p-1} \gamma \equiv \gamma \pmod{p}. \quad (20.9.38)$$

Следовательно, из равенства (20.9.36) получается сравнение

$$D^{(p)} D' \equiv \gamma \pmod{p}. \quad (20.9.39)$$

Отсюда

$$D^{(p)} D' = \gamma + pR, \quad (20.9.40)$$

где (и это существенно для нашего доказательства) коэффициенты в выражении  $R$  при элементах группы — неотрицательные целые числа, так как в произведении  $D^{(p)} D'$  все коэффициенты неотрицательны и в силу сравнения (20.9.38) каждый член  $a_i u_i$ ,  $u_i \in G$ ,

обладает коэффициентом  $a_i \equiv 1 \pmod{p}$ ,  $a_i \geq 0$ . Итак,  $a_i \geq 1$  и  $(a_i - 1)p$  — неотрицательный целый коэффициент при элементе  $u_i$  в выражении  $R$ . Далее, отображение  $x \rightarrow x^{-1}$ ,  $x \in G$ , является автоморфизмом группы  $G$ , определяющим, следовательно, автоморфизм  $h \rightarrow h'$ ,  $h \in G^*$ , группового кольца  $G^*$ ; при этом автоморфизме  $D \rightarrow D'$ . Применив этот автоморфизм к (20.9.40), получаем

$$DD'^{(p)} = \gamma + pR'. \quad (20.9.41)$$

Кроме этого, отображение  $x \rightarrow x^p$  является автоморфизмом группы  $G$ , определяющим автоморфизм  $h \rightarrow h^{(p)}$  группового кольца  $G^*$ . Применяя этот автоморфизм к равенству (20.9.34), получаем

$$D^{(p)}D'^{(p)} = n \cdot 1 + \gamma. \quad (20.9.42)$$

Произведение левых частей равенств (20.9.34) и (20.9.42) равно произведению левых частей равенств (20.9.40) и (20.9.41). Поэтому равны соответствующие произведения правых частей:

$$(n \cdot 1 + \gamma)^2 = (\gamma + pR)(\gamma + pR'). \quad (20.9.43)$$

Применив к равенству (20.9.40) гомоморфизм группового кольца  $G^*$  в кольцо целых чисел, определяемый отображениями  $x \rightarrow 1$ ,  $x \in G$ , получаем

$$(n + 1)^2 = n^2 + n + 1 + pR(1), \quad (20.9.44)$$

где  $R(1)$  — образ элемента  $R$  при этом гомоморфизме. Отсюда  $pR(1) = n$ , а также  $pR'(1) = n$ . Но в групповом кольце  $G^*$  имеет место равенство  $pR\gamma = pR(1)\gamma = n\gamma$ . Используя его для упрощения равенства (20.9.43), находим

$$n^2 \cdot 1 = (pR)(pR'). \quad (20.9.45)$$

Но так как суммы  $pR$  и  $pR'$  имеют неотрицательные коэффициенты, последнее равенство невозможно, если в сумме  $pR$  найдется более одного ненулевого члена. Следовательно,  $pR = bu$  для некоторого целого числа  $b$  и элемента  $u \in G$ . Но  $b = pR(1) = n$ , откуда  $pR = nu$ . Подставляя это в (20.9.40), имеем

$$D^{(p)}D' = \gamma + nu. \quad (20.9.46)$$

Умножая на  $D$  и применяя соотношение (20.9.34), находим

$$\begin{aligned} D^{(p)}D'D &= \gamma D + nDu, \\ D^{(p)}(n + \gamma) &= (n + 1)\gamma + nDu, \\ nD^{(p)} + (n + 1)\gamma &= (n + 1)\gamma + nDu. \end{aligned} \quad (20.9.47)$$

Отсюда

$$D^{(P)} = Du, \quad (20.9.48)$$

а это и есть соотношение (20.9.35), которое мы искали. Этим теорема доказана.

Чтобы показать силу этой теоремы, рассмотрим плоскость порядка 8 с группой коллинеаций порядка 73, которая, конечно, циклична. Точки можно представить как вычеты по модулю 73. Число 2 — множитель плоскости. Если  $a_1, \dots, a_9$  — точки некоторой прямой, то  $2a_1, \dots, 2a_9$  — точки  $a_1 + s, \dots, a_9 + s$ , взятые в некотором порядке (при подходящем  $s$ ). Тогда точки  $a_1 - s, \dots, a_9 - s$  лежат на прямой, оставляемой на месте множителем 2. Если один из вычетов равен 1, то множитель 2 дает полное множество точек прямой 1, 2, 4, 8, 16, 32, 37, 55, 64 ( $\text{mod } 73$ ). Любое другое множество, оставляемое на месте множителем 2, отличается от этого постоянным сомножителем и дает ту же самую плоскость. Эта плоскость дезаргова.

Хьюгес получил дальнейший результат, который одновременно и более частный, и более тонкий, чем теорема 20.9.10.

**Теорема 20.9.12.** Плоскость  $\pi$  порядка  $n$ , где  $n \equiv 2 \pmod{4}$ ,  $n > 2$ , не имеет инволюций.

*Доказательство.* Пусть плоскость  $\pi$  порядка  $n$ , где  $n \equiv 2 \pmod{4}$ ,  $n > 2$ , обладает инволюцией  $b$ . Тогда по теореме 20.9.7, коллинеация  $b$  является элацией, так как число  $n$  четно и не равно квадрату целого числа. Пусть  $M$  — ось, а  $C \in M$  — центр элации  $b$ , и пусть  $Q_i$  ( $i = 1, \dots, n$ ) — остальные точки прямой  $M$ , а  $K_i$  ( $i = 1, \dots, n$ ) — остальные прямые, проходящие через точку  $C$ . Положим  $n = 2m$ , где число  $m$  нечетно. Множество из  $n^2$  прямых, не содержащих точку  $C$ , можно разбить на  $n^2/2 = 2m^2$  пар прямых, отображаемых друг в друга инволюцией  $b$ . Из каждой такой пары прямых выберем одну прямую  $L_i$ ,  $i = 1, \dots, 2m^2$ . Подобным образом множество из  $n$  точек прямой  $K_i$ , отличных от точки  $C$ , можно разбить на  $n/2 = m$  пар, отображаемых друг в друга инволюцией  $b$ . Из каждой такой пары точек выберем одну точку  $P_{ij}$ ,  $j = 1, \dots, n/2 = m$ . Определим теперь числа инцидентности  $a_{ij}^k$ :

$$\begin{aligned} a_{ij}^k &= +1, && \text{если } P_{ij} \in L_k, \\ a_{ij}^k &= -1, && \text{если } P_{ij} b \in L_k, \\ a_{ij}^k &= 0 && \text{во всех других случаях.} \end{aligned} \quad (20.9.49)$$

**Лемма 20.9.3.**  $\sum_k (a_{ij}^k)^2 = n$ .

**Лемма 20.9.4.**  $\sum_k a_{ij}^k a_{st}^k = 0$ , если  $(i, j) \neq (s, t)$ .

*Доказательство леммы 20.9.3.* Точка  $P_{ij}$  лежит или на  $n$  прямых  $L_k$ , или на  $n$  прямых  $L_k b$ , откуда сразу следует требуемое соотношение.

*Доказательство леммы 20.9.4.* Если  $i = s$ ,  $j \neq t$ , то точки  $P_{ij}$  и  $P_{ij}b$  все лежат на прямой  $K_i$  и никакие две из них не лежат на другой прямой, откуда следует, что рассматриваемая сумма равна нулю. Если  $i \neq s$ , пусть  $P_{ij}P_{st} = L_qx$ ,  $P_{ij}P_{st}b = L_r y$ , где коллинеации  $x$  и  $y$  равны 1 или  $b$ . Теперь  $r \neq q$ , так как если  $r = q$  и  $x = y$ , то прямая  $L_qx = L_r y$  содержит точки  $P_{st}$  и  $P_{st}b$ , являющиеся различными точками прямой  $K_s$ , что невозможно. Если же  $r = q$  и  $x = yb$ , то прямая  $L_qx = L_r yb$  содержит различные точки  $P_{ij}$  и  $P_{ij}b$ , лежащие на прямой  $K_i$ , что также невозможно. Итак,  $r \neq q$ . Но тогда  $a_{ij}^q = a_{st}^q$ ,  $a_{ij}^q a_{st}^q = +1$  и  $a_{ij}^r = -a_{st}^r$ ,  $a_{ij}^r a_{st}^r = -1$ . Поэтому ненулевых слагаемых, равных  $+1$ , в сумме леммы 20.9.4 ровно столько, сколько слагаемых, равных  $-1$ . Следовательно, вся сумма равна нулю, и лемма 20.9.4 доказана.

Составим теперь из чисел инцидентности  $a_{ij}^k$  квадратную матрицу порядка  $2m^2$ :

$$A = (a_{ij}^k), \quad ij \text{ — номер строки, } k \text{ — номер столбца,} \quad (20.9.50)$$

обладающую, согласно нашим леммам, свойством

$$AA^T = nI. \quad (20.9.51)$$

Определим теперь числа  $b_{ik}$ :

$$b_{ik} = \sum_{j=1}^m a_{ij}^k, \quad i = 1, \dots, n; \quad k = 1, \dots, 2m^2. \quad (20.9.52)$$

Любое число  $b_{ik}$  равно  $+1$  или  $-1$ , так как каждая прямая  $L_k$  пересекает прямую  $K_i$  в единственной точке  $P_{ij}$  или  $P_{ij}b$ , и поэтому только одно из чисел  $a_{ij}^k$  отлично от нуля. Матрица  $B$  с  $n$  строками и  $2m^2$  столбцами

$$B = (b_{ik}), \quad i = 1, \dots, n; \quad k = 1, \dots, 2m^2, \quad (20.9.53)$$

обладает тем свойством, что ее первая строка равна сумме первых  $m$  строк матрицы  $A$ , ее вторая строка равна сумме вторых  $m$  строк матрицы  $A$  и т. д. Так как, согласно (20.9.51), произведение различных строк матрицы  $A$  равно нулю, это же свойство справедливо и для строк матрицы  $B$ . Столбцы матрицы  $B$  можно умножить на  $+1$  или на  $-1$ , не изменив их скалярного

произведения. Мы так домножим столбцы матрицы  $B$ , чтобы первая строка ее состояла только из единиц со знаком  $+$ . Так как  $n > 2$ , матрица  $B$  имеет не менее трех строк; после соответствующей перестановки столбцов матрицы  $B$  первые ее три строки примут вид

$$\left| \begin{array}{cccc} +1, & \dots & , +1 \\ +1, \dots, +1 & +1, \dots, +1 \\ +1, \dots, +1 & -1, \dots, -1 \end{array} \right| \left| \begin{array}{cccc} +1, & \dots & , +1 \\ -1, \dots, -1 & -1, \dots, -1 \\ +1, \dots, +1 & -1, \dots, -1 \end{array} \right| \quad (20.9.54)$$

$r \qquad s \qquad t \qquad u$

Так как скалярные произведения второй и третьей строк с первой равны нулю, мы имеем  $r+s=t+u$ ,  $r+t=s+u$ . При этом  $r+s+t+u=2m^2$ . Поэтому

$$r+s=t+u=m^2, \quad r+t=s+u=m^2, \quad (20.9.55)$$

откуда

$$u=r, \quad s=t=m^2-r. \quad (20.9.56)$$

Так как скалярное произведение второй и третьей строк также равно нулю,  $r+u=s+t=m^2$ , откуда

$$2r=m^2. \quad (20.9.57)$$

Но это противоречит условию  $n \equiv 2 \pmod{4}$ ,  $n=2m$ , где число  $m$  нечетно. Следовательно, плоскость  $\pi$  не имеет инволюций, и теорема доказана. Этот результат можно также получить из соотношений (20.9.25) путем соответствующей перенумерации элементов кольца  $G^*$  и гомоморфного отображения  $G^*$  в кольцо целых чисел, при котором  $1 \rightarrow 1$ ,  $b \rightarrow -1$ .

Пример недезарговой плоскости порядка 9 был найден Вебленом и Веддербарном [1]. Как показал Хьюгес [2], этот пример является частным случаем бесконечной серии плоскостей такого рода. Пусть  $q=p'$  — степень нечетного простого числа  $p$ . Тогда, как мы показали, существует почти-поле  $K$  порядка  $q^2$ , центром  $Z$  которого является поле  $GF(q)=GF(p')$ . Плоскости Хьюгеса имеют порядок  $q^2$ .

**ОПРЕДЕЛЕНИЕ** плоскостей Хьюгеса. Пусть  $P$  — это множество троек  $P=(xk, yk, zk)$ , где  $x, y, z$  — фиксированные элементы из  $K$ , не все равные нулю, а  $k \neq 0$  — произвольный элемент из  $K$ . Теорема Зингера 20.9.5 дает нам отображение

$$\begin{aligned} x &\rightarrow a_{11}x + a_{12}y + a_{13}z, \\ y &\rightarrow a_{21}x + a_{22}y + a_{23}z, \\ z &\rightarrow a_{31}x + a_{32}y + a_{33}z \end{aligned} \quad (20.9.58)$$

$(a_{ij} \in Z)$ , такое, что отображение

$$(x, y, z) = P \rightarrow PA = (a_{11}x, \dots, \dots, \dots, a_{33}z) \quad (20.9.59)$$

является коллинеацией  $\alpha$  порядка  $m = q^2 + q + 1$  дезарговой плоскости порядка  $q$  с координатами из поля  $Z$ . Плоскость Хьюгеса получается распространением коллинеации  $\alpha$  на точки с координатами из почти-поля  $K$ .

Определим основные прямые  $L_t$  уравнениями

$$x + ty + z = 0, \quad (20.9.60)$$

где или  $t = 1$ , или  $t \notin Z$ , а в остальном  $t$  — произвольный элемент из  $K$ . Число основных прямых равно  $1 + (q^2 - q) = q^2 - q + 1$ . Определим теперь отношение инцидентности:  $P = (xk, yk, zk) \in L_t$  тогда и только тогда, когда тройка чисел  $x, y, z$  является решением уравнения (20.9.60). В силу ассоциативности умножения в почти-поле  $K$  и правого дистрибутивного закона из (20.9.60), мы также имеем

$$0 = (x + ty + z)k = xk + t(yk) + zk, \quad (20.9.61)$$

т. е. отношение инцидентности  $P \in L_t$  не зависит от представления точки  $P$ , удовлетворяющей (20.9.60). Далее, формально определяем прямые  $L_t \alpha^i$ ,  $i = 0, \dots, m - 1$ . При этом

$$PA^i \in L_t \alpha^i, \quad i = 0, \dots, m - 1, \quad (20.9.62)$$

тогда и только тогда, когда  $P \in L_t$ .

Точки прямой  $L_t \alpha^i$  не обязательно удовлетворяют линейному уравнению. Чтобы найти точки прямой  $L_t$ , мы можем в соотношении (20.9.60) выбрать числа  $x$  и  $y$  произвольным образом (но только так, чтобы оба не были одновременно равны нулю) и определить  $z$ . Отсюда получается  $q^4 - 1$  троек чисел, из которых  $q^2 - 1$  представляют одну и ту же точку. Поэтому прямая  $L_t$  состоит из  $q^2 + 1 = n + 1$  различных точек. Следовательно, прямая  $L_t \alpha^i$  также содержит  $n + 1$  точек. Мы имеем всего  $(q^2 - q + 1)(q^2 + q + 1) = q^4 + q^2 + 1 = n^2 + n + 1$  прямых, на каждой из которых  $n + 1$  точек. Всего же точек  $n^2 + n + 1$ . Поэтому, чтобы показать, что это проективная плоскость, достаточно показать, что любые две прямые пересекаются в одной точке. Отображение  $P \rightarrow PA$  взаимно однозначно и имеет порядок  $m = q^2 + q + 1$ . Если  $\{P\}_s$  — множество точек основной прямой  $L_s$ , то прямая  $L_s \alpha^i$  состоит из множества точек  $\{P\}_s A^i$ , а прямая  $L_t \alpha^j$  — из множества точек  $\{P\}_t A^j$ . Теперь, чтобы показать, что прямые  $L_s \alpha^i$

и  $L_t\alpha^j$  пересекаются в одной-единственной точке, достаточно показать, что прямые  $L_s$  и  $L_t\alpha^{j-i} = L_t\alpha^h$  (где показатель степени  $h$  берется по модулю  $m$ ) пересекаются в одной точке.

Пусть  $P = (x, y, z)$  — точка прямой  $L_t\alpha^h$ . Тогда  $PA^{-h}$  — точка прямой  $L_t$ , и обратно. Если теперь

$$(x, y, z) A^{-h} = (b_{11}x + b_{12}y + b_{13}z, \\ b_{21}x + b_{22}y + b_{23}z, b_{31}x + b_{32}y + b_{33}z), \quad (20.9.63)$$

то условие принадлежности точки  $P(x, y, z)$  прямой  $L_t\alpha^h$  выражается соотношением

$$(b_{11}x + b_{12}y + b_{13}z) + t(b_{21}x + b_{22}y + b_{23}z) + \\ + (b_{31}x + b_{32}y + b_{33}z) = 0. \quad (20.9.64)$$

Если же точка  $(x, y, z)$  лежит на прямой  $L_s$ , то

$$x + sy + z = 0. \quad (20.9.65)$$

Мы должны теперь показать, что с точностью до правого сомножителя  $k$  система уравнений (20.9.64) и (20.9.65) имеет единственное решение  $(x, y, z)$ . Из равенства (20.9.65) находим выражение для  $x$ , подставляем это значение в (20.9.64) и получаем

$$uy + az + t(vy + bz) = 0, \quad (20.9.66)$$

где

$$\begin{aligned} u &= b_{12} + b_{32} - (b_{11} + b_{31})s, \\ v &= b_{22} - b_{21}s, \\ z &= b_{13} + b_{33} - (b_{11} + b_{31}), \\ b &= b_{23} - b_{21}. \end{aligned} \quad (20.9.67)$$

Заметим, что  $a, b \in Z$ , но, вообще говоря,  $u, v \notin Z$ . Чтобы решить уравнение (20.9.66), рассмотрим три случая.

Случай 1.  $b \neq 0$ . Уравнение (20.9.66) теперь можно переписать в виде

$$(b^{-1}a + t)(vy + bz) + (u - b^{-1}av)y = 0, \quad (20.9.68)$$

так как элементы  $a$  и  $b^{-1}$  принадлежат центру  $Z$ . Если бы оба коэффициента  $b^{-1}a + t$  и  $u - b^{-1}av$  были равны нулю, то мы бы имели  $t \in Z$ ,  $t = 1$ ,  $a + b = 0$  и  $u + v = 0$ . Но тогда из равенства  $u + v = 0$  мы бы получили, что

$$b_{12} + b_{22} + b_{32} = (b_{11} + b_{21} + b_{31})s, \quad (20.9.69)$$

откуда  $s \in Z$ , т. е.  $s = 1$ , а из равенства  $a + b = 0$  мы бы имели

$$b_{13} + b_{23} + b_{33} = b_{11} + b_{21} + b_{31}. \quad (20.9.70)$$

Но при  $s = 1$  и  $t = 1$  это означает, что уравнения (20.9.64) и (20.9.65) представляют одну и ту же прямую дезарговой плоскости  $\pi_1$  над полем  $GF(q)$ . Но это невозможно, если не имеет место  $L_s = L_t$ ,  $L_t \alpha^t = L_1$ , так как матрица  $A$  порядка  $m = q^2 + q + 1$  определяет коллинеацию плоскости  $\pi_1$ . Итак, хотя бы один из коэффициентов в соотношении (20.9.68) не равен нулю. Так, если  $b^{-1}a + t \neq 0$ , то произвольное значение  $u$  определяет  $vy + bz$  однозначно, а так как  $b \neq 0$ ,  $y$  однозначно определяет  $z$ . Если же  $b^{-1}a + t = 0$ , то  $u - b^{-1}av \neq 0$ . Тогда  $y = 0$ , откуда  $z$  — произвольное число. Таким образом,  $y$  и  $z$  определяются однозначно с точностью до правого сомножителя, а  $x$  определяется однозначно через  $y$  и  $z$  из уравнения (20.9.65). Таким образом, система уравнений (20.9.64) и (20.9.65) удовлетворяется единственной точкой  $(xk, yk, zk)$ . Это и есть искомый результат в случае 1.

**Случай 2.**  $b = 0$ ,  $a \neq 0$ . Теперь уравнение (20.9.66) принимает вид

$$(u + tv)y + az = 0. \quad (20.9.71)$$

Так как  $a \neq 0$ , система уравнений (20.9.71) и (20.9.65) удовлетворяется единственной точкой  $(xk, yk, zk)$ .

**Случай 3.**  $b = 0$ ,  $a = 0$ . Теперь

$$\begin{aligned} b_{13} + b_{33} &= b_{11} + b_{31}, \\ b_{23} &= b_{21}. \end{aligned} \quad (20.9.72)$$

Нетрудно заметить, что точка  $P = (k, 0, -k)$  удовлетворяет уравнениям (20.9.66) и (20.9.65). Кроме того, учитывая соотношение (20.9.63), из равенств (20.9.72) мы видим, что

$$PA^{-h} = (k, 0, -k)A^{-h} = (b_{11} - b_{13})(k, 0, -k) = P, \quad (20.9.73)$$

где  $b_{11} - b_{13} \neq 0$ , так как преобразование  $A^{-h}$  невырожденное. Но так как отображение  $A^h$  оставляет неподвижной точку  $P$  плоскости  $\pi_1$ , то  $h \equiv 0 \pmod{m}$  и поэтому  $L_t \alpha^h = L_t$ . Итак, задача свелась к нахождению точки пересечения двух прямых  $L_s$  и  $L_t$ , где, конечно,  $s \neq t$ . Эти прямые определяются уравнениями  $x + sy + z = 0$  и  $x + ty + z = 0$ , откуда видно, что точка  $P = (k, 0, -k)$  — единственная точка, принадлежащая обеим этим прямым. Таким образом, в каждом случае любые две различные прямые имеют единственную точку пересечения. Этим мы доказали, что они образуют проективную плоскость. Сформулируем полученный результат в виде теоремы.

Теорема 20.9.13. (Хьюгес.) Пусть  $K$  — почти-поле, состоящее из  $q^2$  элементов с центром  $Z = GF(q)$ , где  $q = p^r$ ,  $p$  — простое нечетное число;  $A$  — отображение вида (20.9.58) порядка  $q^2 + q + 1$ , определяющее коллинеацию дезарговой плоскости порядка  $q$ . Тогда прямые  $L_i \alpha^i$ , содержащие точки  $PA^i$  в смысле инцидентностей (20.9.60) и (20.9.61), образуют проективную плоскость  $\pi$  порядка  $q^2$ .

Хьюгес показал, что если почти-поле  $K$  не является полем  $FG(q^2)$ , то плоскость  $\pi$  не только недезаргова, но даже не является плоскостью Веблена — Веддербарна относительно какой-либо системы координат.

## ЛИТЕРАТУРА

Альберт (Albert A. A.)

- [1] On nonassociative division algebras, *Trans. Amer. Math. Soc.*, 72 (1952), 296—309.

Бернсайд (Burnside W.)

- [1] On an unsettled question in the theory of discontinuous groups, *Quart. J. Pure and Appl. Math.*, 33 (1902), 230—238.  
[2] Theory of Groups of Finite Order, Cambridge Univ. Press, 2nd ed., 1911.

Бете (Bethe H. A.)

- [1] Termaufspaltung in Kristallen, *Ann. Phys.*, (5), 3 (1929), 133—208.

Биркгоф (Birkhoff G.)

- [1] Lattice Theory, Colloquium publications, Amer. Math. Soc., vol. XXV, rev. ed., 1948; русский перевод: Биркгоф Г., Теория структур, ИЛ, М., 1952.

Биркгоф, Маклейн (Birkhoff G., MacLane S.)

- [1] A Survey of Modern Algebra, Macmillan Co., rev. ed., 1953.

Брук (Bruck R. H.)

- [1] Difference sets in a finite group, *Trans. Amer. Math. Soc.*, 78 (1955), 464—481.

Брук, Клейнфельд (Bruck R. H., Kleinfield E.)

- [1] The structure of alternative division rings, *Proc. Amer. Math. Soc.*, 2 (1951), 878—890.

Брук, Райзер (Bruck R. H., Ryser H. J.)

- [1] The non-existence of certain finite projective planes, *Can. J. Math.*, 1 (1949), 88—93.

Бэр (Baer R.)

- [1] Erweiterung von Gruppen und ihrer Isomorphismen, *Math. Zeit.*, 38 (1934), 375—416.  
[2] The decomposition of enumerable primary Abelian groups into direct summands, *Quart. J. Math.*, 6 (1935), 217—221.  
[3] The decomposition of Abelian groups into direct summands, *Quart. J. Math.*, 6 (1935), 222—232.  
[4] Types of elements and the characteristic subgroups of Abelian groups, *Proc. London Math. Soc.*, 39 (1935), 481—514.  
[5] The subgroup of elements of finite order of an Abelian group, *Ann. Math.*, 37 (1936), 766—781.  
[6] Dualism in Abelian groups, *Bull. Amer. Math. Soc.*, 43 (1937), 121—124.  
[7] Duality and commutativity of groups, *Duke Math. J.*, 5 (1939), 824—838.  
[8] The significance of the system of subgroups for the structure of a group, *Amer. J. Math.*, 61 (1939), 1—44.  
[9] Abelian groups that are direct summands of every containing Abelian group, *Bull. Amer. Math. Soc.*, 46 (1940), 800—806.

- [10] Homogeneity of projective planes, *Amer. J. Math.*, **64** (1942), 137—152.
- [11] Klassification der Gruppenerweiterungen. *J. reine angew. Math.*, **187** (1949), 75—94.
- [12] Supersoluble groups, *Proc. Amer. Math. Soc.*, **6** (1955), 16—32.
- Ван дер Варден** (van der Waerden B. L.)
- [1] Moderne Algebra, 2nd ed., Berlin, 1940; русский перевод: Ван дер Варден Б. Л., Современная алгебра, Гостехиздат, ч. I, 1947; ч. II, 1948.
- Веблен**, **Веддербурн** (Veblen O., Wedderburn J. H. M.)
- [1] Non-Desarguesian and non-Pascalian geometries, *Trans. Amer. Math. Soc.*, **8** (1907), 379—388.
- Веблен**, **Юнг** (Veblen O., Young J. W.)
- [1] Projective geometry, vol. 1, Ginn and Co., 1910.
- Веддербурн** (Wedderburn J. H. M.)
- [1] On the direct product in the theory of finite groups, *Ann. Math.*, **10** (1909), 173—176.
- Виландт** (Wielandt H.)
- [1] Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad, *Schriften Math. Sem. und Inst. für angew. Math. der Univ. Berlin*, **2** (1934), 151—174.
- [2] Eine Verallgemeinerung der invarianten Untergruppen, *Math. Zeit.*, **45** (1939), 209—244.
- [3]  $p$ -Sylowgruppen und  $p$ -Faktorgruppen, *J. reine angew. Math.*, **182** (1940), 180—183.
- Витт** (Witt E.)
- \* [1] Über die Kommutativität endlicher Schiefkörper, *Abh. Math. Sem. Hamburg*, **8** (1931), 413.
- [2] Treue Darstellung Liescher Ringe, *J. reine angew. Math.*, **177** (1937), 152—160.
- Гашюц** (Gashütz W.)
- [1] Zur Erweiterungstheorie der endlichen Gruppen, *J. reine angew. Math.*, **190** (1952), 93—107.
- Гёльдер** (Hölder O.)
- [1] Zurückführung einer beliebigen algebraischen Gleichung auf eine Kette von Gleichungen, *Math. Ann.*, **34** (1889), 26—56.
- Глисон** (Gleason A. M.)
- [1] Finite Fano planes, *Amer. J. Math.*, **78** (1956), 797—807.
- Гофман** (Hoffmann A. J.)
- [1] Cyclic affine planes, *Can. J. Math.*, **4** (1952), 295—301.
- Грюн** (Grün O.)
- [1] Beiträge zur Gruppentheorie I, *J. reine angew. Math.*, **174** (1935), 1—14.
- Жордан** (Jordan C.)
- [1] Commentaire sur Galois, *Math. Ann.*, **1** (1869), 141—160.
- [2] Recherches sur les substitutions, *J. Math. Pures Appl.* (2), **17** (1872), 351—363.
- Зингер** (Singer J.)
- [1] A theorem in finite projective geometry and some applications to number theory, *Trans. Amer. Math. Soc.*, **43** (1938), 377—385.
- Ивасава** (Iwasawa K.)
- [1] Über die endlichen Gruppen und die Verbände ihrer Untergruppen, *J. Univ. Tokyo*, **43** (1941), 171—199.
- Капланский** (Kaplansky I.)
- [1] Infinite Abelian Groups, Univ. Michigan Press, 1954.

К лейнфельд (Kleinfield E.)

- [1] Alternative division rings of characteristic 2, *Proc. Nat. Acad. Sci. USA*, 37 (1951), 818—820.

- [2] Right alternative rings, *Proc. Amer. Math. Soc.*, 4 (1953), 939—944.

К р у лль (Krull W.)

- [1] Über verallgemeinerte endliche Abelsche Gruppen, *Math. Zeit.*, 23 (1925), 161—196.

- [2] Theorie und Anwendung der verallgemeinerten Abelschen Gruppen, *Sitz. Heidelberg. Akad. Wiss.* (1926), 1—32.

К урош А. Г.

- [1] Die Untergruppen der freien Produkte von beliebigen Gruppen, *Math. Ann.*, 109 (1934), 647—660.

Леви (Levi F. W.)

- [1] Über die Untergruppen der freien Gruppen, *Math. Zeit.*, 32 (1930), 315—318.

Леви, Ван дер Варден (Levi F. W., van der Waerden B. L.)

- [1] Über eine besondere Klasse von Gruppen, *Abh. Math. Sem. Hamburg*, 9 (1933), 154—158.

М а г н у с (Magnus W.)

- [1] Über Beziehungen zwischen höheren Kommutatoren, *J. reine angew. Math.*, 177 (1937), 105—115.

- [2] On a theorem of Marshall Hall, *Ann. Math.*, 40 (1939), 764—768.

- [3] A connection between the Baker-Hausdorff formula and a problem of Burnside, *Ann. Math.*, 52 (1950), 111—126.

М аклейн (MacLane S.)

- [1] A conjecture of Ore on chains in partially ordered sets, *Bull. Amer. Math. Soc.*, 49 (1943), 567—568.

- [2] Cohomology theory in abstract groups, III, *Ann. Math.*, 50 (1949), 736—761.

М а н н (Mann H. B.)

- [1] On certain systems which are almost groups, *Bull. Amer. Math. Soc.*, 50 (1944), 879—881.

М ейер-Вундерли (Meier-Wunderli H.)

- [1] Note on a basis for higher commutators, *Commentarii Math. Helvetica*, 16 (1951), 1—5.

М иллер (Miller G. A.)

- [1] Limits of the degree of transitivity of substitution groups, *Bull. Amer. Math. Soc.*, 22 (1915), 68—71.

М у фанг (Moufang R.)

- [1] Alternativkörper und der Satz vom vollständigen Vierseit, *Abh. Math. Sem. Hamburg*, 9 (1933), 207—222.

Н ейман Б. (Neumann B. H.)

- [1] Die Automorphismengruppe der freien Gruppen, *Math. Ann.*, 107 (1932), 367—386.

- [2] On the number of generators of a free product, *J. London Math. Soc.*, 18 (1943), 12—20.

Н ейман Г. (Neumann H.)

- [1] Generalized free products with amalgamated subgroups I, *Amer. J. Math.*, 70 (1948), 590—625.

- [2] Generalized free products with amalgamated subgroups II, *Amer. J. Math.*, 71 (1949), 491—540.

Н ётер (Noether E.)

- [1] Hyperkomplexe Zahlen und Darstellungstheorie, *Math. Zeit.*, 30 (1929), 641—692.

Нильсен (Nielsen J.)

- [1] Om Regnig med ikke-kommulative Faktorer og dens Anvendelse i Gruppeteorien, *Mat. Tidsskrift*, B (1921), 77—94.

Оре (Ore O.)

- [1] Direct Decompositions, *Duke Math. J.*, 2 (1936), 581—596.  
[2] On the theorem of Jordan — Hölder, *Trans. Amer. Math. Soc.*, 41 (1937), 266—275.  
[3] Chains in partially ordered sets, *Bull. Amer. Math. Soc.*, 49 (1943), 558—566.

Остром (Ostrom T. G.)

- [1] Double transitivity in finite projective planes, *Can J. Math.*, 8 (1956), 563—567.

Паркер (Parker E. T.)

- [1] On collineations of symmetric designs, *Proc. Amer. Math. Soc.*, 8 (1957), 350—351.

Паули (Pauli W.)

- [1] Zur Quantenmechanik der Magnetischen Elektrons, *Zeit. Phys.*, 43 (1927), 601—623.

Пиккерт (Pickert G.)

- [1] Projektive Ebenen, Springer, 1955.

Прюфнер (Prüfer H.)

- [1] Theorie der abelschen Gruppen I, *Math. Zeit.*, 20 (1924), 165—187.  
[2] Theorie der abelschen Gruppen II, *Math. Zeit.*, 22 (1925), 222—249.

Ремак (Remak R.)

- [1] Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, *J. reine angew. Math.*, 139 (1911), 293—308.

- [2] Über die Zerlegung der endlichen Gruppen in direkte unzerlegbare Faktoren, *J. reine angew. Math.*, 153 (1923), 131—140.

Сан Суци (San Soucie R. L.)

- [1] Right alternative division rings of characteristic two, *Proc. Amer. Math. Soc.*, 6 (1955), 291—296.

Судзуки (Suzuki M.)

- [1] Structure of a group and the structure of its lattice of subgroups, *Ergebnisse der Mathematik und ihrer Grenzgebiete*, 10, 1956, Springer, Berlin; русский перевод: Судзуки М., Строение группы и строение структуры ее подгрупп, ИЛ, М., 1960.

Тарри (Tarry G.)

- [1] Le problème des 36 officiers, *C. R. Assoc. Fr. Av. Sci.*, 1900, 122—123; 1901, 170—203.

Ульм (Ul'm H.)

- [1] Zur Theorie der abzählbar unendlichen abelschen Gruppen, *Math. Ann.*, 107 (1933), 774—803.

Федерер, Джонсон (Federer H., Johnson B.)

- [1] Some properties of free groups, *Trans. Amer. Math. Soc.*, 68 (1950), 1—27.

Фробениус (Frobenius G.)

- [1] Über auflösbare Gruppen, IV Berl. Sitz. (1901), 1223—1225.  
[2] Über einen Fundamentalsatz der Gruppentheorie, Berl. Sitz. (1903), 987—991.

Харди, Райт (Hardy G. H., Wright E. M.)

- [1] An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1938.

Хигман (Higman G.)

- [1] On finite groups of exponent five, *Proc. Camb. Philos. Soc.*, 52 (1956), 381—390.

**Хирш (Hirsch K. A.)**

- [1] On infinite soluble groups, *Proc. London Math. Soc.* (2), **44** (1938), 53—60.
- [2] On infinite soluble groups II, там же, **44** (1938), 336—344.
- [3] On infinite soluble groups, III, там же, **49** (1946), 184—194.

**Холике (Holyoke T. C.)**

- [1] On the structure of multiply transitive permutation groups, *Amer. J. Math.*, **74** (1952), 787—796.

**Холл М. (Hall M., Jr.)**

- [1] Group rings and extensions, *Ann. Math.*, **39** (1938), 220—234.
- [2] Projective planes, *Trans. Amer. Math. Soc.*, **54** (1943), 229—277; Correction, *Trans. Amer. Math. Soc.*, **65** (1949), 473—474.
- [3] Cyclic projective planes, *Duke Math. J.*, **14** (1947), 1079—1090.
- [4] Coset representation in free groups, *Trans. Amer. Math. Soc.*, **67** (1949), 421—432.
- [5] Subgroups of finite index in free groups, *Can. J. Math.*, **1** (1949), 187—190.

- [6] A basis for free Lie rings and higher commutators in free groups, *Proc. Amer. Math. Soc.*, **1** (1950), 575—581.
- [7] Subgroups of free products, *Pacific J. Math.*, **3** (1953), 115—120.
- [8] On a theorem of Jordan, *Pacific J. Math.*, **4** (1954), 219—226.
- [9] Solution of the Burnside problem for exponent 6, *Proc. Nat. Acad. Sci. USA*, **43** (1957), 751—753.

**Холл М., Радо (Hall M. Jr., Radó T.)**

- [1] On Schreier systems in free groups, *Trans. Amer. Math. Soc.*, **64** (1948), 386—408.

**Холл М., Райзер (Hall M. Jr., Ryser H. J.)**

- [1] Normal completions of incidence matrices, *Amer. J. Math.*, **76** (1954), 581—589.

**Холл Ф. (Hall Ph.)**

- [1] A note on soluble groups, *J. London Math. Soc.*, **3** (1928), 98—105.
- [2] A contribution to the theory of groups of prime-power order, *Proc. London Math. Soc.*, **36** (1933), 29—95.
- [3] On a Theorem of Frobenius, *Proc. London Math. Soc.*, **40** (1936), 468—501.

**Холл Ф., Хигман Г. (Hall Ph., Higman G.)**

- [1] The  $p$ -length of a  $p$ -soluble group, and reduction theorems for Burnside's problem, *Proc. London Math. Soc.* (3), **7** (1956), 1—42.

**Хупперт (Huppert B.)**

- [1] Normalteiler und maximale Untergruppen endlicher Gruppen, *Math. Zeit.*, **60** (1954), 409—434.

**Хьюгес (Hughes D. R.)**

- [1] Regular collineation groups, *Proc. Amer. Math. Soc.*, **8** (1957), 159—164.
- [2] A class of non-Desarguesian projective planes, *Can. J. Math.*, **9** (1957), 378—388.
- [3] Generalized incidence matrices over group algebras, *Ill. J. Math.*, **1** (1957), 545—551.
- [4] Collineations and generalized incidence matrices, *Trans. Amer. Math. Soc.*, **86** (1957), 284—296.

**Цассенхауз (Zassenhaus H.)**

- [1] Zum Satz von Jordan-Hölder-Schreier, *Abh. Math. Sem. Hamburg*, **10** (1934), 106—108.
- [2] Über endliche Fastkörper, *Abh. Math. Sem. Hamburg*, **11** (1936), 187—220.

- Цорн (Zorn M.)  
 [1] Theorie der alternativen Ringe, *Abh. Math. Sem. Hamburg*, 8 (1931), 123—147.
- Чоула, Райзэр (Chowla S., Ryser H. J.)  
 [1] Combinatorial problems, *Can. J. Math.*, 2 (1950), 93—99.
- Шмидт О. Ю.  
 [1] Über die Zerlegung endlicher Gruppen in direkte unzerlegbare Faktoren, *Изв. Киевского ун-та*, (1912), 1—6.
- Шрейер (Schreier O.)  
 [1] Über die Erweiterung von Gruppen, I, *Monats. Math. und Phys.*, 34 (1926), 165—180.  
 [2] Über die Erweiterung von Gruppen, II, *Abh. Math. Sem. Hamburg*, 4 (1926), 321—346.  
 [3] Die Untergruppen der freien Gruppen, *Abh. Math. Sem. Hamburg*, 5 (1927), 161—183.  
 [4] Über den Jordan—Hölderschen Satz, *Abh. Math. Sem. Hamburg*, 6 (1928), 300—302.
- Эйленберг, Маклейн (Eilenberg S., MacLane S.)  
 [1] Cohomology theory in abstract groups I, *Ann. Math.*, 48 (1947), 51—78.  
 [2] Cohomology theory in abstract groups II, *Ann. Math.*, 48 (1947), 326—341.
- Экман (Eckmann B.)  
 [1] Cohomology of groups and transfer, *Ann. Math.*, 58 (1953), 481—493.

## ДОПОЛНЕНИЕ К ЛИТЕРАТУРЕ

Дополнительно к литературе английского оригинала здесь приводятся названия ряда книг и обзорных статей по теории групп на русском языке, а также небольшое число советских оригинальных работ, примыкающих по своей тематике к разделам теории групп, трактуемым в книге. Более полную библиографию советской литературы по теории групп можно найти в „Теории групп“ А. Г. Куроша [1] (особенно изд. 2) и в сборнике „Математика в СССР за 40 лет“ [3].

### КНИГИ И ОБЗОРНЫЕ СТАТЬИ

- Курош А. Г.  
 [1] Теория групп, изд. 1, Гостехиздат, М., 1944, изд. 2, 1953.  
 [2] Алгебра II (Группы, кольца, структуры), Сборник „Математика в СССР за 30 лет“, Гостехиздат, М., 1948, стр. 106—133.
- Курош А. Г., Глушков В. М.  
 [3] Общая алгебра, Сборник „Математика в СССР за 40 лет“, том 1, Физматгиз, М., 1959, стр. 151—200.
- Курош А. Г., Черников С. Н.  
 [4] Разрешимые и нильпотентные группы, *УМН*, 2, № 3 (1947), 18—59.
- Плоткин Б. И.  
 [5] Обобщенно разрешимые и обобщенно нильпотентные группы, *УМН*, 13, № 4 (1958), 89—172.
- Понtryагин Л. С.  
 [6] Непрерывные группы, изд. 2, Гостехиздат, М., 1954.
- Черников С. Н.  
 [7] Условия конечности в общей теории групп, *УМН*, 14, № 5 (1959), 45—96.
- Шмидт О. Ю.  
 [8] Абстрактная теория групп, изд. 2, Гостехиздат, М., 1933.

**К ПРОБЛЕМЕ БЕРНСАЙДА И К ТЕОРИИ Р-ГРУПП  
(ГЛАВЫ 12 и 18)**

**Кемхадзе Ш. С.**

[1] К определению регулярных  $p$ -групп, *УМН*, 7, № 6 (1952), 193—196.

**Кострикин А. И.**

[2] Решение ослабленной проблемы Бернсайда для показателя 5, *Изв. АН СССР*, сер. матем., 19 (1955), 233—244.

[3] О связях между периодическими группами и кольцами Ли, *Изв. АН СССР*, сер. матем., 21 (1957), 289—310.

[4] Кольца Ли, удовлетворяющие условию Энгеля, *Изв. АН СССР*, 21 (1957), 515—540.

[5] О локальной нильпотентности колец Ли, удовлетворяющих условию Энгеля, *ДАН СССР*, 118 (1958), 1074—1077.

[6] О проблеме Бернсайда, *ДАН СССР*, 119 (1958), 1081—1084.

**Новиков П. С.**

[7] О периодических группах, *ДАН СССР*, 127 (1959), 749—752.

**Санов И. Н.**

[8] Решение проблемы Бернсайда для показателя 4, *Учен. зап. Ленингр. унив.*, сер. матем., 10 (1940), 166—170.

[9] О проблеме Бернсайда, *ДАН СССР*, 57 (1947), 759—761.

[10] Применение колец Ли к теории периодических  $p$ -групп, *УМН*, 4, № 3 (1949), 180.

[11] О некоторой системе соотношений в периодических группах с периодом степенью простого числа, *Изв. АН СССР*, сер. матем., 15 (1951), 477—502.

[12] Установление связи между периодическими группами с периодом простым числом и кольцами Ли, *Изв. АН СССР*, сер. матем., 16 (1952), 23—58.

**К СТРОЕНИЮ СТРУКТУРЫ ПОДГРУПП ГРУППЫ  
(ГЛАВЫ 8 и 19)**

**Кенторович П. Г., Плоткин Б. И.**

[1] Структуры с аддитивным базисом, *Матем. сб.*, 35 (77) (1954), 187—192.

**Курош А. Г.**

[2] Теория Жордана—Гельдера в произвольных структурах, *Сборник памяти акад. Граве* (1940), 110—116.

[3] Изоморфизмы прямых разложений, *Изв. АН СССР*, сер. матем., часть I, 7 (1943), 185—202; часть II, 10 (1946), 42—47.

**Пекелис А. С.**

[4] О группах с изоморфными структурами подгрупп, *Математика*, I (1957), 180—194.

**Петропавловская Р. В.**

[5] Об определяемости группы структурой ее подгрупп, *Матем. сб.*, 29 (71) (1951), 63—78.

[6] Ассоциативные системы, структурно изоморфные группе, *Вестник Ленингр. унив.*, сер. матем., часть I, 13 (1956), 5—26; часть II, 19 (1956), 80—99.

**Садовский Л. Е.**

[7] О структурных изоморфизмах свободных групп и свободных произведений, *Матем. сб.*, 14 (1944), 155—173.

[8] О структурных изоморфизмах свободных произведений групп, *Матем. сб.*, 21 (1947), 63—82.

[9] Структура подгрупп нильпотентной группы без кручения, *УМН*, 12, № 3 (1957), 201—204.

- [10] Структурные изоморфизмы свободной метабелевой группы, *Матем. сб.*, 42 (1957), 445—460.  
**Узков А. И.**  
[11] О теореме Jordan — Hölder, *Матем. сб.*, 4 (1938), 31—43.

#### К ТЕОРИИ КОГОМОЛОГИЙ В ГРУППАХ (ГЛАВА 15)

**Боревич З. И., Фаддеев Д. К.**

- [1] Теория гомологий в группах, *Вестник Ленингр. унив.*, сер. матем., часть I, 7 (1956), 3—39; часть II, 7 (1959), 72—87.

**Фаддеев Д. К.**

- [2] К теории гомологий в группах, *Изв. АН СССР*, сер. матем., 16 (1952), 17—22.  
[3] Об одной теореме теории гомологий в группах, *ДАН СССР*, 92 (1953), 703—705.  
[4] К теории гомологий для конечных групп операторов, *Изв. АН СССР*, сер. матем., 19 (1955), 193—200.

#### ОБОБЩЕНИЯ ТЕОРЕМ СИЛОВА И РАЗРЕШИМЫЕ ГРУППЫ (ГЛАВА 9)

**Гольберг П. А.**

- [1] Холловские базы некоторых классов групп, *Сибирский матем. журнал*, 1 (1960), 14—44.

**Казачков Б. В.**

- [2] О теоремах типа Силова для конечных групп, *Учен. зап. Томского пед. инст.*, 8 (1951), 228—232.

- [3] О теоремах типа Силова, *ДАН СССР*, 80 (1951), 5—7.

**Чунихин С. А.**

- [4] Факторизация конечных групп, *Матем. сб.*, 39 (81) (1956), 465—490.  
[5] П-факторизация конечных групп, *Матем. сб.*, 43 (85) (1957), 49—66.  
[6] Комплексы неспециальных подгрупп и  $p$ -нильпотентность конечных групп, *ДАН СССР*, 118 (1958) 654—656.

#### ПРОЕКТИВНЫЕ ПЛОСКОСТИ (ГЛАВА 20)

**Аргунов Б. И.**

- [1] Конфигурационные постулаты в проективных плоскостях и их алгебраические эквиваленты, *Вестник Моск. унив.*, I (1948), 47—51.  
[2] Конфигурационные постулаты и их алгебраические эквиваленты, *Матем. сб.*, 26 (68) (1950), 425—456.

**Копейкина Л. И. (Головина)**

- [3] Свободные разложения проективных плоскостей, *Изв. АН СССР*, сер. матем., 9 (1945), 495—526.

**Скорняков Л. А.**

- [4] Натуральные тела веблен — веддербарновой проективной плоскости, *Изв. АН СССР*, сер. матем., 13 (1949), 447—472.  
[5] Альтернативные тела, *Укр. матем. журнал*, I (1950), 70—85.  
[6] Правоальтернативные тела, *Изв. АН СССР*, сер. матем., 15 (1951), 177—184.  
[7] Проективные плоскости, *УМН*, 6, № 6 (1951), 112—154.  
[8] Конфигурация  $D_0$ , *Матем. сб.*, 30 (72) (1952), 73—78.  
[9] Топологические проективные плоскости, *Труды Моск. матем. общ.*, 3 (1954), 347—373.

## УКАЗАТЕЛЬ СПЕЦИАЛЬНЫХ ОБОЗНАЧЕНИЙ

Некоторые символы, использованные в этой книге, стандартны. Например,  $A \sqsupseteq B$ ,  $A$  содержит  $B$ ;  $A \supset B$ ,  $A$  строго содержит  $B$ ;  $A \subseteq B$ ,  $A$  содержится в  $B$ ;  $A \subset B$ ,  $A$  строго содержится в  $B$ ;  $a \in A$ ,  $a$  принадлежит множеству  $A$ ;  $a | b$ ,  $a$  делит  $b$ ;  $a \equiv b \pmod{m}$ ,  $a$  сравнимо с  $b$  по модулю  $m$ . Общепринято перечеркивать символ для обозначения отрицания соответствующего отношения. Например,  $p \not\sim s$  обозначает, что  $p$  не делит  $s$ ;  $y \notin G$  обозначает, что  $y$  не принадлежит  $G$ .

$\alpha : x \rightarrow y$  или  $y = (x) \alpha$  — отображение или гомоморфизм

$\alpha : x \rightleftarrows y$  — взаимно однозначное отображение или изоморфизм

$\alpha = \begin{pmatrix} 1, & 2, & 3 \\ 2, & 3, & 1 \end{pmatrix}$  — подстановка

$H \cup K$  — объединение

$H \cap K$  — пересечение

$\{K\}$  — группа, порожденная множеством  $K$

$[G : H]$  — индекс  $H$  в  $G$

$N_H(S)$  — нормализатор  $S$  в  $H$

$C_H(S)$  — централизатор  $S$  в  $H$

$H = G/T$ ;  $H$  — фактор-группа  $G$  по  $T$

$g^\alpha$  — образ  $g$  при действии оператора  $\alpha$

$A \times B$  — прямое произведение

$\prod_{i \in I}$  — декартово произведение

$(x_1, x_2, \dots, x_n)$  — цикл подстановки

$A \cong B$  —  $A$  изоморфно  $B$

$G \wr H$  — сплетение  $G$  и  $H$

$[x]$  — наибольшее целое число, не превосходящее  $x$

$f \sim g$  —  $f$  эквивалентно  $g$

$\Phi(f) = g_i$ ;  $g_i$  — представитель смежного класса элемента  $f$

$a > b$ ;  $a$  покрывает  $b$

$A_i \triangleleft A_{i-1}$ ;  $A_i$  — нормальный делитель  $A_{i-1}$

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

$(x_1, \dots, x_{n-1}, x_n)$  — простой коммутатор

$\Phi = \Phi(G)$  — подгруппа Фраттини группы  $G$

- $\mu(m)$  — функция Мёбиуса  
 $r_+, R_+$  — аддитивные группы рациональных и действительных чисел  
 $Z(p^\infty)$  — определенная абелева группа  
 $\chi(a)$  — характер  
 $V_{G \rightarrow K}(g)$ , или  $V(g)$  — перенос элемента  $g$   
 $(u, v)$  — фактор из системы факторов  
 $\bar{x}$  — представитель смежного класса  
 $\bigoplus$  — прямая сумма правых идеалов  
 $\boxplus$  — прямая сумма двусторонних идеалов  
 $(f_1, f_2)$  — симметрическое билинейное скалярное произведение  
 $\prod^*$  — свободное произведение  
 $[x, y]$  — лиево произведение  
 $Q \xrightarrow{P} R$  — перспективная коллинеация  
 $x \cdot m \circ b$  — тернарная операция  
 $(x, y, z)$  — ассоциатор

## ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- Абелева группа 45  
Абсолютно неприводимое представление 287  
Автоморфизмы 39, 100—107  
— абелевых групп 102  
— свободных групп 130  
Аксиома выбора 28  
Алгебраическое число 311  
Алфавитный порядок 341  
Альтернативное тело 398  
Артина — Цорна теорема 405  
Ассоциативные законы 11, 14, 136
- Базис 47  
Базисные коммутаторы 187  
Бернсайда основная теорема 198  
— проблема 346—365  
— теоремы 57, 164, 227  
Бертрана постулат 81  
Бесконечные группы (замечания о них) 26—29  
Брука — Райзера теорема 424
- Веблена — Веддербарна система 390  
Веддербарна — Ремака — Шмидта теорема 150  
Веддербарна теорема 404  
Верхний центральный ряд 172  
Верхняя грань 135  
Верхняя полумодулярность 140  
Взаимности теорема 309  
Вилендта теорема 236  
Витта формулы 190  
Внешние автоморфизмы 101  
Внутренние автоморфизмы 101  
Вполне характеристическая подгруппа 41
- Гамильтона группы 213  
Гашюца теорема 268  
Геометрии конечные 421
- Главный ряд 144  
Голоморф 403  
Гомология 377  
Гомоморфизмы 19, 37, 38  
Грань верхняя и нижняя 135  
Группа без кручения 46  
Группа диэдра 29  
Группа расширений 248  
Группы определения 14—16  
Группы порядка  $p^a q^b$  317  
Группы порядков  $p$ ,  $p^2, pq, p^3$  60—63  
Грюна теоремы 238, 239
- Дважды транзитивная группа 411  
Двойная группа 325  
Двойной модуль 261  
Двойной смежный класс 25  
Двойственность 219, 374  
Дезаргова плоскость 402  
Дезарга теорема 378  
Декартово произведение 43  
Дистрибутивная структура 137  
Дистрибутивные законы 11  
Допустимая подгруппа 40
- Единица 11, 14  
Единичный элемент структуры 137
- Жордана — Гельдера теорема 147  
Жордана — Дедекинда цепь 139  
Ж — Д условие 139  
Жордана теорема 87
- Замкнутости законы 11  
Знакопеременная группа 72  
Значимый сомножитель 115
- Ивасава теорема 369  
Идемпотент 282

- Идемпотентности законы 136  
 Изоморфизм 18  
 Импримитивное представление 307  
 Импримитивность 77  
 Инварианты абелевой группы 51  
 Инволюция 435  
 Индекс подгруппы 21  
 Интранзитивные группы 75.
- К**вазигруппа 17  
 Кватернионов группа 33  
 Класс нильпотентности группы 172  
 Класс сопряженных элементов 24  
 Когомология 263  
 Кограница 262  
 Коллинеация 376  
 Кольцо 11  
 Кольцо Ли 354  
 Коммутант группы 158  
 Коммутативные законы 11, 136  
 Коммутатор 158  
 Комплекс 20  
 Композиционный ряд 144  
 Координаты 381  
 Коцель 262  
 Кратная транзитивность 68, 81  
 Кронекерово произведение 303  
 Куроша теорема 340  
 Кэли теорема 19
- Л**агранжа теорема 11  
 Локальное свойство 26  
 Локально циклические группы 216,  
     367  
 Лупа 17
- М**аксимальная подгруппа 28  
 Максимальности условие 25, 174  
 Матье группы 95  
 Метациклические группы 167  
 Минимальности условие 26  
 Модулярная структура 137  
 Модуль представления 274  
 Мономиальные подстановки 225  
 Муфангова плоскость 398
- Наибольшая нижняя грань 135  
 Наименьшая верхняя грань 135  
 Неприводимые представления 277  
 Нечетная подстановка 72  
 Нижний центральный ряд 171  
 Нижняя грань 135
- Нижняя полумодулярность 140  
 Нильпотентный 170  
 Нильсена свойство 125  
 Ниль-с 174  
 Нормализатор 24  
 Нормальное произведение 104—106  
 Нормальный делитель 36  
 Нормальный ряд 144  
 Нулевой элемент структуры 137  
 Нуль 11
- О**бобщенные силовские теоремы 161  
 Образ 12  
 Обратный элемент 11, 14  
 Обыкновенное представление 281  
 Объединение подгрупп 20  
 Оператор 39  
 Операторный гомоморфизм 275  
 Операторный изоморфизм 40  
 Определяющие отношения 47  
 Ортогональное представление 321  
 Ортогональности соотношения 300  
 Орэ теорема 145  
 Остаточное свойство 26  
 Отображение 12
- П**еремещение 226  
 Пересечение подгрупп 20  
 Перестановочные подгруппы 144  
 Перспективность 377  
 Перспективные частные 138  
 Поглощения законы 136  
 Подгруппа 18  
 Подпрямое произведение 76  
 Подстановка 13  
 Подстановок группы 65—99  
 Поле 12  
     — конечное 403  
 Полная структура 137  
 Полное упорядочение 27  
 Полные группы 220  
 Полугруппа 17  
 Полумодулярная структура 140  
 Полупростое кольцо 282  
 Полупрямое произведение 104  
 Порядок группы 21  
 Порядок элемента 22  
 Почти-поле 392, 410  
 Представитель смежного класса 21  
 Представление групп матрицами 273  
     — подстановками 68—72  
 Приводимое представление 276  
 Примитивная группа 77  
 Проективные плоскости 373—452

- 
- Проективные частные 138  
 Производная группа 158  
 Простая группа 36  
 Простое кольцо 289  
 Простое упорядочение 17  
 Простой коммутатор 158  
 Просто упорядоченное множество 135  
 Противоположный элемент 11  
 Прямое объединение 147  
 Прямое произведение 43  
  
 Размерность структуры 138  
 Разрешимая группа 158  
 Расширение групп 243—271  
 Регулярная  $p$ -группа 205  
 Регулярное кольцо 282  
 Регулярное представление 19  
 Редуцированное слово 108  
  
 Сверхразрешимая группа 170, 369  
 Свободная абелева группа 222  
 Свободное произведение 336  
 Свободное произведение с объединенной подгруппой 338  
 Свободные группы 111—133  
 Сервантовые подгруппы 221  
 Силовская подгруппа 56  
 Силовские теоремы 55—56  
 Симметрическая группа 72  
 Система факторов 243  
 Слово 108, 186  
 Сложный коммутатор 158  
 Смежный класс 20  
 Собирательный процесс 186, 201  
 Совершенная группа 104  
 Сопряженные элементы 23  
 Сопряженные подгруппы 24  
 Соседние слова 108  
 Спин электрона 325  
 Сплетение 96  
 Стандартное представление 119  
 Степень представления 272  
 Структура 136  
 Структура подгрупп 366—372  
 Субинвариантный 144  
  
 Тело 289  
 Тензорное произведение 302  
 Теорема о полной приводимости 178  
 Транзитивная группа 67  
  
 Транзитивное множество 67  
 Трансфинитная индукция 27  
  
 Унитарное представление 319—323  
  
 Фактор-группа 38  
 Фраттини подгруппа 177  
 Фробениуса теоремы 156, 318  
  
 Характеристическая подгруппа 41  
 Характеры 273, 293—307  
 Холла системы 392  
 Холла Филиппа теоремы 161, 183, 236  
 Холла — Хигмена теоремы 358  
 Хупперта теорема 183  
 Хьюгеса плоскости 447  
  
 Центр 24  
 Центральная коллинеация 377  
 Центральное расширение 247  
 Центральный изоморфизм 147  
 Центральный ряд 172  
 Централизатор 24  
 Цепь 135  
 Цепочка 108, 186  
 Цикл 65  
 Циклическая группа 22, 45  
 Цорна теорема 405  
 Цорна лемма 27  
  
 Частичное упорядочение 27  
 Частично упорядоченное множество 135  
 Частные 138  
 Четырежды транзитивные группы 93  
 Четная подстановка 72  
  
 Шрейера система 111  
 Шура лемма 294  
  
 Эквивалентные представления 274  
 Элация 377  
 Элементарная абелева группа 51  
 Эндоморфизм 39  
 Эрмитовы формы 320  
  
 $p$ -группа 56, 198—215  
 $p$ -дополнение 164  
 $p$ -нормальный 229  
 $p$ -разрешимый 358

## О Г Л А В Л Е Н И Е

Предисловие редактора перевода . . . . .	5
Предисловие . . . . .	9
<b>Г л а в а 1. В в е д е н и е . . . . .</b>	<b>11</b>
1.1. Алгебраические законы . . . . .	11
1.2. Отображения . . . . .	12
1.3. Определения группы и некоторых сходных систем . . . . .	14
1.4. Подгруппы, изоморфизмы, гомоморфизмы . . . . .	18
1.5. Смежные классы. Теорема Лагранжа. Циклические группы Индексы . . . . .	20
1.6. Сопряженные элементы и классы . . . . .	23
1.7. Двойные смежные классы . . . . .	24
1.8. Замечания о бесконечных группах . . . . .	26
1.9. Примеры групп . . . . .	29
Упражнения . . . . .	34
<b>Г л а в а 2. И н в ариантные подгруппы и гомоморфизмы . . . . .</b>	<b>36</b>
2.1. Инвариантные подгруппы . . . . .	36
2.2. Ядро гомоморфизма . . . . .	37
2.3. Фактор-группы . . . . .	37
2.4. Операторы . . . . .	39
2.5. Прямые и декартовы произведения . . . . .	42
Упражнения . . . . .	44
<b>Г л а в а 3. Э л е м е н т а р н а я т е о р и я а б е л е в ю с г р у п п . . . . .</b>	<b>45</b>
3.1. Определение абелевой группы. Циклические группы . . . . .	45
3.2. Некоторые структурные теоремы для абелевых групп . . . . .	46
3.3. Конечные абелевые группы. Инвариантные . . . . .	50
Упражнения . . . . .	53
<b>Г л а в а 4. Т е о р е м ы С и л о в а . . . . .</b>	<b>54</b>
4.1. Ложность обращения теоремы Лагранжа . . . . .	54
4.2. Три теоремы Силова . . . . .	55
4.3. Конечные $p$ -группы . . . . .	58
4.4. Группы порядков $p$ , $p^2$ , $pq$ , $p^3$ . . . . .	60
Упражнения . . . . .	63

---

<b>Г л а в а 5. Группы подстановок . . . . .</b>	65
5.1. Циклы . . . . .	65
5.2. Транзитивность . . . . .	67
5.3. Представления группы подстановками . . . . .	68
5.4. Знакопеременная группа $A_n$ . . . . .	72
5.5. Интранзитивные группы. Подпрямые произведения . . . . .	75
5.6. Примитивные группы . . . . .	77
5.7. Кратно-транзитивные группы . . . . .	81
5.8. О теореме Жордана . . . . .	86
5.9. Сплетение. Силовские подгруппы симметрических групп	96
Упражнения . . . . .	98
<b>Г л а в а 6. Автоморфизмы . . . . .</b>	100
6.1. Автоморфизмы алгебраических систем . . . . .	100
6.2. Автоморфизмы групп. Внутренние автоморфизмы . . . . .	100
6.3. Голоморф группы . . . . .	102
6.4. Совершенные группы . . . . .	104
6.5. Нормальные, или полупрямые, произведения . . . . .	104
Упражнения . . . . .	106
<b>Г л а в а 7. Свободные группы . . . . .</b>	108
7.1. Определение свободной группы . . . . .	108
7.2. Подгруппы свободных групп. Метод Шрейера . . . . .	111
7.3. Свободные образующие подгрупп свободных групп. Метод Нильсена . . . . .	125
Упражнения . . . . .	133
<b>Г л а в а 8. Структуры и композиционные ряды . . . . .</b>	135
8.1. Частично упорядоченные множества . . . . .	135
8.2. Структуры . . . . .	136
8.3. Модулярные и полумодулярные структуры . . . . .	138
8.4. Главные и композиционные ряды . . . . .	143
8.5. Прямые разложения . . . . .	147
8.6. Композиционные ряды в группах . . . . .	151
Упражнения . . . . .	155
<b>Г л а в а 9. Теорема Фробениуса. Разрешимые группы . . . . .</b>	156
9.1. Теорема Фробениуса . . . . .	156
9.2. Разрешимые группы . . . . .	158
9.3. Обобщенные силовские теоремы для разрешимых групп .	161
9.4. Дальнейшие результаты о разрешимых группах . . . . .	165
Упражнения . . . . .	169
<b>Г л а в а 10. Сверхразрешимые и нильпотентные группы . . . . .</b>	170
10.1. Определения . . . . .	170
10.2. Нижний и верхний центральные ряды . . . . .	170

10.3. Теория нильпотентных групп . . . . .	174
10.4. Подгруппа Фраттини . . . . .	177
10.5. Сверхразрешимые группы . . . . .	179
<b>Упражнения . . . . .</b>	<b>185</b>
<b>Г л а в а 11. Базисные коммутаторы . . . . .</b>	<b>186</b>
11.1. Собирательный процесс . . . . .	186
11.2. Формула Витта. Теорема о базисе . . . . .	189
<b>Г л а в а 12. Теория <math>p</math>-групп. Регулярные <math>p</math>-группы . . . . .</b>	<b>198</b>
12.1. Элементарные результаты . . . . .	198
12.2. Теорема Бернсайда о базисе. Автоморфизмы $p$ -групп . . . . .	198
12.3. Собирательная формула . . . . .	200
12.4. Регулярные $p$ -группы . . . . .	205
12.5. Некоторые специальные $p$ -группы. Группы Гамильтона . . . . .	209
<b>Г л а в а 13. Продолжение теории абелевых групп . . . . .</b>	<b>216</b>
13.1. Аддитивные группы. Группы по модулю 1 . . . . .	216
13.2 Характеры абелевых групп. Двойственность абелевых групп . . . . .	217
13.3. Полные группы . . . . .	220
13.4. Сервантные подгруппы . . . . .	221
13.5. Общие замечания . . . . .	222
<b>Г л а в а 14. Мономиальные представления и перемещение . . . . .</b>	<b>224</b>
14.1. Мономиальные подстановки . . . . .	224
14.2. Перемещение . . . . .	226
14.3. Теорема Бернсайда . . . . .	227
14.4. Теоремы Ф. Холла, Грюна и Виландта . . . . .	229
<b>Г л а в а 15. Расширения групп и когомология в группах . . . . .</b>	<b>243</b>
15.1. Композиция инвариантной подгруппы и фактор-группы . . . . .	243
15.2. Центральные расширения . . . . .	247
15.3. Циклические расширения . . . . .	249
15.4. Определяющие отношения и расширения . . . . .	251
15.5. Групповые кольца и центральные расширения . . . . .	253
15.6. Двойные модули . . . . .	260
15.7. Коцепи, кограницы и группы когомологий . . . . .	261
15.8. Применение когомологии к теории расширений . . . . .	265
<b>Г л а в а 16. Представления групп . . . . .</b>	<b>272</b>
16.1. Общие замечания . . . . .	272
16.2. Матричные представления. Характеры . . . . .	273
16.3. Теорема о полной приводимости . . . . .	276
16.4. Полупростые групповые кольца и обыкновенные представления . . . . .	281
16.5. Абсолютно неприводимые представления. Структура простых колец . . . . .	287

16.6. Соотношения между обыкновенными характерами . . . . .	293
16.7. Импрimitивные представления . . . . .	307
16.8. Некоторые применения теории характеров . . . . .	310
16.9. Унитарные и ортогональные представления . . . . .	319
16.10. Несколько примеров представлений групп . . . . .	323
<b>Г л а в а 17. Свободные произведения и свободные произведения с объединенными подгруппами . . . . .</b>	<b>336</b>
17.1. Определение свободного произведения . . . . .	336
17.2. Свободные произведения с объединенной подгруппой . .	338
17.3. Теорема Куроша . . . . .	340
<b>Г л а в а 18. Проблема Бернсайда . . . . .</b>	<b>346</b>
18.1. Постановка проблемы . . . . .	346
18.2. Проблема Бернсайда для $n = 2$ и $n = 3$ . . . . .	346
18.3. Конечность группы $B(4, r)$ . . . . .	350
18.4. Ограниченнная проблема Бернсайда. Теоремы Ф. Холла и Г. Хигмена. Конечность группы $B(6, r)$ . . . . .	352
<b>Г л а в а 19. Структуры подгрупп . . . . .</b>	<b>366</b>
19.1. Общие свойства . . . . .	366
19.2. Локально циклические группы и дистрибутивные структуры . . . . .	367
19.3. Теорема Ивасава . . . . .	369
<b>Г л а в а 20. Теория групп и проективные плоскости . . . . .</b>	<b>373</b>
20.1. Аксиомы . . . . .	373
20.2. Коллинеации и теорема Дезарга . . . . .	376
20.3. Введение координат . . . . .	381
20.4. Системы Веблена — Веддербарна. Системы Холла . . .	384
20.5. Муфанговы и дезарговы плоскости . . . . .	394
20.6. Теорема Веддербарна и теорема Артина — Цорна . . .	403
20.7. Дважды транзитивные группы и почти- поля . . . . .	410
20.8. Конечные плоскости. Теорема Брука — Райзера . . .	421
20.9. Коллинеации в конечных плоскостях . . . . .	428
<b>Литература . . . . .</b>	<b>452</b>
<b>Дополнения к литературе . . . . .</b>	<b>457</b>
<b>Указатель специальных обозначений . . . . .</b>	<b>460</b>
<b>Предметный указатель . . . . .</b>	<b>462</b>

**М. Х о л л**  
**Т Е О Р И Я Г Р У П П**

Редактор *В. В. Гольдберг*, Художник *В. П. Заикин*.

Художественный редактор *В. И. Шаповалов*.

Технический редактор *А. Д. Хомяков*. Корректор *И. П. Максимова*.

Сдано в производство 12/X 1961 г. Подписано к печати 31/V 1962 г. Бумага 60×90 $\frac{1}{16}$ =  
=14,6 бум. л., 29,2 печ. л. Уч.-издл. л. 27,9. Изд. № 1/0178. Цена 2 р. 15 к. Зак. 2888

**ИЗДАТЕЛЬСТВО ИНОСТРАННОЙ ЛИТЕРАТУРЫ**  
Москва, 1-й Рижский пер., 2

Типография № 2 им. Евг. Соколовой УПП Ленсовнархоза.

Ленинград, Измайловский пр., 29