

Министерство образования Республики Беларусь
Учреждение образования
“Гомельский государственный университет
имени Франциска Скорины”

В.С.МОНАХОВ

**ВВЕДЕНИЕ В ТЕОРИЮ КОНЕЧНЫХ ГРУПП
И ИХ КЛАССОВ**

Учебное пособие

Гомель 2003

ББК 22.144
М 77
УДК 512.542
Монахов В.С.

Введение в теорию конечных групп и их классов: Учебное пособие / В.С.Монахов. — Гомель: УО "ГГУ им. Ф.Скорины", 2003. — 108 с.

В основу данного учебного пособия положены курсы лекций по теории конечных групп, читанные автором на математическом факультете Гомельского государственного университета им. Ф.Скорины начиная с 1986/87 учебного года в рамках специализации "Алгебра и теория чисел". Здесь изложены основы теории конечных групп и основы теории классов конечных групп: формаций, классов Шунка, классов Фиттинга.

Книга состоит из пяти глав: группы и их подгруппы; гомоморфизмы и произведения групп; абелевы и нильпотентные группы; разрешимые и сверхразрешимые группы; проекторы и инъекторы.

Предназначено для студентов и аспирантов математических факультетов ВУЗов.

Библиогр.: 31 назв.

Рецензенты:

кафедра высшей алгебры Белорусского госуниверситета,
д-р физ.-мат. наук, профессор Э.М.Пальчик

Предисловие

Начало развития исследований в области теории конечных групп в Гомеле связано с приездом в 1953 году профессора Сергея Антоновича Чунихина в только что открывшийся Белорусский государственный институт инженеров железнодорожного транспорта, ныне — Белорусский государственный университет транспорта. Здесь он возглавил кафедру высшей математики, а позднее в 1959 году создал лабораторию теории конечных групп Института математики АН БССР и в 1964 году кафедру алгебры и геометрии Гомельского педагогического института, преобразованного в 1969 году в университет. В 1956 году он был избран членом-корреспондентом АН БССР, а в 1966 году — академиком АН БССР.

За время работы С.А. Чунихина в г. Гомеле в 1953–1985 гг. создана крупная научная алгебраическая школа, активно развивающаяся в настоящее время под руководством члена-корреспондента НАН Беларуси профессора Л.А. Шеметкова различные направления современной теории групп и теории классов алгебраических систем. Об этом свидетельствуют монографии участников Гомельского алгебраического семинара С.А. Чунихина [16], Л.А. Шеметкова [19], [22], А.Н. Скибы [22], [13], М.В. Селькина [12], [5], С.Ф. Каморникова [5], Го Вэньбиня [25].

К учебным изданиям по теории групп участников Гомельского алгебраического семинара следует отнести прежде всего машинописные варианты текстов лекций С.А. Чунихина [17] и Л.А. Шеметкова [21], а также учебные пособия Л.А. Шеметкова [20], В.А. Ведерникова [3], В.С. Монахова [10] и А.Н. Скибы [14].

Настоящая книга — расширенная запись лекций по теории конечных групп, читанных автором на математическом факультете Гомельского государственного университета имени Франциска Скорины начиная с 1986/87 учебного года в рамках специализации "Алгебра и теория чисел". Её цель — изложить основы теории конечных групп и основы теории классов конечных групп: формаций, классов Шунка, классов Фиттинга.

При подборке материала автор использовал методики построения текстов лекций Л.А. Шеметкова [21] и Гашюца [24], а также отдельные фрагменты монографий Хупперта [26], Робинсона [30], учебных изданий Курцвейля и Стельмахера [29] и Верфрица [31].

Более углубленное изучение теории конечных групп и их классов читатель может осуществить по монографиям и обзорным статьям, указанным в литературе.

Автор выражает искреннюю благодарность члену-корреспонденту НАН Беларуси профессору Л.А. Шеметкову и профессору В.А. Ведерникову за многочисленные полезные консультации, способствующие улучшению качества излагаемого материала. Автор также благодарен рецензентам: коллективу кафедры высшей алгебры Белорусского госуниверситета, возглавляемому профессором О.И. Тавгеном, профессору этой кафедры О.В. Мельникову, заведующему кафедрой прикладной математики Полоцкого госуниверситета профессору Э.М. Пальчику

за конструктивные замечания, и к.ф.-м.н. И.В.Близнецу за помощь в подготовке рукописи книги к изданию.

г.Гомель, апрель 2003 г.

В.Монахов

Условные обозначения

$\mathbb{N}$ — множество всех натуральных чисел.

$\mathbb{Z}$ — множество всех целых чисел.

$\mathbb{Q}$ — множество всех рациональных чисел.

$\mathbb{R}$ — множество всех действительных чисел.

$\mathbb{C}$ — множество всех комплексных чисел.

Если X — множество с нулевым элементом 0 , то $X^\# = X \setminus \{0\}$.

$\{\alpha \mid \beta\}$ — множество всех α для которых выполняется условие β .

π — некоторое множество простых чисел.

π' — дополнение к π во множестве всех простых чисел.

Пусть G — группа. Тогда:

$|G|$ — порядок группы G ;

$|x|$ — порядок элемента x группы G ;

e — единичный элемент;

E — единичная подгруппа группы G ;

$\pi(G)$ — множество всех простых делителей порядка группы G .

$\pi(n)$ — множество всех различных простых делителей натурального числа n .

π -группа — группа G , для которой $\pi(G) \subseteq \pi$.

p -группа — группа G , для которой $\pi(G) = \{p\}$.

$\Phi(G)$ — подгруппа Фраттини группы G , т.е. пересечение всех максимальных подгрупп группы G , если $G \neq E$, и $\Phi(E) = E$.

$F(G)$ — подгруппа Фиттинга группы G , т.е. произведение всех нормальных нильпотентных нормальных подгрупп группы G .

G' — коммутант группы G , т.е. подгруппа, порожденная коммутаторами всех элементов группы G .

$C_G(H)$ — централизатор подгруппы H в группе G .

$N_G(H)$ — нормализатор подгруппы H в группе G .

$Z(G)$ — центр группы G .

$O_p(G)$ — наибольшая нормальная p -подгруппа группы G .

$O_{p'}(G)$ — наибольшая нормальная p' -подгруппа группы G .

$O_\pi(G)$ — наибольшая нормальная π -подгруппа группы G .

$O_{\pi'}(G)$ — наибольшая нормальная π' -подгруппа группы G .

G_p — силовская p -подгруппа группы G .

G_π — π -холлова подгруппа группы G .

$G_{p'}$ — дополнение к силовской p -подгруппе в группе G , т.е. p' -холлова подгруппа группы G .

$G_{\pi'}$ — дополнение к π -холловой подгруппе в группе G , т.е. π' -холлова подгруппа группы G .

$\text{Aut } G$ — группа всех автоморфизмов группы G .

$\text{Inn } G$ — группа всех внутренних автоморфизмов группы G .

$n(G)$ — нильпотентная длина группы G .

$d(G)$ — производная длина группы G .

Следующая запись означает, что:

$H \leq G$ — H является подгруппой группы G ;

$H < G$ — H является собственной подгруппой группы G ;
 $M < \cdot G$ — M является максимальной подгруппой группы G ;
 $H \triangleleft G$ — H является нормальной подгруппой группы G ;
 $H \triangleleft \triangleleft G$ — H является субнормальной подгруппой группы G ;
 $H \cdot \triangleleft G$ — H является минимальной нормальной подгруппой группы G ;

$|G : H|$ — индекс подгруппы H в группе G ;
 $\pi(G : H) = \pi(|G : H|)$.

Если A и B — подгруппы группы G , то:

$A \times B$ — прямое произведение подгрупп A и B ;

$[A]B$ — полупрямое произведение нормальной подгруппы A и подгруппы B ;

$A \simeq B$ — группы A и B изоморфны.

Группу G называют:

примарной, если $|\pi(G)| \leq 1$;

бипримарной, если $|\pi(G)| = 2$.

p -группой, если $\pi(G) = \{p\}$;

p -замкнутой, если $G_p \triangleleft G$;

p -нильпотентной, если $G_{p'} \triangleleft G$;

p -разложимой, если G_p и $G_{p'}$ нормальны в G ; — π -группой, если $\pi(G) \subseteq \pi$;

π -замкнутой, если $G_\pi \triangleleft G$;

π -нильпотентной, если $G_{\pi'} \triangleleft G$;

π -разложимой, если G_π и $G_{\pi'}$ нормальны в G .

Скобки $\langle \rangle$ применяются для обозначения подгрупп, порождённых некоторым множеством элементов или подгрупп.

Если $x, y \in G$, то $[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов x и y .

Если $x \in G$, $A \subseteq G$, то $A^x = x^{-1}Ax$ — множество, сопряженное с множеством A посредством элемента x .

Классы групп обозначаются прописными готическими буквами. За некоторыми классами закреплены стандартные обозначения:

$\mathfrak{G}$ — класс всех (конечных) групп;

$\mathfrak{A}$ — класс всех абелевых групп;

$\mathfrak{N}$ — класс всех nilпотентных групп;

$\mathfrak{U}$ — класс всех сверхразрешимых групп;

$\mathfrak{S}$ — класс всех разрешимых групп.

S_n — симметрическая группа степени n ;

A_n — знакопеременная группа степени n ;

$GL(n, P)$ — полная линейная группа степени n над полем P ;

$SL(n, P)$ — специальная линейная группа степени n над полем P ;

$PGL(n, P)$ — проективная полная линейная группа степени n над полем P ;

$PSL(n, P)$ — проективная специальная линейная группа степени n над полем P ;

D_n — диэдральная группа порядка n ;

Q_8 — группа кватернионов порядка 8;

Z_n — циклическая группа порядка n .

ГЛАВА 1.

ГРУППЫ И ИХ ПОДГРУППЫ

1.1. Группы, примеры групп

Бинарной алгебраической операцией на множестве X называют отображение декартова квадрата $X \times X$ во множество X . Если $\varphi : X \times X \rightarrow X$ — бинарная операция на X , то каждой упорядоченной паре (a, b) элементов из X соответствует однозначно определенный элемент $c = \varphi(a, b)$. Бинарную операцию на X обозначают одним из символов: $+$, $\cdot$, $\oplus$, $\circ$, $\otimes$, $*$ и т.д. Если вместо φ условимся писать $\circ$, то вместо $c = \varphi(a, b)$ пишем $c = a \circ b$.

Наиболее часто используются две формы записи алгебраической операции: аддитивная и мультипликативная. При *аддитивной* записи операцию называют *сложением* и вместо $c = a \circ b$ пишут $c = a + b$. При *мультипликативной* записи операцию называют *умножением* и вместо $c = a \circ b$ пишут $c = a \cdot b$ или $c = ab$. Будем использовать мультипликативную запись.

Говорят, что на множестве X *определена* бинарная операция (умножение), если $ab \in X$ для всех $a, b \in X$.

Если $a(bc) = (ab)c$ для всех $a, b, c \in X$, то операция называется *ассоциативной*.

Если $ab = ba$ для всех $a, b \in X$, то операция называется *коммутативной*.

Элемент $e \in X$ называется *единичным*, если $ae = ea = a$ для всех $a \in X$.

Обратным к элементу a называется такой элемент a^{-1} , что $aa^{-1} = a^{-1}a = e$.

Полугруппой называется непустое множество P с бинарной алгебраической операцией (умножение), удовлетворяющей следующим требованиям:

- (1) операция определена на P , т.е. $ab \in P$ для всех a и $b \in P$;
- (2) операция ассоциативна, т.е. $a(bc) = (ab)c$ для любых $a, b, c \in P$.

ТЕОРЕМА 1.1. *В полугруппе может быть не более одного единичного элемента. Если в полугруппе имеется единичный элемент, то каждый элемент обладает не более, чем одним обратным.*

Пусть e_1 и e_2 — единичные элементы полугруппы P . Тогда $e_1e_2 = e_1$, поскольку e_2 — единичный элемент, и $e_1e_2 = e_2$, поскольку e_1 — единичный элемент. Поэтому $e_1 = e_2$.

Пусть теперь e — единичный элемент. Предположим, что a_1 и a_2 — обратные к a элементы, т.е. $a_1a = aa_1 = e = a_2a = aa_2$. Тогда $a_1 = a_1e = a_1(aa_2) = (a_1a)a_2 = ea_2 = a_2$.

ТЕОРЕМА 1.2. *В полугруппе результат применения операции к нескольким элементам не зависит от способа распределения скобок.*

Пусть $a_1, a_2, \dots, a_n$ — элементы мультипликативной полугруппы P . Не меняя порядка следования элементов, можно разными способами вычислять произведение этих элементов. Для $n \leq 4$ можно составить следующие произведения:

$$n = 1 \quad a_1;$$

$$\begin{aligned} n = 2 & \quad a_1 a_2; \\ n = 3 & \quad (a_1 a_2) a_3, \quad a_1 (a_2 a_3); \\ n = 4 & \quad ((a_1 a_2) a_3) a_4, \quad (a_1 (a_2 a_3)) a_4, \quad a_1 ((a_2 a_3) a_4), \\ & \quad a_1 (a_2 (a_3 a_4)), \quad (a_1 a_2) (a_3 a_4). \end{aligned}$$

Поскольку операция ассоциативна, то $(a_1 a_2) a_3 = a_1 (a_2 a_3)$. Для $n = 4$, используя ассоциативность, легко проверить, что все пять произведений совпадают.

Продолжим доказательство индукцией по n . Считаем, что для числа элементов $< n$ справедливость утверждения установлена. Нам нужно показать, что

$$(a_1 \dots a_k)(a_{k+1} \dots a_n) = (a_1 \dots a_l)(a_{l+1} \dots a_n) \quad < 1 >$$

при любых k и l , $1 \leq k, l \leq n - 1$. По предположению индукции внутри скобок произведения вычисляются однозначно. Пусть $k > l$. Тогда

$$\begin{aligned} & (a_1 \dots a_k)(a_{k+1} \dots a_n) = \\ & = ((a_1 \dots a_l)(a_{l+1} \dots a_k))(a_{k+1} \dots a_n) = \\ & = (a_1 \dots a_l)((a_{l+1} \dots a_k)(a_{k+1} \dots a_n)) = \\ & = (a_1 \dots a_l)(a_{l+1} \dots a_n). \end{aligned}$$

Теорема 1.2 позволяет в полугруппах использовать знак кратного умножения:

$$a_1 a_2 = \prod_{i=1}^2 a_i; \quad a_1 a_2 a_3 = \prod_{i=1}^3 a_i; \quad \dots; \quad a_1 a_2 \dots a_n = \prod_{i=1}^n a_i.$$

В частности, при $a_1 = a_2 = \dots = a_n = a$ произведение $aa \dots a$ обозначают через a^n и называют n -й степенью элемента a . Следствием теоремы 1.2 являются соотношения

$$a^n a^m = a^{n+m}; \quad (a^n)^m = a^{nm}, \quad < 2 >$$

справедливые для всех натуральных n и m . В полугруппе P с единицей e для любого $a \in P$ полагают $a^0 = e$. Заметим еще, что если $ab = ba$, то

$$(ab)^n = a^n b^n \quad \text{для всех натуральных } n, \quad < 3 >$$

что легко проверяется индукцией по n .

Группой называется непустое множество G с бинарной алгебраической операцией (умножением), удовлетворяющей следующим требованиям:

- (1) операция определена на G , т.е. $ab \in G$ для всех a и $b \in G$;
- (2) операция ассоциативна, т.е. $a(bc) = (ab)c$ для любых $a, b, c \in G$;
- (3) в G существует единичный элемент, т.е. такой элемент $e \in G$, что $ae = ea = a$ для всех $a \in G$;
- (4) каждый элемент обладает обратным, т.е. для любого $a \in G$ существует такой элемент $a^{-1} \in G$, что $aa^{-1} = a^{-1}a = e$.

Более кратко, полугруппа с единицей, в которой каждый элемент обладает обратным, называется *группой*.

Группу с коммутативной операцией называют *коммутативной* или *абелевой*. Если G — конечное множество, являющееся группой, то G называют *конечной группой*, а число $|G|$ элементов в G — *порядком группы* G .

Отметим некоторые начальные свойства групп, которые сформулируем в виде лемм. Следующее свойство вытекает из теоремы 1.1.

ЛЕММА 1.3. В группе имеется единственный единичный элемент и для каждого элемента существует единственный обратный. $\square$

ЛЕММА 1.4. $(a^{-1})^{-1} = a$ и $(ab)^{-1} = b^{-1}a^{-1}$ для любых элементов a и b группы G .

Первое равенство очевидно. Так как

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} = aea^{-1} = e, \\ (b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}a)b = b^{-1}eb = e,\end{aligned}$$

то $b^{-1}a^{-1}$ — обратный элемент для ab . Поэтому

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

Определим отрицательные целые степени элемента группы как обратные положительным степеням, т.е. положим,

$$a^{-n} = (a^n)^{-1} \quad <4>$$

для всех натуральных n .

ЛЕММА 1.5. $(a^s)^{-1} = (a^{-1})^s = a^{-s}$ для любого элемента a группы G и любого целого s .

Пусть $s > 0$. Тогда по лемме 1.4 имеем

$$(a^s)^{-1} = (a \dots a)^{-1} = a^{-1} \dots a^{-1} = (a^{-1})^s.$$

Теперь $(a^s)^{-1} = a^{-s}$ по $<4>$.

Если $s = 0$, то

$$(a^s)^{-1} = e = (a^{-1})^s = a^{-s}.$$

Если $s < 0$, то

$$(a^s)^{-1} = ((a^{-1})^{|s|})^{-1} = ((a^{|s|})^{-1})^{-1} = a^{|s|} = a^{-s}$$

и

$$(a^{-1})^s = (a^{-1})^{-|s|} = ((a^{-1})^{|s|})^{-1} = ((a^{|s|})^{-1})^{-1} = a^{|s|} = a^{-s}.$$

ЛЕММА 1.6. Для любых целых s и t и любого элемента a группы G справедливы равенства:

$$a^s a^t = a^{s+t}; \quad (a^s)^t = a^{st}.$$

Для натуральных показателей эти равенства уже получены в $<2>$. Если один из показателей нуль, то равенства также справедливы. Пусть s и t — отрицательные. Тогда используя леммы 1.5 и 1.4 и равенства $<2>$ получаем, что

$$\begin{aligned}a^s a^t &= a^{-|s|} a^{-|t|} = (a^{-1})^{|s|} (a^{-1})^{|t|} = (a^{-1})^{|s|+|t|} = a^{s+t}; \\ (a^s)^t &= (a^{-|s|})^t = ((a^{|s|})^{-1})^t = (a^{|s|})^{-t} = (a^{|s|})^{|t|} = a^{|s||t|} = a^{st}.\end{aligned}$$

Если $s < 0$, $t > 0$, то

$$a^s a^t = a^{-|s|} a^t = \underbrace{a^{-1} \dots a^{-1}}_{|s|} \underbrace{a \dots a}_t = a^{t-|s|}$$

(или $a^{|s|-t}$, если $|s| \geq t$) $= a^{t+s}$;

$$(a^s)^t = \underbrace{a^s \dots a^s}_t = \underbrace{a^{-1} \dots a^{-1}}_{|s|} \dots \underbrace{a^{-1} \dots a^{-1}}_{|s|} = (a^{-1})^{|s|t} = a^{st};$$

Случай $s > 0, t < 0$ проверяется аналогично.

ЛЕММА 1.7. В группе G уравнения $ax = b$ и $yc = d$ имеют единственные решения $x = a^{-1}b$ и $y = dc^{-1}$.

Так как

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

то $a^{-1}b$ — решение уравнения $ax = b$. Если t — произвольное решение уравнения $ax = b$, то

$$t = et = (a^{-1}a)t = a^{-1}(at) = a^{-1}b.$$

Аналогично проводятся рассуждения для уравнения $yc = d$.

ТЕОРЕМА 1.8. Полугруппа P является группой тогда и только тогда, когда уравнения $ax = b, ya = b$ имеют решения для любых элементов $a, b \in P$.

Если P — группа, то по лемме 1.7 уравнения $ax = b, ya = b$ имеют решения для любых $a, b \in P$.

Обратно, пусть P — полугруппа и уравнения $ax = b, ya = b$ имеют решения для всех a и $b \in P$. Зафиксируем элемент $c \in P$ и обозначим через x_c решение уравнения $cx = c$. Пусть g — произвольный элемент из P и пусть y^* — решение уравнения $yc = g$. Умножив обе части равенства $cx_c = c$ слева на y^* , получим: $y^*cx_c = y^*c$ или $gx_c = g$. Таким образом, $gx_c = g$ для всех $g \in P$.

Решение уравнения $gx = x_c$ обозначим через g^{-1} . Итак $gg^{-1} = x_c$ для всех $g \in P$.

Пусть a — произвольный элемент из P и пусть $x_ca = b$. Умножим обе части равенства на a^{-1} справа. Имеем: $x_caa^{-1} = ba^{-1}$ или $x_cx_c = ba^{-1}$. Но $x_cx_c = x_c$, поэтому $x_c = ba^{-1}$. Так как $aa^{-1} = x_c$, то $aa^{-1} = ba^{-1}$. Через t обозначим решение уравнения $a^{-1}x = x_c$, т.е. $a^{-1}t = x_c$. Умножив обе части уравнения $aa^{-1} = ba^{-1}$ справа на t , получим:

$$aa^{-1}t = ax_c = a = ba^{-1}t = bx_c = b,$$

т.е. $a = b$ и x_c — единичный элемент полугруппы P . По теореме 1.1 единичный элемент в P единственный.

Допустим, что $g^{-1}g = f$, где g и $f \in P$. Умножив обе части равенства справа на g^{-1} получим: $g^{-1}gg^{-1} = fg^{-1}$ или $g^{-1}x_c = g^{-1} = fg^{-1}$. Так как в P единичный элемент единственный, то $f = x_c$ и g^{-1} — обратный элемент к элементу g в полугруппе P . Поэтому P — группа.

Теорема 1.8 позволяет ввести следующее определение группы, эквивалентное исходному.

Группой называется непустое множество G с бинарной алгебраической операцией (умножением), удовлетворяющей следующим требованиям:

- (1) операция определена на G ;
- (2) операция ассоциативна;
- (3) уравнения $ax = b, ya = b$ имеют решения для любых элементов $a, b \in G$.

Говорят, что элемент a группы G сопряжен с элементом b посредством элемента x , если $a = x^{-1}bx$. Вместо $x^{-1}bx$ удобнее писать b^x . Через $a^G = \{a^x \mid x \in G\}$ обозначим совокупность всех элементов группы G , сопряженных с элементом a , и назовём *классом сопряженных элементов*. Ясно, что в абелевой группе каждый класс сопряженных элементов состоит из одного элемента, т.е. если группа G абелева, то $a^G = \{a\}$ для всех $a \in G$.

ЛЕММА 1.9. Пусть $a, b, x, y \in G$. Тогда:

$$(1) a^{xy} = (a^x)^y;$$

$$(2) (ab)^x = a^x b^x;$$

$$(3) (a^x)^{-1} = (a^{-1})^x;$$

$$(4) (a^x)^k = (a^k)^x \text{ для любого целого } k;$$

(5) два класса сопряженных элементов либо совпадают, либо их пересечение пусто;

(6) группа является объединением непересекающихся классов сопряженных элементов.

Утверждения (1–4) очевидны.

(5) Пусть $a^G \cap b^G \neq \emptyset$; $d \in a^G \cap b^G$. Тогда $d = a^x = b^y$ для некоторых $x, y \in G$. Поэтому

$$x^{-1}ax = y^{-1}by; \quad a = xy^{-1}byx^{-1} = b^{yx^{-1}} \in b^G.$$

Если $c = a^z \in a^G$, то $c = b^{yx^{-1}z} \in b^G$ и $a^G \subseteq b^G$. Аналогично проверяется, что $b^G \subseteq a^G$, поэтому $a^G = b^G$.

(6) Так как $a = a^e \in a^G$, то каждый элемент группы G принадлежит некоторому классу сопряженных элементов и ввиду (5) группа распадается на непересекающиеся классы сопряженных элементов.

Все приведенные определения и полученные результаты легко переносятся с соответствующим изменением терминологии как указано далее в таблице на множества с аддитивной записью операции. Аддитивная запись используется, как правило, для абелевых групп и крайне редко — для неабелевых. Связь между аддитивной и мультипликативной записями операций представлена в следующей таблице.

Мультипликативная запись операции	Аддитивная запись операции
умножение	сложение
произведение ab $\prod_{i=1}^n a_i = a_1 a_2 \dots$ $\dots a_n$	сумма $a + b$ $\sum_{i=1}^n a_i = a_1 + a_2 + \dots$ $\dots + a_n$
единичный элемент e $ae = ea = a$	нулевой элемент 0 $a + 0 = 0 + a = a$
обратный элемент a^{-1} $aa^{-1} = a^{-1}a = e$	противоположный элемент $-a$ $a + (-a) = -a + a = 0$
ассоциативность $(ab)c = a(bc)$	ассоциативность $(a + b) + c = a + (b + c)$
коммутативность $ab = ba$	коммутативность $a + b = b + a$
степень a^n при $n > 0$ $a^n = \underbrace{a \dots a}_{n \text{ раз}}$	кратное na при $n > 0$ $na = \underbrace{a + \dots + a}_{n \text{ раз}}$
степень a^n при $n < 0$ $a^n = \underbrace{a^{-1} \dots a^{-1}}_{-n \text{ раз}}$	кратное na при $n < 0$ $na = \underbrace{(-a) + \dots + (-a)}_{-n \text{ раз}} =$
$a^n = e$ при $n = 0$	$na = 0$ при $n = 0$
$a^n a^m = a^{n+m}$	$na + ma = (n + m)a$
$(a^n)^m = a^{nm}$	$m(na) = (mn)a$
$(ab)^n = a^n b^n$, если $ab = ba$	$n(a + b) = na + nb$, если $a + b = b + a$

Нам потребуются следующие стандартные обозначения:

$\mathbb{N}$ — множество всех натуральных чисел;

$\mathbb{Z}$ — множество всех целых чисел;

$\mathbb{Q}$ — множество всех рациональных чисел;

$\mathbb{R}$ — множество всех действительных чисел;

$\mathbb{C}$ — множество всех комплексных чисел.

Эти обозначения будут использоваться в примерах и везде далее.

ПРИМЕР 1.1. ЧИСЛОВЫЕ ГРУППЫ.

(a) Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с операцией сложения — абелевы группы. Все требования определения группы проверяются без труда. $\square$

(b) Множество $\mathbb{N}$ со сложением не является группой, так как в $\mathbb{N}$ нет нулевого элемента и противоположных. Однако $\mathbb{N}$ со сложением — полугруппа. $\square$

(c) Ни одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с умножением группу не образует. Если положим $\mathbb{R}^\# = \mathbb{R} \setminus \{0\}$, $\mathbb{Q}^\# = \mathbb{Q} \setminus \{0\}$, $\mathbb{C}^\# = \mathbb{C} \setminus \{0\}$, то $\mathbb{R}^\#$, $\mathbb{Q}^\#$ и $\mathbb{C}^\#$ с умножением являются абелевыми группами. $\mathbb{Z}^\# = \mathbb{Z} \setminus \{0\}$ и $\mathbb{N}$ с умножением полугруппы, но не группы. $\square$

(d) Множество $\{-1, 1\}$ с умножением — конечная абелева группа порядка 2. $\square$

ПРИМЕР 1.2. МАТРИЧНЫЕ ГРУППЫ.

(a) Пусть P — некоторое поле. Через $M(n, P)$ обозначим совокупность всех квадратных $n \times n$ -матриц с элементами из P . Ясно, что $M(n, P)$ с операцией умножения матриц — полугруппа с единичной матрицей в качестве единичного элемента. Так как только невырожденные матрицы обладают обратными, то $M(n, P)$ не является группой. $\square$

(b) Пусть $GL(n, P) = \{A \in M(n, P) \mid \det A \neq 0\}$. Тогда $GL(n, P)$ — группа, которую называют *полной* или *общей линейной группой степени n над P* . $\square$

(c) $SL(n, P) = \{A \in GL(n, P) \mid \det A = 1\}$ — группа, которая называется *специальной линейной группой степени n над P* . $\square$

ПРИМЕР 1.3. ГРУППЫ ПЕРЕСТАНОВОК.

(a) Пусть $X = \{1, 2, \dots, n\}$. Взаимно однозначное отображение множества X на себя называется *перестановкой степени n* . Совокупность всех перестановок степени n обозначают через S_n . Перестановку $\tau \in S_n$ удобно изображать двустрочной таблицей, полностью указывая образы всех элементов:

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$$

или

$$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix},$$

где $\{a_1, a_2, \dots, a_n\} = X$; $\tau : 1 \mapsto a_1, \dots, n \mapsto a_n$.

Тождественное преобразование ε_X является взаимно однозначным отображением и поэтому $\varepsilon_X \in S_n$. Очевидно, что

$$\varepsilon = \varepsilon_X = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Произведение $\delta\tau$ двух перестановок δ и τ находится как произведение отображений:

$$\delta\tau(k) = \delta(\tau(k)), \quad k = 1, 2, \dots, n.$$

Легко проверить, что множество S_n всех перестановок степени n с операцией умножения перестановок образует конечную группу порядка $n!$ с единичным элементом

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix},$$

которую называют *симметрической группой степени n* . При $n \geq 3$ эта группа неабелева. $\square$

(b) Четные перестановки образуют конечную группу A_n порядка $n!/2$, которую называют *знакопеременной группой степени n* . При $n \geq 4$ эта группа неабелева. $\square$

ПРИМЕР 1.4. ГРУППЫ ФУНКЦИЙ.

(a) Проверим, что четыре функции $f_1(x) = x$, $f_2(x) = -x$, $f_3(x) = \frac{1}{x}$, $f_4(x) = -\frac{1}{x}$ с операцией умножения образуют группу. Составим таблицу умножения этих функций.

	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

Произведение $f_i f_j$ ставится на пересечении строки f_i и столбца f_j . Например,

$$f_2 f_3 : x \xrightarrow{f_3} \frac{1}{x} \xrightarrow{f_2} -\frac{1}{x},$$

поэтому $f_2 f_3 = f_4$.

Из таблицы видно, что умножение определено на множестве $\{f_1, f_2, f_3, f_4\}$ и коммутативно. Поскольку умножение отображений ассоциативно, то выполняется второе требование определения группы. Функция f_1 является единичным элементом, а $f_i^{-1} = f_i$, т.е. каждый элемент является для себя обратным элементом. Таким образом, множество $\{f_1, f_2, f_3, f_4\}$ с умножением является конечной абелевой группой порядка 4. $\square$

(b) *Аффинным преобразованием прямой* называется отображение

$$\varphi_{a,b} : x \mapsto ax + b, \quad a, b \in \mathbb{R}, \quad a \neq 0$$

множества $\mathbb{R}$ в $\mathbb{R}$. Совокупность всех аффинных преобразований прямой обозначается через $A_1(\mathbb{R})$. В соответствии с умножением отображений аффинные преобразования прямой перемножаются так:

$$\varphi_{a,b} \varphi_{c,d} : x \mapsto cx + d \mapsto c(ax + b) + d = acx + (bc + d)$$

и $\varphi_{a,b} \varphi_{c,d} = \varphi_{ac, bc+d}$. Поэтому $A_1(\mathbb{R})$ является неабелевой группой с единичным элементом $\varphi_{1,0}$ и обратным элементом $\varphi_{a^{-1}, -a^{-1}b}$ для элемента $\varphi_{a,b}$. $\square$

ПРИМЕР 1.5. Перечислим все классы сопряженных элементов группы S_3 .

$$S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}.$$

Вычислим $(12)^x$, где x пробегает элементы из S_3 . Ясно, что

$$(12)^\varepsilon = (12)^{(12)} = (12).$$

Далее

$$(12)^{(13)} = (13)^{-1}(12)(13) = (31)(12)(13) = (23);$$

$$(12)^{(23)} = (32)(12)(23) = (13);$$

$$(12)^{(123)} = (321)(12)(123) = (13);$$

$$(12)^{(132)} = (231)(12)(132) = (23).$$

$$\text{Итак, } (12)^{S_3} = \{(12), (23), (13)\}.$$

Вычислив x^y для всех x и y из S_3 , получаем, что в S_3 имеется три класса сопряженных элементов:

$$\varepsilon^{S_3} = \{\varepsilon\};$$

$$(12)^{S_3} = (13)^{S_3} = (23)^{S_3} = \{(12), (13), (23)\};$$

$$(123)^{S_3} = (132)^{S_3} = \{(123), (132)\}.$$

$$\text{Поэтому } S_3 = \varepsilon^{S_3} \cup (12)^{S_3} \cup (123)^{S_3}. \quad \square$$

ТЕОРЕМА 1.10. Две перестановки сопряжены в S_n тогда и только тогда, когда они имеют одинаковое число независимых циклов каждой длины.

Пусть

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

— разложение перестановки τ на независимые циклы, и пусть π — произвольная перестановка из S_n . Мы можем перестановку записать следующим образом:

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

Тогда для произвольного b_{ik} имеем:

$$\pi^{-1}\tau\pi : b_{ik} \xrightarrow{\pi} a_{ik} \xrightarrow{\tau} \begin{cases} a_{ik+1} \xrightarrow{\pi^{-1}} b_{ik+1} \\ a_{i1} \xrightarrow{\pi^{-1}} b_{i1} \end{cases}.$$

Поэтому

$$\pi^{-1}\tau\pi = (b_{11} \dots b_{1r})(b_{21} \dots b_{2s}) \dots (b_{m1} \dots b_{mt}),$$

т.е. сопряженные перестановки имеют одинаковое число циклов каждой длины.

Обратно, если перестановки

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

и

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

имеют одинаковое число циклов каждой длины, то

$$\alpha = \begin{pmatrix} d_{11} & \dots & d_{1r} & d_{21} & \dots & d_{2s} & \dots & d_{m1} & \dots & d_{mt} \\ c_{11} & \dots & c_{1r} & c_{21} & \dots & c_{2s} & \dots & c_{m1} & \dots & c_{mt} \end{pmatrix}$$

— такая перестановка, что $\alpha^{-1}\sigma\alpha = \delta$. Таким образом, перестановки δ и σ с одинаковым числом циклов каждой длины сопряжены.

ПРИМЕР 1.6. Рассмотрим симметрическую группу степени 4. Запись $(...)(.)$ обозначает любую перестановку в S_4 , разлагающуюся на циклы длины 3 и 1. В S_4 возможны следующие разложения:

$$(.)(.)(.)(.); (.)(.)(.); (.)(...); (..)(.); (....).$$

На основании теоремы 1.15 группа S_4 имеет пять классов сопряженных элементов. $\square$

1.2. Подгруппы

Среди непустых подмножеств множества G некоторые могут быть группами. Подмножество H группы G называется *подгруппой*, если H — группа относительно той же операции, которая определена на группе G . Для подгруппы используется следующее обозначение: $H \leq G$. Запись $H \leq G$ читается так: H — подгруппа группы G .

ТЕОРЕМА 1.11. (КРИТЕРИЙ ПОДГРУППЫ) *Непустое подмножество H группы G будет подгруппой тогда и только тогда, когда $h_1h_2 \in H$ и $h_1^{-1} \in H$ для всех $h_1, h_2 \in H$.*

Пусть H — подгруппа группы G , т. е. H — группа относительно той же операции, которая определена на группе G . На H определена алгебраическая операция, поэтому $h_1h_2 \in H$ для всех $h_1, h_2 \in H$.

Проверим, что единица e_1 подгруппы H совпадает с единицей e группы G . Ясно, что $e_1e = ee_1 = e_1$, т.к. e_1 — элемент из G . В группе G для e_1 имеется обратный элемент e_1^{-1} , то есть $e_1^{-1}e_1 = e_1e_1^{-1} = e$. Так как e_1 — единица в H , то $e_1e_1 = e_1$. Умножив обе части последнего равенства на e_1^{-1} , получим: $e_1^{-1}e_1e_1 = e_1^{-1}e_1$ или $ee_1 = e$, поэтому $e_1 = e$. Таким образом, единицы подгруппы H и группы G совпадают.

Так как H — подгруппа, то для каждого $h \in H$ существует в подгруппе H обратный элемент h^{-1} , то есть такой элемент, что $h^{-1}h = hh^{-1} = e_1 = e$. Это означает, что h^{-1} является обратным элементом в группе G для элемента $h \in H$.

Обратно, пусть $h_1h_2 \in H$ и $h_1^{-1} \in H$ для всех $h_1, h_2 \in H$. Тогда алгебраическая операция определена на H . Она ассоциативна в H , так как ассоциативность справедлива для всех элементов из G . Элемент h^{-1} обратный к $h \in H$ также принадлежит H , поэтому $h^{-1}h \in H$ и $hh^{-1} \in H$. Поскольку $h^{-1}h = e = hh^{-1}$, то $e \in H$ и H — группа.

Отметим, что каждая группа G обладает *единичной подгруппой* $E = \{e\}$. Сама группа G также считается подгруппой в G . Эти подгруппы называют *тривиальными подгруппами*. *Нетривиальная подгруппа* группы G это такая подгруппа H из G , которая отлична от G и отлична от единичной подгруппы E . *Собственной* называется подгруппа, отличная от группы. Очевидна следующая

ЛЕММА 1.12. (1) *Если H — подгруппа группы G и K — подгруппа в H , то K — подгруппа группы G ;*

(2) если H и K — подгруппы группы G и H содержится в K , то H — подгруппа в K . $\square$

Пусть T — подмножество группы G и $x \in G$. Через

$$T^x = \{x^{-1}tx \mid t \in T\}$$

обозначим подмножество всех элементов группы G вида $x^{-1}tx = t^x$, где t пробегает все элементы множества T . Подмножество T^x называется подмножеством, *сопряженным* подмножеству T посредством элемента x .

ЛЕММА 1.13. Если H — подгруппа группы G , то H^x — также подгруппа группы G для любого $x \in G$.

Воспользуемся критерием подгруппы. Пусть $t_1, t_2 \in H^x$. Тогда существуют элементы $h_1, h_2 \in H$ такие, что $t_1 = h_1^x, t_2 = h_2^x$. Поэтому

$$t_1 t_2 = h_1^x h_2^x = (h_1 h_2)^x \in H^x,$$

т.к. $h_1 h_2 \in H$. Кроме того,

$$t_1^{-1} = (x^{-1} h_1 x)^{-1} = x^{-1} h_1^{-1} x \in H^x,$$

т.к. $h_1^{-1} \in H$. Условия теоремы 2.1 выполняются, поэтому H^x — подгруппа группы G .

Подгруппа H^x называется подгруппой, *сопряженной* подгруппе H посредством элемента x .

ЛЕММА 1.14. Пересечение любого непустого семейства подгрупп группы является подгруппой.

Пусть $D = \bigcap_{\alpha \in I} H_\alpha$, где H_α — подгруппа группы G для любого $\alpha \in I$ и I — некоторое множество индексов. Если d_1 и $d_2 \in D$, то d_1 и $d_2 \in H_\alpha$ для всех $\alpha \in I$. Поэтому $d_1 d_2 \in H_\alpha$ и $d_1 d_2 \in D$. Если $d \in D$, то $d \in H_\alpha$ и $d^{-1} \in H_\alpha$ для всех $\alpha \in I$. Поэтому $d^{-1} \in D$ и D — подгруппа группы G по теореме 2.1.

Пересечение пустого семейства подгрупп группы G будем считать равным G .

Подгруппа, порожденная множеством. Пусть T — подмножество группы G . Пересечение всех подгрупп группы G , содержащих подмножество T , называется *подгруппой, порожденной подмножеством T* , и обозначается через $\langle T \rangle$. Таким образом,

$$\langle T \rangle = \bigcap_{T \subseteq H \leq G} H.$$

Из этого определения вытекает равенство $\langle \emptyset \rangle = E$ — единичная подгруппа группы G , а также следующее утверждение.

ЛЕММА 1.15. Подгруппа, порожденная непустым множеством T , является наименьшей подгруппой, содержащей множество T . $\square$

Условимся через T^{-1} обозначать множество всех обратных элементов к элементам из T , т.е.

$$T^{-1} = \{t^{-1} \mid t \in T\}.$$

ТЕОРЕМА 1.16. Пусть T — непустое подмножество группы G . Тогда подгруппа $\langle T \rangle$, порожденная подмножеством T , состоит из всех конечных произведений элементов из T и их обратных элементов, т.е.

$$\langle T \rangle = \{t_1 \cdots t_n \mid t_i \in \{T \cup T^{-1}\}, n \in \mathbb{N}\}.$$

Пусть

$$F = \{t_1 \cdots t_n \mid t_i \in \{T \cup T^{-1}\}, n \in \mathbb{N}\}$$

и пусть $u, v \in F$. Тогда

$$u = t_1 \cdots t_n, v = h_1 \cdots h_k, t_i, h_j \in \{T \cup T^{-1}\}, n, k \in \mathbb{N}.$$

Поэтому

$$uv = t_1 \cdots t_n h_1 \cdots h_k$$

также является конечным произведением элементов из $\{T \cup T^{-1}\}$. Кроме того,

$$u^{-1} = (t_1 \cdots t_n)^{-1} = t_n^{-1} \cdots t_1^{-1} \in F,$$

т.к. $t_i^{-1} \in \{T \cup T^{-1}\}$. Требования критерия подгруппы выполняются, поэтому F — подгруппа.

По определению

$$\langle T \rangle = \bigcap_{T \subseteq H \leq G} H.$$

Если H — подгруппа и $T \subseteq H$, то по критерию подгруппы $T^{-1} \subseteq H$ и $F \subseteq H$. Поэтому $F \subseteq \langle T \rangle$.

Подгруппа F содержит подмножество T , поэтому F встречается среди подгрупп, участвующих в пересечении

$$\langle T \rangle = \bigcap_{T \subseteq H \leq G} H.$$

Следовательно, $\langle T \rangle \subseteq F$. Таким образом, $\langle T \rangle = F$.

Решетка подгрупп. Пусть $\mathbf{S}(G)$ обозначает множество всех подгрупп группы G с бинарным отношением $\leq$. Две подгруппы A и $B \in \mathbf{S}(G)$ группы G находятся в бинарном отношении $\leq$ тогда и только тогда, когда A — подгруппа в B . Ясно, что отношение $\leq$ рефлексивно, антисимметрично и транзитивно. Поэтому $\mathbf{S}(G)$ — частично упорядоченное множество с наименьшим элементом E и наибольшим элементом G .

Напомним, что *решеткой* называется частично упорядоченное множество, в котором каждое двухэлементное подмножество обладает как точной верхней, так и точной нижней гранью.

Для каждой пары $\{A, B\}$ подгрупп пересечение $A \cap B$ будет наибольшей подгруппой, содержащейся в A и в B . Поэтому $A \cap B$ — точная нижняя грань двухэлементного множества $\{A, B\}$, т.е. $A \cap B = A \wedge B$. Из следствия 2.6 получаем, что $\langle A \cup B \rangle$ будет точной верхней гранью множества $\{A, B\}$, т.е. $A \vee B = \langle A \cup B \rangle$. Таким образом, доказана

ТЕОРЕМА 1.17. *Множество $\mathbf{S}(G)$ всех подгрупп группы G с бинарным отношением $\leq$ является решеткой.* $\square$

Централизатор. Пусть T — непустое подмножество группы G . Совокупность всех элементов группы G , перестановочных с каждым элементом множества T , называется *централизатором* множества T в группе G и обозначается через $C_G(T)$. Таким образом,

$$C_G(T) = \{x \in G \mid xt = tx \text{ для всех } t \in T\}.$$

ЛЕММА 1.18. (1) Если T — подмножество группы G , то централизатор $C_G(T)$ является подгруппой группы G .

(2) Если S и T — подмножества группы G и $S \subseteq T$, то $C_G(T) \subseteq C_G(S)$.

(3) Если T — подмножество группы G и $x \in G$, то $C_G(T^x) = C_G(T)^x$.

(1) Пусть x и $y \in C_G(T)$. Тогда для любого элемента $t \in T$ получаем, что $xt = tx$, $yt = ty$. Поэтому

$$xyt = xty = txy, \quad xy \in C_G(T).$$

Умножив обе части равенства $xt = tx$ на x^{-1} слева, получим:

$$t = x^{-1}tx, \quad tx^{-1} = x^{-1}t, \quad x^{-1} \in C_G(T).$$

По критерию подгруппы централизатор $C_G(T)$ является подгруппой группы G .

(2) Если $x \in C_G(T)$, то x перестановочен со всеми элементами из T , а так как $S \subseteq T$, то x будет перестановочен со всеми элементами из S . Поэтому $x \in C_G(S)$ и $C_G(T) \subseteq C_G(S)$.

(3) Если $g \in C_G(T^x)$, то $gt^x = t^xg$ для всех $t \in T$. Так как

$$gt^x = gx^{-1}tx = t^xg = x^{-1}txg,$$

то

$$xgx^{-1}t = txgx^{-1}, \quad xgx^{-1} \in C_G(T).$$

Поэтому $g \in C_G(T)^x$ и

$$C_G(T^x) \subseteq C_G(T)^x.$$

Аналогично проверяется обратное включение.

Центр группы. Центром группы G называется совокупность всех элементов группы G , перестановочных с каждым элементом группы G . Центр группы G обозначается через $Z(G)$. Ясно, что $Z(G) = C_G(G)$, т.е. центр группы G совпадает с централизатором подмножества G в группе G . Кроме того,

$$Z(G) = \bigcap_{g \in G} C_G(g).$$

ЛЕММА 1.19. Для группы G справедливы следующие утверждения:

(1) если $a \in Z(G)$, то класс сопряженных с a элементов состоит из одного элемента a , т.е. $a^G = \{a\}$; обратно, если $a^G = \{a\}$, то $a \in Z(G)$;

(2) $Z(G)^x = Z(G)$ для всех $x \in G$;

(3) центр $Z(G)$ группы G является абелевой подгруппой группы G ;

(4) группа G абелева тогда и только тогда, когда она совпадает со своим центром;

(5) если H — подгруппа группы G , то

$$C_G(H) \cap H = Z(H);$$

(6) если $x \in G$, то $\langle Z(G), x \rangle$ — абелева подгруппа.

(1) Если $a \in Z(G)$, то $a^G = \{a^x | x \in G\} = \{a\}$, т.к. $a^x = x^{-1}ax = x^{-1}xa = a$. Обратно, если $a^G = \{a\}$, то $a^x = a$ для всех $x \in G$ и $a \in Z(G)$;

(2) Так как $Z(G) = C_G(G)$, то

$$Z(G)^x = C_G(G)^x = C_G(G^x) = C_G(G) = Z(G)$$

для всех $x \in G$. Здесь использовали лемму 2.8(3).

(3) По лемме 2.8 множество $Z(G) = C_G(G)$ является подгруппой. Если x и $y \in Z(G)$, то $xg = gx$, $yg = gy$ для всех элементов $g \in G$. В частности, $xy = yx$ и $Z(G)$ абелева.

(4) Если G абелева, то каждый элемент группы G перестановочен со всеми элементами группы G , поэтому $G = Z(G)$. Обратно, если $G = Z(G)$, то из (1) следует, что G абелева.

(5) Пусть H — подгруппа группы G . Если $z \in Z(H)$, то $zh = hz$ для всех $h \in H$, поэтому $z \in C_G(H)$ и

$$Z(H) \subseteq H \cap C_G(H).$$

Обратно, если

$$c \in H \cap C_G(H),$$

то $ch = hc$ для всех $h \in H$ и $c \in Z(H)$, т.е.

$$H \cap C_G(H) \subseteq Z(H).$$

Таким образом,

$$Z(H) = H \cap C_G(H).$$

(6) Пусть x — произвольный элемент группы G и $H = \langle Z(G), x \rangle$ — подгруппа, порожденная подмножеством $S = Z(G) \cup \{x\}$. Ясно, что любые два элемента s и t подмножества S перестановочны. Поэтому перестановочны элементы s^{-1} и t^{-1} . Теперь по теореме 2.5 подгруппа H абелева.

ПРИМЕР 1.7. (а) В примере 1.1(а) показано, что с операцией сложения множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ и $\mathbb{C}$ являются группами. Поэтому

$$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}.$$

Так как эти группы абелевы, то они совпадают со своими центрами. $\square$

(б) В примере 1.1(с–d) показано, что с операцией умножения следующие множества являются группами: $\mathbb{Q}^\#, \mathbb{R}^\#, \mathbb{C}^\#, \{-1, 1\}$. Поэтому

$$\{-1, 1\} \leq \mathbb{Q}^\# \leq \mathbb{R}^\# \leq \mathbb{C}^\#.$$

Так как эти группы абелевы, то они совпадают со своими центрами. $\square$

ПРИМЕР 1.8. В примере 1.2 показано, что $GL(n, P)$ и $SL(n, P)$ — группы, где P — некоторое поле. Поэтому $SL(n, P) \leq GL(n, P)$. $\square$

ПРИМЕР 1.9. В примере 1.3 показано, что совокупность S_n всех перестановок степени n и совокупность A_n всех четных перестановок с операцией умножения перестановок являются группами. Поэтому $A_n \leq S_n$. Можно показать, что при $n \geq 4$ центры этих групп являются единичными подгруппами. $\square$

1.3. Циклические группы

Зафиксируем элемент a в группе G . Пересечение всех подгрупп группы G , содержащих элемент a , назовем *циклической подгруппой, порожденной*

элементом a , и обозначим через $\langle a \rangle$. Таким образом,

$$\langle a \rangle = \bigcap_{a \in H \leq G} H.$$

Из теоремы 2.5 в случае $T = \{a\}$ вытекает

ТЕОРЕМА 1.20. *Циклическая подгруппа $\langle a \rangle$, порождённая элементом a , состоит из всевозможных целых степеней элемента a , т.е. $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.* $\square$

СЛЕДСТВИЕ. *Циклическая подгруппа абелева.*

Пусть G — группа, $\langle a \rangle$ — циклическая подгруппа, порождённая элементом $a \in G$, и x, y — произвольные элементы подгруппы $\langle a \rangle$. Тогда по теореме 3.1 $x = a^n$, $y = a^m$ для некоторых целых чисел n, m и

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx,$$

т.е. подгруппа $\langle a \rangle$ абелева.

Порядок элемента. Для элемента $a \in G$ имеются следующие две возможности.

Все степени элемента a различны, т.е. $a^m \neq a^n$ для целых $m \neq n$. В этом случае говорят, что элемент a имеет *бесконечный порядок*.

Имеются совпадения $a^m = a^n$ при $m \neq n$. Если, например, $m > n$, то $m - n > 0$ и $a^{m-n} = e$, т.е. существуют натуральные степени элемента a , равные единичному элементу. Наименьшее натуральное число k , при котором $a^k = e$, называют *порядком* элемента a и пишут $|a| = k$.

Ясно, что в любой группе единичный элемент e имеет порядок 1. Других элементов порядка 1 в группе нет. В конечной группе все элементы, очевидно, имеют конечные порядки.

Следующая теорема показывает, что циклическая подгруппа, порождённая элементом конечного порядка k , состоит точно из k элементов.

ТЕОРЕМА 1.21. *Пусть элемент $a \in G$ имеет конечный порядок k . Тогда $\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}$ и $a^m = e$ тогда и только тогда, когда $m = kq$, где q — целое число.*

По теореме 3.1 циклическая подгруппа

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$$

состоит из всевозможных степеней a^m , где m пробегает все целые числа. Любое целое число m можно представить в виде

$$m = kq + r, \quad 0 \leq r \leq k-1.$$

Поэтому

$$a^m = a^{kq+r} = a^{kq} a^r = (a^k)^q a^r = a^r$$

и

$$\langle a \rangle \subseteq \{e, a, \dots, a^{k-1}\}.$$

Обратное включение очевидно, значит,

$$\langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}.$$

Так как $a^m = a^r$, то $a^m = e$ лишь при $r = 0$, т.е. тогда $m = kq$.

Если группа G совпадает с одной из своих циклических подгрупп, то группу G называют *циклической группой*. В этом случае в группе G име-

ется элемент a такой, что $G = \langle a \rangle$ и по теореме 3.1 все элементы в группе G являются целыми степенями элемента a :

$$G = \langle a \rangle = \{a^m \mid m \in \mathbb{Z}\} = \{\dots, a^{-2}, a^{-1}, a^0 = e, a, a^2, \dots\}.$$

Если элемент a имеет бесконечный порядок, то все эти элементы в группе G попарно различны и G — *бесконечная циклическая группа*.

Если элемент a имеет конечный порядок k , то $G = \langle a \rangle = \{e, a, \dots, a^{k-1}\}$ по теореме 3.3, т.е. циклическая группа G , порожденная элементом a порядка k , состоит из k элементов. В этом случае G — *конечная циклическая группа порядка k* .

Подгруппы циклических групп.

ТЕОРЕМА 1.22. *Все подгруппы бесконечной циклической группы $G = \langle a \rangle$ исчерпываются единичной подгруппой $E = \{e\}$ и бесконечными циклическими подгруппами $\langle a^m \rangle$ для каждого натурального m .*

Пусть H — произвольная подгруппа бесконечной циклической группы $G = \langle a \rangle$. Тогда $e \in H$ и если других элементов в H нет, то $H = \{e\}$ — единичная подгруппа.

Пусть $a^t \in H$, $a^t \neq e$. Тогда обратный элемент a^{-t} также принадлежит H и можно выбрать в H элемент a^m с наименьшим натуральным показателем m . Если a^n — произвольный элемент из H , то

$$n = mq + r, \quad 0 \leq r < m$$

и

$$a^r = a^{n-mq} = a^n a^{-mq} = a^n ((a^m)^q)^{-1} \in H.$$

По выбору m заключаем, что $r = 0$ и n кратно m . Таким образом, $H \subseteq \langle a^m \rangle$. Так как H — подгруппа, то выполняется и обратное включение $\langle a^m \rangle \subseteq H$. Итак, $H = \langle a^m \rangle$. Заметим, что для каждого $m \geq 2$ подгруппа $\langle a^m \rangle$ бесконечна и не совпадает с G .

СЛЕДСТВИЕ. *Все неединичные подгруппы бесконечной циклической группы являются бесконечными циклическими подгруппами.* $\square$

Напомним, что (n, m) означает наибольший общий делитель чисел n и m .

ЛЕММА 1.23. *Если $\langle a \rangle$ — циклическая группа порядка n , то элемент a^m имеет порядок $n/(n, m)$. В частности, элемент a^m имеет порядок n тогда и только тогда, когда n и m взаимно просты.*

Пусть $n = dn_1$, $m = dm_1$, где $d = (n, m)$. Ясно, что n_1 и m_1 взаимно просты. Если $a^{mt} = e$, то dn_1 делит $mt = dm_1 t$ и n_1 делит t . Так как

$$a^{mn_1} = a^{dm_1 n_1} = a^{nm_1} = e,$$

то n_1 — порядок элемента a^m .

ТЕОРЕМА 1.24. *Все подгруппы конечной циклической группы $\langle a \rangle$ порядка n исчерпываются циклическими подгруппами $\langle a^m \rangle$ порядка n/t для каждого натурального t , делящего n .*

Пусть H — подгруппа группы

$$\langle a \rangle = \{e, a, \dots, a^{n-1}\}.$$

Тогда $e \in H$ и если других элементов в H нет, то $H = \{e\} = \langle a^n \rangle$ — единичная подгруппа порядка 1.

Пусть $a^m \in H$, $a^m \neq e$, m — наименьшее. Допустим, что a^t — произвольный элемент из H . Разделим число t на m с остатком:

$$t = mq + r, \quad 0 \leq r < m.$$

Теперь,

$$a^r = a^{t-mq} = a^t a^{-mq} = a^t (a^{mq})^{-1} \in H,$$

поскольку a^t и $a^m \in H$. По выбору m получаем, что $r = 0$ и t делится на m . Итак, в H все элементы являются степенями элемента a^m . Следовательно, $H = \langle a^m \rangle$ — циклическая группа.

Убедимся, что m делит n . Пусть

$$n = mq + r, \quad 0 \leq r < m.$$

Тогда

$$a^r = a^{n-mq} = a^n (a^{mq})^{-1} = e((a^m)^q)^{-1} \in H.$$

Из минимальности m следует, что $r = 0$ и n делится на m . По лемме 3.6 порядок H равен n/m .

СЛЕДСТВИЕ. В конечной циклической группе порядка n для каждого натурального делителя d числа n существует единственная подгруппа порядка d .

Пусть $G = \langle a \rangle$ — конечная циклическая группа порядка n и d — натуральное число, делящее n . По теореме 3.7 в группе G существует подгруппа $D = \langle a^{n/d} \rangle$ порядка d . Если M — другая подгруппа порядка d , то по теореме 3.7 подгруппа $M = \langle a^m \rangle$, m делит n и $|a^m| = n/m = d$. Поэтому $m = n/d$ и $M = \langle a^m \rangle = \langle a^{n/d} \rangle = D$.

Следующая теорема позволяет упростить критерий подгруппы в случае, когда группа конечная.

ТЕОРЕМА 1.25. Пусть H — непустое подмножество группы G и пусть каждый элемент из H имеет конечный порядок. Если $h_1 h_2 \in H$ для всех h_1 и $h_2 \in H$, то H — подгруппа.

Так как каждый элемент $h \in H$ имеет конечный порядок, то

$$\langle h \rangle = \{e, h, \dots, h^{k-1}\}, \quad k = |h|.$$

Очевидно,

$$hh^{k-1} = h^{k-1}h = h^k = e, \quad h^{k-1} = h^{-1}.$$

По условию теоремы

$$h^{-1} = \underbrace{h \dots h}_{(k-1) \text{ раз}} \in H.$$

Теперь H — подгруппа по теореме 2.1.

СЛЕДСТВИЕ. Если H — непустое подмножество конечной группы G и $h_1 h_2 \in H$ для всех h_1 и $h_2 \in H$, то H — подгруппа. $\square$

ПРИМЕР 1.10. Рассмотрим аддитивную группу $\mathbb{Z}$ целых чисел. В аддитивной записи теорема 3.1 принимает вид: циклическая подгруппа $\langle a \rangle$, порожденная элементом a , состоит из всевозможных кратных элемента a , то есть $\langle a \rangle = \{ta \mid t \in \mathbb{Z}\}$. Так как $\langle 1 \rangle = \{m1 \mid m \in \mathbb{Z}\}$, то циклическая подгруппа, порожденная элементом 1, совпадает со всей группой. Итак, $(\mathbb{Z}, +)$ — бесконечная циклическая группа. Ясно, что $\langle -1 \rangle = \mathbb{Z}$ и $\langle a \rangle \neq \mathbb{Z}$ для любого целого $a \notin \{-1, 1\}$. $\square$

ПРИМЕР 1.11. Для каждого натурального n в мультипликативной группе $\mathbb{C}^\#$ комплексных чисел без нуля имеется n различных корней степени n из единицы, которые находятся по следующей формуле:

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad k = 0, 1, \dots, n-1.$$

Так как $\varepsilon_k = \varepsilon_1^k$, то множество корней степени n из единицы образует циклическую группу $\langle \varepsilon_1 \rangle$ порядка n , порожденную элементом ε_1 . $\square$

ТЕОРЕМА 1.26. *Порядок перестановки есть наименьшее общее кратное длин её независимых циклов.*

Если $(a_1 a_2)$ — цикл длины 2, то $(a_1 a_2)(a_1 a_2) = \varepsilon$, т.е. транспозиция есть перестановка порядка 2. Если $(a_1 a_2 a_3)$ — цикл длины 3, то

$$(a_1 a_2 a_3)(a_1 a_2 a_3) = (a_1 a_3 a_2); \quad (a_1 a_2 a_3)^3 = \varepsilon,$$

т.е. цикл длины 3 имеет порядок 3. Аналогично цикл $(a_1 a_2 \dots a_k)$ длины k есть перестановка порядка k .

Пусть теперь перестановка

$$\tau = (a_1 a_2 \dots a_{l_1}) \dots (b_1 b_2 \dots b_{l_t})$$

разложима в произведение независимых циклов длины $l_1, l_2, \dots, l_t$. Так как независимые циклы перестановочны, то

$$\tau^k = (a_1 a_2 \dots a_{l_1})^k \dots (b_1 b_2 \dots b_{l_t})^k.$$

Поэтому $\tau^k = \varepsilon$ тогда и только тогда, когда k делится на $l_1, l_2, \dots, l_t$, т.е. k — кратное числам $l_1, l_2, \dots, l_t$. Если k — порядок перестановки τ , то k — наименьшее натуральное число, для которого $\tau^k = \varepsilon$. Следовательно, порядок перестановки есть наименьшее общее кратное длин её независимых циклов.

ПРИМЕР 1.12. Перечислим порядки элементов в группе S_3 .

Так как $S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}$, то на основании теоремы 3.13 имеем:

$$|\varepsilon| = 1, |(12)| = |(13)| = |(23)| = 2, |(123)| = |(132)| = 3.$$

$\square$

ПРИМЕР 1.13. Перечислим порядки элементов в группе S_4 .

Запись $(\dots)(\dots)$ обозначает любую перестановку в S_4 , разлагающуюся на циклы длины 3 и 1. В S_4 возможны следующие разложения: $(\dots)(\dots)(\dots)$, $(\dots)(\dots)(\dots)$, $(\dots)(\dots)$, $(\dots)(\dots)$, $(\dots)$. На основании теоремы 3.13 в группе S_4 элементы имеют порядки 1, 2, 3, 4. $\square$

ПРИМЕР 1.14. В группе S_6 нет элементов порядка 7, 8, 9, 10. $\square$

ЛЕММА 1.27. *Если в группе все неединичные элементы имеют порядок 2, то группа абелева.*

Пусть $|a| = 2$ для всех $a \in G^\#$. Тогда $a^2 = e$ и $a = a^{-1}$ для всех $a \in G$. Так как $(ab)^2 = abab = e$ для всех $a, b \in G$, то $ab = b^{-1}a^{-1} = ba$.

ЛЕММА 1.28. *Порядки сопряженных элементов равны.*

Воспользуемся леммой 1.9(4). Пусть $a, x \in G$ и $|a| = k$. Тогда

$$(a^x)^k = (a^k)^x = e$$

и $|a^x|$ делит k по теореме 3.3. Если $|a^x| = l$, то

$$a^l = ((a^x)^{x^{-1}})^l = ((a^x)^l)^{x^{-1}} = e$$

и l делится на k .

1.4. Изоморфизм групп

Две группы G и G_1 называются *изоморфными*, если существует биекция $f : G \rightarrow G_1$ такая, что $f(ab) = f(a)f(b)$ для всех $a, b \in G$. Факт изоморфизма записывают так: $G \simeq G_1$.

Отметим простейшие свойства изоморфизма.

ЛЕММА 1.29. Пусть $f : G \rightarrow G_1$ — изоморфизм группы G на группу G_1 . Тогда:

- (1) если e — единичный элемент группы G , то $f(e)$ — единичный элемент группы G_1 ;
- (2) если a^{-1} — обратный элемент к элементу a в группе G , то $f(a^{-1}) = f(a)^{-1}$, т.е. $f(a^{-1})$ — обратный элемент к элементу $f(a)$ в группе G_1 . $\square$

ЛЕММА 1.30. (1) $G \simeq G$.

(2) Пусть $f : G \rightarrow G_1$ — изоморфизм групп. Тогда обратное отображение $f^{-1} : G_1 \rightarrow G$ является изоморфизмом. Таким образом, если $G \simeq G_1$, то $G_1 \simeq G$.

(3) Если $G \simeq G_1$, а $G_1 \simeq G_2$, то $G \simeq G_2$.

(4) Отношение “быть изоморфными группами” является отношением эквивалентности.

(1) Отображение $e_G : G \rightarrow G$, переводящее каждый элемент в себя, т.е. $e_G : g \mapsto g$ для всех $g \in G$, очевидно, изоморфизм G на G .

(2) Известно, что для каждого биективного отображения $f : G \rightarrow G_1$ существует обратное отображение $f^{-1} : G_1 \rightarrow G$, которое также будет биекцией. Если $a \in G$ и $f(a) = a_1 \in G_1$, то $f^{-1}(a_1) = a$. Пусть еще $b \in G$ и $b_1 = f(b) \in G_1$. Тогда $f^{-1}(b_1) = b$ и

$$a_1 b_1 = f(a) f(b) = f(ab)$$

поскольку f изоморфизм. Отсюда

$$f^{-1}(a_1 b_1) = ab = f^{-1}(a_1) f^{-1}(b_1),$$

что доказывает изоморфизм f^{-1} .

(3) Пусть $f : G \rightarrow G_1$ — изоморфизм групп G и G_1 , а $\varphi : G_1 \rightarrow G_2$ — изоморфизм G_1 и G_2 . Тогда φf — биективное отображение G на G_2 причем,

$$\begin{aligned} \varphi f(ab) &= \varphi(f(ab)) = \varphi(f(a)f(b)) = \\ &= \varphi(f(a))\varphi(f(b)) = \varphi f(a)\varphi f(b) \end{aligned}$$

для любых a и $b \in G$. Значит, φf — изоморфизм G и G_2 .

(4) следует из (1-3).

Теперь можно утверждать, что множество всех групп распадается на непересекающиеся классы изоморфных групп.

ТЕОРЕМА 1.31. (1) Все бесконечные циклические группы изоморфны между собой и изоморфны аддитивной группе целых чисел.

(2) Все конечные циклические группы одного порядка изоморфны между собой.

(1) Пусть $\langle g \rangle$ — бесконечная циклическая группа, порожденная элементом g , а $\mathbb{Z}$ — аддитивная группа целых чисел. Все степени g^n различны, поэтому отображение $f : n \mapsto g^n$ будет биекцией между $\mathbb{Z}$ и $\langle g \rangle$. Так как $g^{m+n} = g^m g^n$, то

$$f(m+n) = g^{m+n} = g^m g^n = f(m)f(n)$$

и f — изоморфизм. Таким образом, каждая бесконечная циклическая группа изоморфна аддитивной группе целых чисел. Поэтому все бесконечные циклические группы изоморфны между собой.

(2) Пусть теперь

$$G_1 = \{e_1, g_1, g_1^2, \dots, g_1^{k-1}\}; \quad G_2 = \{e_2, g_2, g_2^2, \dots, g_2^{k-1}\}$$

— две мультипликативные циклические группы порядка k . Определим отображение

$$f : g_1^t \mapsto g_2^t, \quad t = 0, 1, 2, \dots, k-1.$$

Для любых n и $m \in \{0, 1, \dots, k-1\}$ пусть $n+m = kq+r$, $0 \leq r \leq k-1$. Тогда

$$\begin{aligned} f(g_1^n g_1^m) &= f(g_1^{n+m}) = f(g_1^r) = g_2^r = g_2^{n+m} \\ &= g_2^n g_2^m = f(g_1^n) f(g_1^m). \end{aligned}$$

Матрица перестановки. Установим теперь связь между перестановками из симметрической группы S_n степени n и квадратными $n \times n$ -матрицами. Матрицей перестановки $\pi \in S_n$ назовем $n \times n$ -матрицу $\mathcal{M}(\pi) = (a_{ij})$, определенную так:

$$a_{ij} = \begin{cases} 1, & \text{если } i = \pi(j), \\ 0, & \text{если } i \neq \pi(j). \end{cases}$$

Таким образом, в матрице перестановки n единиц, остальные элементы равны нулю. Единица встречается один раз в каждой строке и в каждом столбце. В j -ом столбце единица стоит на $\pi(j)$ -м месте, т.е. в матрице $\mathcal{M}(\pi)$ только элементы $a_{\pi(k)k} = 1$, где $k = 1, 2, \dots, n$, остальные нули. Очевидно, $\mathcal{M}(\varepsilon) = E$. Через $\text{sgn}(\pi)$ обозначается знак перестановки π .

ТЕОРЕМА 1.32. (1) Матрица произведения перестановок равна произведению матриц перестановок, т.е. $\mathcal{M}(\pi\tau) = \mathcal{M}(\pi)\mathcal{M}(\tau)$ для всех π и $\tau \in S_n$.

(2) $\det \mathcal{M}(\pi) = \text{sgn}(\pi)$ для всех $\pi \in S_n$.

(3) Отображение $\mathcal{M} : \tau \mapsto \mathcal{M}(\tau)$ осуществляет изоморфизм симметрической группы S_n степени n и подгруппы $\text{Im} \mathcal{M} = \{\mathcal{M}(\tau) \mid \tau \in S_n\}$ из группы $GL(n, \mathbb{R})$.

(1) Пусть $\pi(k) = \tau$, тогда в строке $\mathcal{M}(\pi)_i$ единица стоит на k -ом месте. В столбце $\mathcal{M}(\tau)^j$ единица стоит на $\tau(j)$ -м месте. Поэтому

$$\begin{aligned} \mathcal{M}(\pi)_i \mathcal{M}(\tau)^j &= (0 \dots 1 \dots 0)[0 \dots 1 \dots 0] = \\ &= \begin{cases} 1, & \text{если } k = \tau(j), \text{ где } \pi(k) = i, \\ 0, & \text{если } k \neq \tau(j) \end{cases} \end{aligned}$$

$$= \begin{cases} 1, & \text{если } i = \pi\tau(j), \\ 0, & \text{если } i \neq \pi\tau(j). \end{cases}$$

Так как $\mathcal{M}(\pi\tau) = a(ij)$, где

$$a_{ij} = \begin{cases} 1, & \text{если } i = \pi\tau(j), \\ 0, & \text{если } i \neq \pi\tau(j), \end{cases}$$

то $a_{ij} = \mathcal{M}(\pi)_i \mathcal{M}(\tau)^j$ и $\mathcal{M}(\pi\tau) = \mathcal{M}(\pi)\mathcal{M}(\tau)$.

(2) В матрице $\mathcal{M}(\pi) = (a_{ij})$ только элементы $a_{\pi(k)k}$ равны единице, где $k = 1, 2, \dots, n$, остальные нули. Если $\tau \neq \pi^{-1}$, то существует число m такое, что $\tau(m) \neq \pi^{-1}(m)$ и $a_{n\pi^{-1}(m)} \neq a_{m\tau(m)}$. Но

$$a_{m\tau(m)} = a_{\pi(\pi^{-1}(m))\pi^{-1}(m)} = 1,$$

значит $a_{m\tau(m)} = 0$ и в сумме

$$\det \mathcal{M}(\pi) = \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{1\tau(1)} \dots a_{n\tau(n)}$$

только одно ненулевое слагаемое, которое отвечает перестановке π^{-1} . Поэтому

$$\det \mathcal{M}(\pi) = \operatorname{sgn}(\pi^{-1}) a_{1\pi^{-1}(1)} \dots a_{n\pi^{-1}(n)}.$$

Поскольку $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$, а

$$a_{i\pi^{-1}(i)} = a_{\pi(\pi^{-1}(i))\pi^{-1}(i)} = 1,$$

то $\det \mathcal{M}(\pi) = \operatorname{sgn}(\pi)$.

(3) Так как

$$\det \mathcal{M}(\tau) = \operatorname{sgn}(\tau) \in \{-1, 1\},$$

то $\mathcal{M}$ отображение S_n в $GL(n, \mathbb{R})$. Из построения $\mathcal{M}(\tau)$ следует, что $\mathcal{M}$ — инъекция. Покажем, что $\operatorname{Im} \mathcal{M}$ — подгруппа группы $GL(n, \mathbb{R})$. Так как $\mathcal{M}(\tau)\mathcal{M}(\pi) = \mathcal{M}(\tau\pi)$ по (1), то $\mathcal{M}(\tau)\mathcal{M}(\pi) \in \operatorname{Im} \mathcal{M}$. Далее, $\mathcal{M}(\varepsilon) = E$, и если τ имеет порядок t , то $\tau^t = \varepsilon$ и $\mathcal{M}(\tau^t) = E = \mathcal{M}(\tau)^t$, т.е. порядок матрицы $\mathcal{M}(\tau)$ делит t . Таким образом, все матрицы перестановок имеют конечные порядки и $\operatorname{Im} \mathcal{M}$ — подгруппа $GL(n, \mathbb{R})$ по теореме 3.9. Поэтому $\mathcal{M} : S_n \rightarrow \operatorname{Im} \mathcal{M}$ — биекция, а по (1) отображение $\mathcal{M}$ — изоморфизм.

ТЕОРЕМА 1.33. (КЭЛИ) *Любая конечная группа порядка n изоморфна подгруппе симметрической группы S_n степени n .*

Пусть G — конечная группа порядка n и $G = \{g_1 = e, g_2, \dots, g_n\}$ — все её элементы. Можно считать, что S_n — совокупность всех биективных отображений множества $\{e, g_2, \dots, g_n\}$ на себя. Для каждого $x \in G$ определим отображение $l_x : g_i \mapsto xg_i = l_x(g_i)$ множества G в себя. Если $xg_i = xg_j$, то $g_i = g_j$ и l_x — инъекция. Но инъекция конечного множества всегда биекция, поэтому $l_x \in S_n$.

Зададим теперь отображение $\varphi : G \rightarrow S_n$, полагая $\varphi : x \mapsto l_x$. Тогда $\operatorname{Im} \varphi = \{lg_1, lg_2, \dots, lg_n\}$. Покажем, что $\operatorname{Im} \varphi$ — подгруппа группы S_n . Если l_x и l_y — произвольные элементы из $\operatorname{Im} \varphi$, то

$$l_x l_y(g_i) = l_x(l_y(g_i)) = l_x(yg_i) = xyg_i = l_{xy}(g_i) \quad <1>$$

и $l_x l_y = l_{xy} \in \operatorname{Im} \varphi$. По теореме 3.9 множество $\operatorname{Im} \varphi$ есть подгруппа группы S_n . Из <1> заключаем, что $l_x l_y = l_{xy}$, поэтому $\varphi(xy) = \varphi(x)\varphi(y)$ и φ —

изоморфизм между G и $\text{Im}\varphi$.

Сопоставляя теорему Кэли с теоремой 4.4(3), получаем

СЛЕДСТВИЕ. Любая конечная группа порядка n изоморфна подгруппе полной линейной группы $GL(n, \mathbb{R})$ степени n над $\mathbb{R}$. $\square$

СЛЕДСТВИЕ. Число неизоморфных групп данного порядка конечно.

Зафиксируем натуральное число n . По теореме Кэли каждая группа порядка n изоморфна подгруппе симметрической группы S_n . Так как группа S_n конечна, то число её неизоморфных подгрупп конечно.

Автоморфизмы групп. Положив $G_1 = G$ в определении изоморфизма, получим изоморфное отображение группы G на себя, которое называют *автоморфизмом* группы G . Совокупность всех автоморфизмов группы G обозначим через $\text{Aut}G$. Если φ и ψ — автоморфизмы группы G , то согласно определению умножения отображений произведение автоморфизмов определяется так:

$$\begin{aligned}\varphi\psi(ab) &= \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) = \\ &= \varphi(\psi(a))\varphi(\psi(b)) = \varphi\psi(a)\varphi\psi(b)\end{aligned}$$

для любых a и $b \in G$. Поэтому $\varphi\psi$ — автоморфизм G и умножение автоморфизмов определено на $\text{Aut}G$. Ассоциативность умножения автоморфизмов вытекает из ассоциативности умножения отображений. Единичное отображение $e_G : G \rightarrow G$, переводящее каждый элемент в себя, является автоморфизмом группы G . По лемме 4.2 каждый автоморфизм обладает обратным. Таким образом доказана следующая

ТЕОРЕМА 1.34. Совокупность $\text{Aut}G$ всех автоморфизмов группы G является группой. $\square$

ПРИМЕР 1.15. Проверим, что

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

— группа относительно умножения, изоморфная мультипликативной группе $G_1 = \{1, -1\}$.

Так как

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

то

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in G.$$

Остальные произведения элементов из G также принадлежат G , поэтому G — группа. Отображение

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

очевидно, будет изоморфизмом. $\square$

ПРИМЕР 1.16. Покажем, что мультипликативная группа $\mathbb{R}_+$ положительных действительных чисел изоморфна аддитивной группе $\mathbb{R}$ всех действительных чисел. В качестве изоморфного отображения может служить логарифмическая функция $\ln x$. Если x и $y \in \mathbb{R}_+$, то $\ln(xy) = \ln x + \ln y$. Так как функция $y = \ln x$ задает биективное отображение $\mathbb{R}_+$ на $\mathbb{R}$, то $\ln$ — изоморфизм групп $\mathbb{R}_+$ и $\mathbb{R}$. $\square$

ПРИМЕР 1.17. Найдем матрицы, соответствующие перестановкам степени 3.

Так как $S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}$, то

$$\begin{aligned}\mathcal{M}(\varepsilon) &= E; & \mathcal{M}(12) &= \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}; \\ \mathcal{M}(13) &= \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}; & \mathcal{M}(23) &= \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}; \\ \mathcal{M}(123) &= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}; & \mathcal{M}(132) &= \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.\end{aligned}$$

$\square$

ПРИМЕР 1.18. Пусть $H \leq G$ и $x \in G$. Зададим отображение $f : H \rightarrow H^x$ полагая $f(h) = h^x$ для всех $h \in H$. Ясно, что f — биекция. Так как

$$f(h_1 h_2) = (h_1 h_2)^x = (h_1)^x (h_2)^x = f(h_1) f(h_2),$$

то f — изоморфизм. Таким образом, в любой группе сопряженные подгруппы изоморфны. $\square$

1.5. Смежные классы

Пусть G — группа, $H \leq G$ и $g \in G$. *Правым смежным классом* группы G по подгруппе H называется множество

$$Hg = \{hg \mid h \in H\}$$

всех элементов группы G вида hg , где h пробегает все элементы подгруппы H .

Аналогично определяется *левый смежный класс*

$$gH = \{gh \mid h \in H\}.$$

ЛЕММА 1.35. Пусть G — группа, H — подгруппа. Тогда:

- (1) $H = He$;
- (2) $g \in Hg$ для каждого $g \in G$;
- (3) если $a \in H$, то $Ha = H$; если $b \in Ha$, то $Hb = Ha$;
- (4) $Ha = Hb$ тогда и только тогда, когда $ab^{-1} \in H$;
- (5) два смежных класса либо совпадают, либо их пересечение пусто;
- (6) если H — конечная подгруппа, то $|Hg| = |H|$ для всех $g \in G$.

Первые три свойства вытекают из определения правого смежного класса.

(4) Если $Ha = Hb$, то $ea = hb$, $h \in H$ и $ab^{-1} = h \in H$. Обратно, если $ab^{-1} \in H$, то $ab^{-1} = h \in H$, поэтому $a = hb$ и $Ha = Hhb = Hb$.

(5) Пусть $Ha \cap Hb \neq \emptyset$ и $c \in Ha \cap Hb$. Тогда $c = h_1a = h_2b$ и $ab^{-1} = h_1^{-1}h_2 \in H$. Теперь $Ha = Hb$ по свойству (4).

(6) Для каждого $g \in G$ отображение $\phi : h \mapsto hg$ есть биекция множеств H и Hg . Поэтому $|H| = |Hg|$.

Из свойств (2) и (5) следует, что каждый элемент группы G содержится точно в одном правом смежном классе по подгруппе H . Это свойство позволяет ввести следующее определение.

Трансверсаль. Пусть H — подгруппа группы G . Подмножество T элементов группы G называется *правой трансверсалью* подгруппы H в группе G , если T содержит точно один элемент из каждого правого смежного класса группы G по подгруппе H . Итак, если

$$T = \{t_\alpha \mid \alpha \in I\}$$

— правая трансверсаль подгруппы H в группе G , то

$$G = \bigcup_{t_\alpha \in T} Ht_\alpha, \quad Ht_\alpha \cap Ht_\beta = \emptyset \quad \text{при} \quad \alpha \neq \beta.$$

Таким образом справедлива

ТЕОРЕМА 1.36. *Группа G является объединением непересекающихся правых смежных классов по подгруппе H .*

□

Если G — конечная группа, то число различных правых смежных классов по подгруппе H также будет конечно, оно называется *индексом подгруппы H в группе G* и обозначается через $|G : H|$. Ясно, что индекс подгруппы H в конечной группе G совпадает с числом элементов в правой трансверсали T подгруппы H , т.е.

$$|G : H| = |T| = |G|/|H|.$$

ТЕОРЕМА 1.37. (ЛАГРАНЖ) *Если H — подгруппа конечной группы G , то $|G| = |H| \cdot |G : H|$. В частности, порядок конечной группы делится на порядок каждой своей подгруппы.*

Пусть индекс подгруппы H в группе G равен n . По теореме 5.2 имеем разложение

$$G = Hg_1 \cup Hg_2 \cup \dots \cup Hg_n, \quad Hg_i \cap Hg_j = \emptyset \quad \text{при} \quad i \neq j.$$

Так как $|Hg_i| = |H|$ для всех i , то $|G| = |H| \cdot |G : H|$.

СЛЕДСТВИЕ. *Порядок каждого элемента конечной группы делит порядок всей группы.*

Порядок элемента a совпадает с порядком циклической подгруппы $\langle a \rangle$, порожденной этим элементом, см. теорему 3.3. Поэтому, $|\langle a \rangle| = |a|$ делит $|G|$.

Аналогично определяется *левая трансверсаль* подгруппы H в группе G . Если

$$L = \{l_\alpha \mid \alpha \in J\}$$

— левая трансверсаль подгруппы H в группе G , то

$$G = \cup_{\alpha \in J} l_{\alpha}H, \quad l_{\alpha}H \cap l_{\beta}H = \emptyset \quad \text{при} \quad \alpha \neq \beta.$$

Ясно, что индекс подгруппы H в конечной группе G совпадает с числом элементов в левой трансверсали L подгруппы H , т.е. $|G : H| = |L|$. Для левой трансверсали справедлив аналог теоремы 5.2. Поэтому из теоремы Лагранжа вытекает

СЛЕДСТВИЕ. Число левых и число правых смежных классов конечной группы G по подгруппе H совпадают. □

ТЕОРЕМА 1.38. В группе простого порядка нет нетривиальных подгрупп. В частности, группа простого порядка циклическая.

Пусть G — конечная группа простого порядка p . Если H — подгруппа группы G , то по теореме Лагранжа $|H|$ делит $|G|$. Поэтому либо $|H| = 1$ и H — единичная подгруппа, либо $|H| = p$ и H совпадает с группой G . Выберем неединичный элемент a в группе G и рассмотрим циклическую подгруппу $\langle a \rangle$, порожденную этим элементом. Так как $a \neq e$, то $\langle a \rangle \neq E$, поэтому $\langle a \rangle = G$ и G — циклическая группа.

ТЕОРЕМА 1.39. Пусть $H \leq K \leq G$ и G — конечная группа. Если T — правая трансверсаль подгруппы H в группе K , а S — правая трансверсаль подгруппы K в группе G , то TS — правая трансверсаль подгруппы H в группе G . В частности,

$$|G : H| = |G : K| |K : H|.$$

Пусть $T = \{t_1, \dots, t_k\}$, $S = \{s_1, \dots, s_n\}$. Тогда

$$\begin{aligned} K &= Ht_1 \cup \dots \cup Ht_k, \quad Ht_i \cap Ht_j = \emptyset, \quad i \neq j; \\ G &= Ks_1 \cup \dots \cup Ks_n, \quad Ks_i \cap Ks_j = \emptyset, \quad i \neq j. \end{aligned}$$

Теперь

$$G = (Ht_1 \cup \dots \cup Ht_k)s_1 \cup \dots \cup (Ht_1 \cup \dots \cup Ht_k)s_n. \quad <1>$$

Предположим, что $Ht_a s_b = Ht_c s_d$ для некоторых натуральных a, b, c и d . Тогда

$$t_a s_b (t_c s_d)^{-1} = t_a s_b s_d^{-1} t_c^{-1} \in H \leq K,$$

поэтому

$$s_b s_d^{-1} \in t_a^{-1} K t_c = K, \quad K s_b = K s_d.$$

Но s_b и s_d — элементы из правой трансверсали подгруппы K в группе G , поэтому $s_b = s_d$ и $b = d$. Теперь

$$t_a s_b (t_c s_d)^{-1} = t_a t_c^{-1} \in H, \quad Ht_a = Ht_c$$

и $a = c$. Таким образом, $<1>$ является разложением группы G по подгруппе H и TS — правая трансверсаль подгруппы H в группе G . Так как индекс подгруппы совпадает с числом элементов в правой трансверсали этой подгруппы, то

$$|G : H| = |TS| = |T| |S| = |K : H| |G : K|.$$

Отметим, что теорема Лагранжа вытекает из теоремы 5.7 при $H = E$.

Двойные смежные классы. Пусть H и K — подгруппы группы G и $g \in G$. Множество

$$HgK = \{h g k \mid h \in H, k \in K\}$$

называется *двойным смежным классом* группы G по подгруппам H и K .

ЛЕММА 1.40. Пусть H и K — подгруппы группы G . Тогда справедливы следующие утверждения:

(1) каждый элемент $g \in G$ содержится в единственном двойном смежном классе HgK ;

(2) два двойных смежных класса по H и K либо совпадают, либо их пересечение пусто;

(3) группа G есть объединение непересекающихся двойных смежных классов по подгруппам H и K ;

(4) каждый двойной смежный класс по H и K есть объединение правых смежных классов по H ; каждый двойной смежный класс по H и K есть объединение левых смежных классов по K ;

(5) если группа G конечна, то двойной смежный класс HgK содержит $|K : H^g \cap K|$ правых смежных классов по H и $|H : H \cap K^{g^{-1}}|$ левых смежных классов по K .

(1) Так как каждая подгруппа содержит единичный элемент, то

$$g = e g e \in H g K.$$

Допустим, что $g \in H x K$. Тогда $g = h x k$ для некоторых $h \in H$, $k \in K$ и

$$H g K = H(h x k)K = H x K.$$

(2) и (3) следуют из (1).

(4) Так как

$$H g K = \bigcup_{k \in K} H g k = \bigcup_{h \in H} h g K,$$

то утверждение (4) доказано.

(5) Подсчитаем число правых смежных классов в разложении

$$H g K = \bigcup_{k \in K} H g k.$$

Допустим, что $H g k_1 = H g k_2$. Тогда $H g k_1 k_2^{-1} = H g$ и

$$k_1 k_2^{-1} \in g^{-1} H g \cap K = H^g \cap K$$

по лемме 1.35. Справедливо и обратное, т.е. если $k_1 k_2^{-1} \in H^g \cap K$, то

$$k_1 k_2^{-1} \in g^{-1} H g, \quad g k_1 k_2^{-1} \in H g, \quad g k_1 \in H g k_2$$

и $H g k_1 = H g k_2$. Поэтому, в двойном смежном классе $H g K$ правых смежных классов по H столько, сколько их в группе K по подгруппе $H^g \cap K$.

Аналогично,

$$H g K = \bigcup_{h \in H} h g K \quad \text{и} \quad h_1 g K = h_2 g K$$

тогда и только тогда, когда $h_1^{-1} h_2 \in H \cap K^{g^{-1}}$. Поэтому, в $H g K$ левых смежных классов по K будет точно столько, каков индекс $|H : H \cap K^{g^{-1}}|$.

Произведение подгрупп. При $g = e$ двойной смежный класс

$$H g K = H K = \{h k \mid h \in H, k \in K\}$$

превращается в произведение подгрупп H и K . В общем случае $H K$ не является подгруппой.

Говорят, что подгруппы H и K *перестановочны*, если $HK = KH$. Равенство $HK = KH$ означает, что для любых $h_1 \in H, k_1 \in K$ существуют $h_2 \in H, k_2 \in K$ такие, что $h_1 k_1 = k_2 h_2$.

ТЕОРЕМА 1.41. *Произведение двух подгрупп является подгруппой тогда и только тогда, когда эти подгруппы перестановочны.*

Пусть H и K — подгруппы группы G . Предположим, что HK — подгруппа, и пусть $h \in H, k \in K$. Тогда

$$kh = (h^{-1}k^{-1})^{-1} \in HK \quad \text{и} \quad KH \subseteq HK.$$

Поскольку для элемента hk в подгруппе HK существует элемент $h_1 k_1$ такой, что $(h_1 k_1)^{-1} = hk$, то

$$hk = k_1^{-1} h_1^{-1} \in KH \quad \text{и} \quad HK \subseteq KH.$$

Итак, если HK — подгруппа, то $HK = KH$.

Обратно, пусть $HK = KH$. Тогда для любых $h_1, h_2 \in H, k_1, k_2 \in K$ имеем: $k_1 h_2 = h_3 k_3$, где $h_3 \in H, k_3 \in K$. Поэтому

$$(h_1 k_1)(h_2 k_2) = h_1 (k_1 h_2) k_2 = h_1 h_3 k_3 k_2 \in HK$$

и

$$(h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH = HK.$$

Значит, HK — подгруппа.

ТЕОРЕМА 1.42. *Если H и K — подгруппы конечной группы G , то $|HK| = |H| |K| / |H \cap K|$.*

Рассмотрим HeK и применим лемму 5.8. По этой лемме HK есть объединение правых смежных классов по H и этих правых смежных классов $|K : K \cap H|$ штук. Так как $|Hk| = |H|$ и различные правые смежные классы имеют пустое пересечение, то

$$|HK| = |H| |K : K \cap H| = |H| |K| / |K \cap H|.$$

Если $HK = G$, то говорят, что группа G есть *произведение своих подгрупп H и K* , либо группа G *факторизуема подгруппами H и K* . В этом случае каждый элемент $g \in G$ представим в виде $g = hk$, где $h \in H, k \in K$.

ЛЕММА 1.43. *Если H и K — подгруппы группы G и $G = HK$, то $G = KH$ и $G = H^x K$ при любом $x \in G$.*

Так как $G = HK$ — подгруппа группы G , то $G = HK = KH$ по теореме 5.9. Если x — произвольный элемент из группы G , то $x = hk$, где $h \in H, k \in K$ и

$$\begin{aligned} H^x K &= H^{hk} K = H^k K = k^{-1} H k K = \\ &= k^{-1} H K = k^{-1} K H = K H = G. \end{aligned}$$

ЛЕММА 1.44. *Если H — собственная подгруппа группы G , то $H^x H \neq G$ при любом $x \in G$.*

Допустим противное, т.е. предположим, что существует $x \in G$ такой, что $H^x H = G$. По лемме 5.11

$$G = (H^x)^{x^{-1}} H = H H = H,$$

противоречие. Поэтому предположение неверно и $H^x H \neq G$ при любом $x \in G$.

ТЕОРЕМА 1.45. *Для любого простого числа p группа порядка p^2 абелева. Кроме того, группа порядка p^2 либо циклическая, либо является произведением двух своих подгрупп порядка p .*

Пусть p — простое число и G — группа порядка p^2 . Выберем неединичный элемент $a \in G$ и пусть $A = \langle a \rangle$. Если $A = G$, то G — циклическая группа. Пусть $A \neq G$. По теореме Лагранжа $|A| = p$. Выберем $b \in G \setminus A$ и пусть $B = \langle b \rangle$. Если $B = G$, то $G = \langle b \rangle$ — циклическая группа. Пусть $B \neq G$. По теореме Лагранжа $|B| = p$. Так как $A \cap B$ — собственная подгруппа в A и в B , то по теореме Лагранжа $A \cap B = E$ и

$$|AB| = |A| |B| = p^2, \text{ т.е. } AB = BA = G.$$

По лемме 5.12 подгруппы A и B не сопряжены между собой. Если существует элемент $g \in G$ такой, что $A \neq A^g$, то $A \cap A^g = E$ и

$$|AA^g| = |A| |A^g| = |G|, \text{ т.е. } G = AA^g,$$

что противоречит лемме 5.12. Поэтому допущение неверно и $A = A^g$ при любом $g \in G$. Аналогично, $B = B^g$ при любом $g \in G$. Теперь для любых $a \in A$, $b \in B$ имеем:

$$aba^{-1}b^{-1} = (aba^{-1})b^{-1} \in B^{a^{-1}}B = B,$$

$$aba^{-1}b^{-1} = a(ba^{-1}b^{-1}) \in AA^{b^{-1}} = A,$$

поэтому $aba^{-1}b^{-1} \in A \cap B = E$, $aba^{-1}b^{-1} = e$ и $ab = ba$.

ЛЕММА 1.46. *Для группы G справедливы следующие утверждения:*

(1) *если H — абелева подгруппа группы G , то $Z(G)H$ — также абелева подгруппа группы G ;*

(2) *если K — подгруппа группы G , то $Z(G)Z(K)$ — абелева подгруппа группы G .*

(1) Пусть H — абелева подгруппа группы G . Из определения центра группы следует, что для $Z(G)$ и H выполняются условия теоремы 5.9, поэтому $Z(G)H = HZ(G)$ — подгруппа группы G . Если x и $y \in Z(G)H$, то $x = z_1h_1$, $y = z_2h_2$, где $z_i \in Z(G)$, $h_i \in H$, $i = 1, 2$. Теперь

$$xy = z_1h_1z_2h_2 = z_2h_2z_1h_1 = yx,$$

т.е. $Z(G)H$ абелева.

(2) Пусть K — произвольная подгруппа группы G . Тогда центр $Z(K)$ является абелевой подгруппой группы G и $Z(G)Z(K)$ — абелева подгруппа по (1).

Произведение двух непустых подмножеств T и S группы G определяется как множество

$$TS = \{ts \mid t \in T, s \in S\}.$$

ЛЕММА 1.47. *Пусть T и S — непустые подмножества группы G , x и $y \in G$. Тогда:*

$$(1) T^{(xy)} = (T^x)^y;$$

(2) *множество всех элементов $g \in G$, для которых $T^g = T$, образует подгруппу группы G ;*

$$(3) (TS)^x = T^x S^x;$$

$$(4) (T \cap S)^x = T^x \cap S^x.$$

(1) Каждый элемент множества $T^{(xy)}$ может быть записан в виде $(xy)^{-1}txy$, где $t \in T$. Так как

$$(xy)^{-1}txy = y^{-1}x^{-1}txy \text{ и } x^{-1}tx \in T^x,$$

то

$$y^{-1}(x^{-1}tx)y \in (T^x)^y, \text{ т.е. } T^{(xy)} \subseteq (T^x)^y.$$

Обратно, каждый элемент множества $(T^x)^y$ может быть записан в виде $y^{-1}(x^{-1}sx)y$, где $s \in T$. Поэтому

$$y^{-1}(x^{-1}sx)y = (xy)^{-1}s(xy) \in T^{(xy)},$$

т.е. $(T^x)^y \subseteq T^{(xy)}$. Таким образом, $(T^x)^y = T^{(xy)}$.

(2) Пусть H — множество всех элементов g группы G , для которых $T^g = T$. Если g и $h \in H$, то

$$T^{(gh)} = (T^g)^h = T^h = T \text{ и } gh \in H.$$

Из равенства $T = T^g$ получаем, что

$$T^{g^{-1}} = (T^g)^{g^{-1}} = T^{gg^{-1}} = T,$$

поэтому $g^{-1} \in H$ и H — подгруппа группы G .

Утверждения (3) и (4) проверяются элементарно.

Нормализатор. Если T — непустое подмножество группы G и $g \in G$, то

$$gT = \{gt \mid t \in T\} \text{ и } Tg = \{tg \mid t \in T\}.$$

Элемент $g \in G$ называется *перестановочным* с подмножеством T , если $gT = Tg$. Равенство $gT = Tg$ означает, что для любого элемента $t_1 \in T$ существует такой элемент $t_2 \in T$, что $gt_1 = t_2g$. Если элемент g перестановочен с подмножеством T , то

$$gT = Tg \text{ и } T = g^{-1}Tg = T^g.$$

Совокупность всех элементов группы G , перестановочных с подмножеством T называется *нормализатором* подмножества T в группе G и обозначается через $N_G(T)$. Итак,

$$N_G(T) = \{g \in G \mid gT = Tg\} = \{g \in G \mid T^g = T\}.$$

ЛЕММА 1.48. Пусть T — непустое подмножество группы G , g — произвольный элемент группы G . Тогда:

- (1) $N_G(T) \leq G$;
- (2) $C_G(T) \leq N_G(T)$;
- (3) $N_G(T^g) = N_G(T)^g$;
- (4) $N_G(T) \leq N_G(C_G(T))$;
- (5) если H — подгруппа группы G , то $H \leq N_G(H)$.

Утверждение (1) следует из леммы 5.15(2).

(2) Если $x \in C_G(T)$, то x перестановочен с каждым элементом множества T , поэтому $xT = Tx$ и $x \in N_G(T)$.

(3) Если $x \in N_G(T^g)$, то $(T^g)^x = T^g$ и $T^{(gxg^{-1})} = T$ по лемме 1.47. Поэтому $gxg^{-1} \in N_G(T)$ и

$$x \in g^{-1}N_G(T)g = N_G(T)^g.$$

Таким образом, $N_G(T^g) \subseteq N_G(T)^g$. Обратно, если $y \in N_G(T)^g$, то $y = z^g$ для некоторого $z \in N_G(T)$ и $zT = Tz$. Отсюда $g^{-1}zTg = g^{-1}Tzg$ и

$$g^{-1}zTg = g^{-1}zgg^{-1}Tg = z^gT^g = yT^g.$$

Аналогично,

$$g^{-1}Tzg = g^{-1}Tgg^{-1}zg = T^gz^g = T^gy.$$

Таким образом, $yT^g = T^gy$ и $y \in N_G(T^g)$, т.е. $N_G(T)^g \subseteq N_G(T^g)$. Следовательно, $N_G(T)^g = N_G(T^g)$.

(4) Если $x \in N_G(T)$, то $T = T^x$ и

$$C_G(T) = C_G(T^x) = C_G(T)^x, \text{ т.е. } x \in N_G(C_G(T)).$$

(5) Если $h \in H$, то $hH = H = Hh$ и $h \in N_G(H)$, т.е. $H \leq N_G(H)$.

ТЕОРЕМА 1.49. Пусть S — непустое подмножество конечной группы G . Если $T = \{t_1, \dots, t_n\}$ — правая трансверсаль нормализатора $N_G(S)$ в группе G , то $\Sigma = \{S^{t_1}, \dots, S^{t_n}\}$ — совокупность всех подмножеств, сопряженных с S в группе G и $S^{t_i} \neq S^{t_j}$ при $i \neq j$. В частности, число подмножеств, сопряженных с S в группе G , совпадает с индексом нормализатора $N_G(S)$.

Пусть $K = N_G(S)$. По условию

$$G = Kt_1 \cup \dots \cup Kt_n, \quad Kt_i \neq Kt_j \text{ при } i \neq j.$$

Если x — произвольный элемент из группы G , то $x = kt_i$ для некоторого $k \in K$ и натурального i . Поэтому

$$S^x = S^{kt_i} = S^{t_i} \in \Sigma.$$

Если предположить, что $S^{t_i} = S^{t_j}$, то $S = S^{t_j t_i^{-1}}$ и $t_j t_i^{-1} \in K$, т.е. $Kt_j = Kt_i$. Так как элементы t_i и t_j из правой трансверсали подгруппы K в группе G , то $i = j$ и во множестве Σ все элементы попарно различны. Таким образом, $|\Sigma| = |T| = |G : N_G(S)|$.

Теперь с помощью теоремы Лагранжа получаем

СЛЕДСТВИЕ. Число подмножеств, сопряженных данному непустому подмножеству S в конечной группе G , делит порядок группы G . $\square$

Пусть множество S состоит из одного элемента s , т.е. $S = \{s\}$. Тогда нормализатор и централизатор множества S совпадают. Поэтому справедливо

СЛЕДСТВИЕ. Если s — элемент конечной группы G и $T = \{t_1, \dots, t_n\}$ — правая трансверсаль централизатора $C_G(s)$, то $s^G = \{s^{t_1}, \dots, s^{t_n}\}$. В частности, число элементов, сопряженных элементу s в группе G , совпадает с индексом централизатора $C_G(s)$ в группе G и делит порядок группы G . $\square$

В дальнейшем неоднократно будет использоваться следующее утверждение.

ЛЕММА 1.50. (ТОЖДЕСТВО ДЕДЕКИНДА) Если A, B и C — подгруппы группы G и $A \leq C$, то

$$C \cap AB = A(C \cap B).$$

Если $x \in C \cap AB$, то $x = ab$, где $a \in A$, $b \in B$. Так как $A \leq C$, то $a \in C$. Но $x \in C$, поэтому $b = a^{-1}x$ также принадлежит C . Таким образом, $x = ab \in A(C \cap B)$.

Обратно, пусть

$$x = ab \in A(C \cap B), \quad a \in A, \quad b \in C \cap B.$$

Поскольку $A \leq C$, то $a \in C$ и $x = ab \in C$. Таким образом, $x = ab \in C \cap AB$.

ПРИМЕР 1.19. Найдем разложение симметрической группы S_3 в левые смежные классы по подгруппе $\langle(12)\rangle$.

Для этого найдем все левые смежные классы группы

$$S_3 = \{\epsilon, (12), (13), (23), (123), (132)\}$$

по подгруппе $H = \langle a \rangle = \{\epsilon, (12)\}$.

$$\epsilon H = \epsilon\{\epsilon, (12)\} = \{\epsilon, (12)\} = H;$$

$$(12)H = (12)\{\epsilon, (12)\} = \{(12), \epsilon\} = H;$$

$$(13)H = (13)\{\epsilon, (12)\} = \{(13), (123)\};$$

$$(23)H = (23)\{\epsilon, (12)\} = \{(23), (132)\};$$

$$(123)H = (123)\{\epsilon, (12)\} = \{(123), (13)\} = (13)H;$$

$$(132)H = (132)\{\epsilon, (12)\} = \{(132), (23)\} = (23)H.$$

Искомое разложение принимает вид:

$$S_3 = \epsilon H \cup (13)H \cup (23)H.$$

□

ПРИМЕР 1.20. Найдем все подгруппы группы S_3 .

Порядок группы S_3 равен 6. По теореме Лагранжа ее подгруппы могут быть только следующих порядков: 1, 2, 3, 6. Подгруппы порядка 1 и 6 это единичная подгруппа $H_1 = \{\epsilon\}$ и вся группа $H_2 = G$. Подгруппы порядка 2 и 3 по теореме 1.38 циклические, поэтому для их нахождения надо перебрать все циклические подгруппы в S_3 . Перебирая все элементы группы S_3 получаем следующие подгруппы:

$$H_3 = \langle(12)\rangle = \{\epsilon, (12)\};$$

$$H_4 = \langle(13)\rangle = \{\epsilon, (13)\};$$

$$H_5 = \langle(23)\rangle = \{\epsilon, (23)\};$$

$$H_6 = \langle(123)\rangle = \{\epsilon, (123), (132)\} = \langle(132)\rangle.$$

Итак, S_3 имеет шесть подгрупп. Так как элементы $(12), (13), (23)$ сопряжены в S_3 (см. пример 1.14), то подгруппы H_3, H_4, H_5 сопряжены, причем $H_3^{(23)} = H_4, H_3^{(13)} = H_5$. Следовательно, группа S_3 содержит четыре класса сопряженных подгрупп:

$$\{H_1\}, \{H_2\}; \{H_3, H_4, H_5\}, \{H_6\}.$$

□

1.6. Нормальные подгруппы и факторгруппы

Подгруппа H называется *нормальной подгруппой* группы G , если $xH = Hx$ для всех $x \in G$. Запись $H \triangleleft G$ читается так: H — нормальная подгруппа группы G . Равенство $xH = Hx$ означает, что для любого элемента $h_1 \in H$ существует элемент $h_2 \in H$ такой, что $xh_1 = h_2x$.

ТЕОРЕМА 1.51. (КРИТЕРИЙ НОРМАЛЬНОЙ ПОДГРУППЫ) Для подгруппы H группы G следующие утверждения эквивалентны:

(1) H — нормальная подгруппа группы G ;

(2) подгруппа H вместе с каждым своим элементом содержит все ему сопряжённые элементы, т.е. $h^x \in H$ для всех $h \in H$ и всех $x \in G$;

(3) подгруппа H совпадает с каждой своей сопряженной подгруппой, т.е. $H = H^x$ для всех $x \in G$.

Доказательство проведем по схеме $(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (1)$.

$(1) \Rightarrow (2)$ Пусть $H \triangleleft G$, т.е. $xH = Hx$ для всех $x \in G$. Если h — произвольный элемент из H , то $hx \in Hx = xH$. Поэтому существует элемент $h_1 \in H$ такой, что $hx = xh_1$. Теперь $x^{-1}hx = h_1 \in H$.

$(2) \Rightarrow (3)$ Пусть выполняются требование (2). Тогда $H^x = \{h^x \mid h \in H\} \subseteq H$ для всех $x \in G$. В частности, $H^{x^{-1}} \subseteq H$, т.е. $xHx^{-1} \subseteq H$. Теперь $H \subseteq x^{-1}Hx = H^x$ и $H = H^x$ для всех $x \in G$.

$(3) \Rightarrow (1)$ Если $H^x = H$ для всех $x \in G$, то $x^{-1}Hx = H$ и $Hx = xH$ для всех $x \in G$, т.е. H нормальна в G .

СЛЕДСТВИЕ. Если $H \triangleleft G$ и $h \in H$, то $h^G \subseteq H$. Обратно, если $h^G \subseteq H$ для всех $h \in H$, то $H \triangleleft G$. $\square$

Понятие "нормальная подгруппа" можно рассматривать не только по отношению ко всей группе, но и относительно подгрупп. Если $H \leq K \leq G$, то подгруппа H будет нормальной в K , если $xH = Hx$ для всех $x \in K$.

ЛЕММА 1.52. Пусть H — подгруппа группы G . Тогда:

(1) $H \triangleleft N_G(H)$;

(2) если $H \leq K \leq G$ и $H \triangleleft K$, то $K \leq N_G(H)$;

(3) $N_G(H)$ — наибольшая подгруппа группы G , в которой H нормальна;

(4) если $H \triangleleft G$, то $N_G(H) = G$. Обратно, если $N_G(H) = G$, то $H \triangleleft G$;

(5) $C_G(T) \triangleleft N_G(T)$ для любого непустого подмножества T группы G .

(1) Если $x \in N_G(H)$, то $H^x = H$ и $H \triangleleft N_G(H)$.

(2) Пусть $H \leq K \leq G$ и $H \triangleleft K$. Если $x \in K$, то $H^x = H$ и $x \in N_G(H)$, т.е. $K \leq N_G(H)$.

(3) Из (1) следует, что $H \triangleleft N_G(H)$, а из (2) получаем, что $N_G(H)$ содержит любую подгруппу, в которой H нормальна. Поэтому $N_G(H)$ — наибольшая подгруппа, содержащая подгруппу H в качестве нормальной подгруппы.

Утверждение (4) следует из (3).

(5) Если $x \in N_G(T)$, то $T = T^x$. Поэтому $C_G(T)^x = C_G(T)$ по лемме 2.8(3) и $C_G(T) \triangleleft N_G(T)$.

ЛЕММА 1.53. Пусть H — нормальная подгруппа группы G . Тогда:

(1) если $L \leq G$, то $HL \leq G$ и $H \cap L \triangleleft L$;

(2) если $L \triangleleft G$, то $HL \triangleleft G$ и $H \cap L \triangleleft G$;

(3) $C_G(H) \triangleleft G$;

(4) $Z(H) \triangleleft G$.

(1) Если $L \leq G$, то $HL = LH$ и $HL \leq G$ по теореме 5.9. Так как

$$(H \cap L)^l = H^l \cap L^l = H \cap L$$

для всех $l \in L$, то $H \cap L \triangleleft L$.

(2) Если $L \triangleleft G$, то, очевидно, $HL \triangleleft G$ и $H \cap L \triangleleft G$.

(3) Так как $C_G(H) \triangleleft N_G(H)$ по лемме 6.3(5) и $N_G(H) = G$ по лемме 6.3(4), то $C_G(H) \triangleleft G$.

(4) Так как $Z(H) = H \cap C_G(H)$ по лемме 2.9(5), то $Z(H) \triangleleft G$ по (2).

Простая группа. В каждой группе G тривиальные подгруппы (единичная подгруппа E и сама группа G) являются нормальными подгруппами. Если в неединичной группе G нет других нормальных подгрупп, то группа G называется *простой*. Единичную группу E считают непростой группой.

ТЕОРЕМА 1.54. *Абелева простая группа является циклической группой простого порядка. Обратно, каждая группа простого порядка будет простой абелевой группой.*

Очевидно, что в абелевых группах все подгруппы нормальны. Поэтому в простой абелевой группе совокупность всех подгрупп исчерпывается тривиальными подгруппами.

Пусть G — абелева простая группа и $G \neq E$. Тогда в G существует неединичный элемент a и циклическая подгруппа $\langle a \rangle$ нормальна в G . Так как G простая, то $\langle a \rangle = G$ и G — циклическая группа. По теореме 3.4 бесконечная циклическая группа $\langle a \rangle$ обладает нетривиальной подгруппой, например, $\langle a^2 \rangle$, поэтому она не простая.

Пусть $G = \langle a \rangle$ — конечная циклическая группа, $|a| = n$ и p — простое число, делящее n . Элемент a^p имеет порядок n/p , поэтому циклическая подгруппа $\langle a^p \rangle$, порождённая элементом a^p , отлична от G . Но тогда она нормальна в G . Это возможно лишь в случае, когда $\langle a^p \rangle = E$ — единичная подгруппа, т.е. когда $n = p$ — простое число.

Обратно, пусть G — группа простого порядка p . По теореме 5.6 в группе G все подгруппы тривиальны и G — простая группа.

Существуют неабелевы простые группы, например, знакопеременная группа A_n степени n является простой неабелевой группой для любого $n > 4$.

Факторгруппа. Пусть H — нормальная подгруппа группы G . Обозначим через $\overline{G}$ совокупность всех левых смежных классов группы G по подгруппе H , т.е. $\overline{G} = \{xH \mid x \in G\}$. Положим

$$(xH)(yH) = xyH. \quad <1>$$

Проверим, что это равенство задает алгебраическую операцию на множестве $\overline{G}$. Если $xH = x_1H$, $yH = y_1H$ для некоторых $x_1, y_1 \in G$, то $x_1 = xh$, $y_1 = yg$, h и $g \in H$. Поэтому

$$(x_1H)(y_1H) = x_1y_1H = (xh)(yg)H = xy(y^{-1}hy)gH = xyH,$$

т.к. $y^{-1}hy \in H$ по теореме 6.1. Таким образом, равенство $<1>$ не зависит от выбора представителей смежных классов и каждой паре xH , yH ставится в соответствие единственный элемент xyH .

Ясно, что предложенная операция $<1>$ определена на $\overline{G}$ и ассоциативна. Элемент $eH = H$ будет единичным, а элемент $a^{-1}H$ — обратным к элементу aH . Таким образом, доказана следующая

ТЕОРЕМА 1.55. *Совокупность $\overline{G} = \{xH \mid x \in G\}$ всех левых смежных классов группы G по нормальной подгруппе H с операцией*

$$(xH)(yH) = xyH$$

образует группу с единичным элементом $eH = H$ и обратным элементом $(aH)^{-1} = a^{-1}H$. $\square$

Группа $\overline{G}$ называется *факторгруппой* группы G по подгруппе H и обозначается через G/H .

Если H не будет нормальной подгруппой, то равенство $\langle 1 \rangle$ не будет задавать алгебраическую операцию, и совокупность левых смежных классов не будет группой.

Очевидно, что если группа G конечна, то факторгруппа группы G по любой нормальной подгруппе H также будет конечной группой порядка, равного индексу подгруппы H в группе G , т.е.

$$|G/H| = |G : H| = |G| / |H|.$$

ЛЕММА 1.56. Если $G/Z(G)$ циклическая, то G абелева.

Пусть $G/Z(G) = \langle gZ(G) \rangle$ циклическая и a, b — произвольные элементы группы G . Тогда

$$a = g^k z_1, \quad b = g^l z_2, \quad z_1, z_2 \in Z(G), \quad k, l \in \mathbb{Z}$$

и

$$ab = g^k z_1 g^l z_2 = g^k g^l z_1 z_2 = g^l g^k z_2 z_1 = g^l z_2 g^k z_1 = ba.$$

ТЕОРЕМА 1.57. Все факторгруппы бесконечной циклической группы $\langle a \rangle$ исчерпываются бесконечной циклической группой $\langle a \rangle / E \simeq \langle a \rangle$ и конечными циклическими группами $\langle a \langle a^m \rangle \rangle$ порядка m для каждого натурального m .

По теореме 3.4, с. 23, все подгруппы бесконечной циклической группы $A = \langle a \rangle$ исчерпываются единичной подгруппой E и бесконечными циклическими подгруппами $M = \langle a^m \rangle$, $m \in \mathbb{N}$. Так как каждая циклическая группа абелева, то в ней любая подгруппа нормальна. Факторгруппа A/E очевидно будет бесконечной циклической группой, изоморфной A .

Так как $A = \{a^k \mid k \in \mathbb{Z}\}$, то факторгруппа A/M состоит из смежных классов $a^k M$, $k \in \mathbb{Z}$. Если два смежных класса совпадут $a^s M = a^t M$, то $a^{s-t} \in M$ и $s - t$ кратно m . Отсюда следует, что смежные классы

$$M, aM, a^2M, \dots, a^{m-1}M$$

попарно различны. Кроме того, для любого $a^t M \in A/M$ имеем:

$$t = mq + r, \quad 0 \leq r < m \quad \text{и} \quad a^t M = a^{mq} a^r M = a^r M.$$

Таким образом,

$$A/M = \{M, aM, a^2M, \dots, a^{m-1}M\} = \langle aM \rangle,$$

т.е. факторгруппа A/M будет конечной циклической группой порядка m .

ТЕОРЕМА 1.58. Все факторгруппы конечной циклической группы $\langle a \rangle$ порядка n исчерпываются конечными циклическими группами $\langle a \langle a^m \rangle \rangle$ порядка m для каждого натурального m делящего n .

По теореме 3.7, с. 23, все подгруппы конечной циклической группы $A = \langle a \rangle$ порядка n исчерпываются циклическими подгруппами $M = \langle a^m \rangle$ порядка n/m для каждого натурального m , делящего n . Легко проверить, что

$$A/M = \langle aM \rangle = \{aM, a^2M, \dots, a^{m-1}M, M\},$$

т.е. A/M будет циклической группой порядка m , порожденной элементом $a \langle a^m \rangle$.

Теорема о соответствии. Условимся через $\mathbf{S}(G, H)$ обозначать совокупность всех подгрупп группы G , содержащих подгруппу H . В частности, $\mathbf{S}(G, E) = \mathbf{S}(G)$ — совокупность всех подгрупп группы G , а $\mathbf{S}(G, G) = \{G\}$.

ТЕОРЕМА 1.59. (ТЕОРЕМА О СООТВЕТСТВИИ) Пусть H — нормальная подгруппа группы G . Тогда:

(1) если U — подгруппа группы G и $H \leq U$, то $\bar{U} = U/H$ — подгруппа факторгруппы $\bar{G} = G/H$;

(2) каждая подгруппа факторгруппы $\bar{G} = G/H$ имеет вид $\bar{V} = V/H$, где V — подгруппа группы G и $H \leq V$;

(3) отображение $\varphi : U \mapsto \bar{U}$ является биекцией множества $\mathbf{S}(G, H)$ на множество $\mathbf{S}(\bar{G})$;

(4) если $N \in \mathbf{S}(G, H)$, то N — нормальная подгруппа группы G тогда и только тогда, когда N/H — нормальная подгруппа факторгруппы G/H .

(1) Пусть $U \in \mathbf{S}(G, H)$ и пусть $\bar{U} = \{uH \mid u \in U\}$ — совокупность смежных классов группы U по своей нормальной подгруппе H . Если $u_1H, u_2H \in \bar{U}$, то $u_1, u_2 \in U$, а так как U — подгруппа, то $u_1u_2 \in U$ и $u_1^{-1} \in U$. Поэтому,

$$(u_1H)(u_2H) = u_1u_2H \in \bar{U}, \quad (u_1H)^{-1} = u_1^{-1}H \in \bar{U}$$

и по критерию подгруппы совокупность $\bar{U}$ — подгруппа группы $\bar{G}$.

(2) Пусть $\bar{V}$ — произвольная подгруппа из $\bar{G}$. Тогда $\bar{V}$ состоит из некоторых смежных классов группы G по подгруппе H . Обозначим через V множество всех тех элементов группы G , из которых состоят смежные классы, принадлежащие $\bar{V}$, т.е. $V = \{x \in G \mid xH \in \bar{V}\}$. Если $v_1, v_2 \in V$, то $v_1H, v_2H \in \bar{V}$, а так как $\bar{V}$ — подгруппа, то

$$(v_1H)(v_2H) = v_1v_2H \in \bar{V} \quad \text{и} \quad (v_1H)^{-1} = v_1^{-1}H \in \bar{V}.$$

Следовательно, $v_1v_2 \in V$ и $v_1^{-1} \in V$, т.е. V — подгруппа группы G . Ясно, что $H \leq V$.

(3) Отображение $\varphi : U \mapsto \bar{U}$ будет сюръекцией по (2). Докажем, что φ — инъекция. Пусть U и V — подгруппы, содержащие H , и предположим, что подгруппы $\bar{U} = \{uH \mid u \in U\}$ и $\bar{V} = \{vH \mid v \in V\}$ совпадают. Тогда для любого элемента $u \in U$ существует элемент $v \in V$ такой, что $uH = vH$. Поэтому $v^{-1}u \in H \leq V \cap U$. Теперь $u \in V$ и $U \leq V$. Аналогично проверяется обратное включение. Следовательно $U = V$ и φ — инъекция.

(4) Если $N \triangleleft G$, $N \in \mathbf{S}(G, H)$, то

$$(gH)^{-1}(nH)(gH) = g^{-1}ngH \in N/H$$

для всех $g \in G$, $n \in N$. Поэтому $\bar{N} = N/H \triangleleft \bar{G}$. Обратно, если $\bar{N} \triangleleft \bar{G}$, то

$$g^{-1}ngH = (gH)^{-1}(nH)(gH) \in \bar{N}$$

и $g^{-1}ng \in N$, значит $N \triangleleft G$.

Совокупность всех нормальных подгрупп группы G обозначим через $\mathbf{Sn}(G)$.

ТЕОРЕМА 1.60. Множество $\mathbf{Sn}(G)$ с бинарным отношением $\leq$ является подрешеткой решетки $\mathbf{S}(G)$ всех подгрупп группы G .

В теореме 2.7, с. 19, доказано, что множество $\mathbf{S}(G)$ с бинарным отношением $\leq$ является решеткой. Ясно, что $\mathbf{Sn}(G) \subseteq \mathbf{S}(G)$. По лемме 6.4(2)

$H \cap L \triangleleft G$ и $\langle H \cup L \rangle = HL \triangleleft G$ для всех $H, L \triangleleft G$, поэтому $H \cap L = H \wedge L$, $HL = H \vee L$ и $\mathbf{Sn}(G)$ — подрешетка решетки $\mathbf{S}(G)$.

Собственная нормальная подгруппа H неединичной группы G называется *максимальной нормальной подгруппой* группы G , если из условий: $H \leq K \triangleleft G$ следует, что $H = K$, либо $K = G$. У единичной группы E максимальной нормальной подгруппой считают саму группу E .

ТЕОРЕМА 1.61. (1) Если H — максимальная нормальная подгруппа неединичной группы G , то факторгруппа G/H является простой группой.

(2) Если H — нормальная подгруппа группы G и факторгруппа G/H простая, то H — максимальная нормальная подгруппа группы G .

(1) Предположим, что факторгруппа G/H непростая. Тогда существует нетривиальная нормальная подгруппа K/H группы G/H . По теореме 6.10(4) подгруппа K нормальна в G и $K \neq G$, $K \neq H$, $H \leq K$. Противоречие, с тем, что H — максимальная нормальная подгруппа группы G .

(2) Пусть H — нормальная подгруппа группы G и факторгруппа G/H простая. Предположим, что существует нормальная подгруппа L группы G такая, что $H \leq L$, $H \neq L$, $L \neq G$. Тогда L/H — нетривиальная нормальная подгруппа факторгруппы G/H , т.е. факторгруппа G/H непростая. Противоречие.

ТЕОРЕМА 1.62. Если p — наименьший простой делитель порядка конечной группы, то каждая подгруппа индекса p нормальна в группе.

Пусть G — конечная группа, p — наименьший простой делитель $|G|$ и H — подгруппа индекса p . Предположим, что подгруппа H не является нормальной подгруппой группы G . По теореме 6.1 существует элемент $x \in G$ такой, что $H \neq H^x$. Так как $|H| / |H \cap H^x| \neq 1$ и делит $|G|$, то $|H| / |H \cap H^x| \geq p$ и

$$\begin{aligned} |G| &\geq |HH^x| = |H| |H^x| / |H \cap H^x| \geq \\ &\geq |H| p = |H| |G : H| = |G| \end{aligned}$$

по теореме 5.10. Поэтому $G = HH^x$, что противоречит лемме 5.12.

ПРИМЕР 1.21. Подгруппа индекса 2 нормальна в группе. В частности, $A_n \triangleleft S_n$. $\square$

ПРИМЕР 1.22. Найти все факторгруппы группы S_3 .

Среди подгрупп группы S_3 со своими сопряженными совпадают подгруппы

$$E = H_1, S_3 = H_2, H = H_6 = \langle (123) \rangle,$$

см. пример 5.22. По теореме 6.1 эти три подгруппы нормальны в S_3 .

E — единичная подгруппа, поэтому

$$S_3/E = \{E, (12)E, (13)E, (23)E, (123)E, (132)E\}$$

изоморфна S_3 .

Так как

$$S_3/H_2 = S_3/S_3 = \{S_3\},$$

то S_3/S_3 — группа, изоморфная единичной группе.

Осталось рассмотреть нормальную подгруппу $H = H_6 = \langle (123) \rangle$. Ее порядок равен 3, а порядок S_3/H равен 2. Поэтому S_3/H — циклическая

группа порядка 2. Смежные классы S_3 по H исчерпываются двумя классами: H и $(12)H$. Таким образом, группа S_3 имеет три факторгруппы:

$$S_3/E \simeq S_3, S_3/S_3 \simeq E, S_3/H = \{H, (12)H\} = \langle (12)H \rangle.$$

□

ПРИМЕР 1.23. В аддитивной группе $\mathbb{Z}$ целых чисел рассмотрим подгруппу $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\}$ чисел, кратных 5. Так как $\mathbb{Z}$ абелева, то $5\mathbb{Z} \triangleleft \mathbb{Z}$. Смежные классы $\mathbb{Z}$ по $5\mathbb{Z}$ имеют вид: $i + 5\mathbb{Z}$, где $i = 0, 1, 2, 3, 4$. Факторгруппа

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

состоит из пяти элементов. Нулевым элементом будет $5\mathbb{Z}$. Сложение в аддитивной факторгруппе G/H определяется равенством

$$(a + H) + (b + H) = (a + b) + H.$$

Например,

$$(2 + 5\mathbb{Z}) + (4 + 5\mathbb{Z}) = 6 + 5\mathbb{Z} = 1 + 5\mathbb{Z}.$$

Вычисляя остальные суммы, можно было бы составить таблицу сложения для факторгруппы. Ясно, что $\mathbb{Z}/5\mathbb{Z} = \langle 1 + 5\mathbb{Z} \rangle$ — циклическая группа порядка 5. □

1.7. Силовские подгруппы конечных групп

По теореме Лагранжа порядок каждой подгруппы делит порядок конечной группы. Обратное утверждение не всегда верно, т.е. если натуральное число d делит порядок конечной группы G , то в группе G может и не быть подгруппы порядка d .

ПРИМЕР 1.24. Знакопеременная группа A_4 порядка 12 не содержит подгруппы порядка 6.

Допустим противное, пусть H — подгруппа порядка 6 в группе A_4 . Тогда $|A_4 : H| = 2$ и $H \triangleleft A_4$ по примеру 6.14. Группа A_4 содержит подгруппы

$$K_1 = \langle (234) \rangle; K_2 = \langle (134) \rangle.$$

Если $K_i \not\subseteq H$, то $H \cap K_i = E$ и $|HK_i| = |H| |K_i| = 18$, противоречие. Поэтому $K_1 K_2 \subseteq H$, а т.к. $K_1 \cap K_2 = E$, то $|K_1 K_2| = 9$. Противоречие. Поэтому допущение неверно и группа A_4 не содержит подгруппы порядка 6. □

Вполне естественно возникает вопрос: для каких делителей d порядка конечной группы имеется подгруппа порядка d ?

Положительный ответ на этот вопрос в случае, когда d — степень простого числа, дает теорема Силова. Для доказательства теоремы Силова потребуется следующая

ЛЕММА 1.63. Если порядок конечной абелевой группы G делится на простое число p , то в группе G существует элемент порядка p .

Предположим противное, т.е. допустим, что существует абелева группа G порядка n , простое число p делит n и в группе G нет элементов порядка p . Пусть $G = \{a_1, \dots, a_n\}$.

Если p делит $|a_i|$ для некоторого i , то $a_i^{|a_i|/p}$ — элемент порядка p , противоречие. Поэтому все элементы группы G имеют порядки, не делящиеся на p . По теореме 1.42, с. 34,

$$|\langle a_1 \rangle \langle a_2 \rangle| = \frac{|\langle a_1 \rangle| |\langle a_2 \rangle|}{|\langle a_1 \rangle \cap \langle a_2 \rangle|}$$

не делится на p .

Так как группа G абелева, то $A_2 = \langle a_1 \rangle \langle a_2 \rangle$ — подгруппа по теореме 1.41, с. 34, и к произведению $A_2 \langle a_3 \rangle$ можно вновь применить теорему 1.42, с. 34. По этой теореме

$$|A_2 \langle a_3 \rangle| = \frac{|A_2| |\langle a_3 \rangle|}{|A_2 \cap \langle a_3 \rangle|}$$

не делится на p .

Затем $A_2 \langle a_3 \rangle$ обозначаем через A_3 и опять получаем, что $|A_3 \langle a_4 \rangle|$ не делится на p . Через конечное число шагов приходим к выводу, что $|A_{n-1} \langle a_n \rangle|$ не делится на p . Но

$$A_{n-1} = \langle a_1 \rangle \dots \langle a_{n-1} \rangle$$

и $A_{n-1} \langle a_n \rangle = G$, т.е. получаем, что $|G|$ не делится на p . Противоречие. Значит, допущение неверно и лемма справедлива.

Пусть p — простое число. p -Группой называют конечную группу, порядок которой есть степень числа p . Конечная группа называется *примарной*, если она является p -группой для некоторого простого p .

ТЕОРЕМА 1.64. (СИЛОВ) Пусть конечная группа G имеет порядок $p^m s$, где p — простое число и p не делит s . Тогда справедливы следующие утверждения:

(1) в группе G существует подгруппа порядка p^i для каждого $i = 1, 2, \dots, m$;

(2) если H — p -подгруппа группы G и P — подгруппа порядка p^m , то существует такой элемент $a \in G$, что $H \leq P^a$;

(3) любые две подгруппы порядка p^m сопряжены в группе G ;

(4) число подгрупп порядка p^m в группе G сравнимо с единицей по модулю p и делит s .

(1) Доказательство проведем индукцией по $|G|$. По индукции считаем, что для всех групп, порядок которых меньше порядка G утверждение (1) теоремы выполняется. Рассмотрим два случая.

СЛУЧАЙ 1. ПОРЯДОК ЦЕНТРА $Z(G)$ ДЕЛИТСЯ НА p .

Так как $Z(G)$ — абелева группа, то к $Z(G)$ применима лемма 1.63. По этой лемме в $Z(G)$ есть элемент z порядка p . Так как $N = \langle z \rangle$ — нормальная подгруппа группы G порядка p , то факторгруппа G/N имеет порядок $p^{m-1}s < |G|$ и по индукции в группе $G/N = \overline{G}$ имеется подгруппа $\overline{P}_i$ порядка p^i для каждого $i = 1, 2, \dots, m-1$. По теореме о соответствии в группе G имеется подгруппа P_i такая, что $P_i \geq N$ и $P_i/N = \overline{P}_i$. Теперь $|P_i| = p^{i+1}$, где $i = 1, 2, \dots, m-1$. Итак, в группе G имеется подгруппа N порядка p и подгруппы $P_1, P_2, \dots, P_{m-1}$ порядков $p^2, p^3, \dots, p^m$ соответственно.

СЛУЧАЙ 2. ПОРЯДОК ЦЕНТРА $Z(G)$ ГРУППЫ G НЕ ДЕЛИТСЯ НА p .

Рассмотрим разложение группы G в объединение различных классов сопряженных элементов

$$G = K_1 \cup K_2 \cup \dots \cup K_d, \quad < 1 >$$

где

$$K_i = x_i^G = \{x_i^g \mid g \in G\}$$

— класс сопряженных с x_i элементов. По лемме 1.9 различные классы сопряженных элементов имеют пустое пересечение, а по следствию 5 число элементов в классе x_i^G равно индексу централизатора $C_G(x_i)$. Пусть

$$k_i = |K_i| = |G : C_G(x_i)|.$$

Централизатор каждого элемента из центра совпадает с группой G . И обратно, если централизатор некоторого элемента совпадает с группой, то этот элемент попадает в центр G . Поэтому из $<1>$ получаем

$$|G| = \underbrace{1 + 1 + \dots + 1}_{|Z(G)|} + k_c + k_{c+1} + \dots + k_d, \quad < 2 >$$

где $k_j > 1$ для каждого $j \geq c$. Если все числа $k_c, \dots, k_d$ делятся на p , то из $<2>$ следует, что $|Z(G)|$ делится на p , что противоречит рассматриваемому случаю. Итак, существует k_f , где $f \geq c$ такое, что p не делит k_f . Поскольку $k_f = |G : C_G(x_f)|$, то

$$|C_G(x_f)| = p^m s_1 < |G|,$$

где $s_1 = s/k_f$ — целое число и p не делит s_1 . Теперь к группе $C_G(x_f)$ применима индукция. По индукции в группе $C_G(x_f)$ существует подгруппа порядка p^i для каждого $i = 1, 2, \dots, m$. Эта подгруппа будет искомой и для группы G .

(2) Рассмотрим разложение группы G на двойные смежные классы по подгруппам P и H :

$$G = Px_1H \cup Px_2H \cup \dots \cup Px_tH. \quad < 3 >$$

Зададим отображение

$$\varphi_i : gx_ih \mapsto x_i^{-1}gx_ih, \quad g \in P, h \in H,$$

переводящее элементы двойного смежного класса Px_iH в элементы произведения подгрупп $x_i^{-1}Px_i = P^{x_i}$ и H . Легко проверить, что отображение φ_i взаимно однозначно, поэтому, используя теорему 1.42, получаем:

$$|Px_iH| = |P^{x_i}H| = \frac{|P^{x_i}| |H|}{|P^{x_i} \cap H|} = \frac{p^m p^b}{|P^{x_i} \cap H|},$$

где $p^b = |H|$. Так как $P^{x_i} \cap H$ есть подгруппа в H , то по теореме Лагранжа $|P^{x_i} \cap H|$ делит p^b и $p^b / |P^{x_i} \cap H|$ — целое число. Из $<3>$ теперь получаем:

$$p^m s = \sum_{i=1}^t |Px_iH| = \sum_{i=1}^t p^m \frac{p^b}{|P^{x_i} \cap H|} = p^m \sum_{i=1}^t \frac{p^b}{|P^{x_i} \cap H|}.$$

Сокращая обе части на p^m получим:

$$s = \sum_{i=1}^t \frac{p^b}{|P^{x_i} \cap H|}. \quad < 4 >$$

Так как s взаимно просто с p , а $p^b / |P^{x_i} \cap H|$ — целое число, являющееся

степенью p , то в правой части $< 4 >$ существует слагаемое, равное единице. Пусть, например, $p^b = |P^{x_j} \cap H|$, где $1 \leq j \leq t$. Тогда $H \leq P^{x_j}$.

(3) Пусть P_1 и P_2 — подгруппы порядка p^m . По (2) существует элемент $a \in G$ такой, что $P_1 \leq P_2^a$. Так как $|P_1| = |P_2^a|$, то $P_1 = P_2^a$.

(4) Пусть G — группа порядка $p^m s$, $(p, s) = 1$, P — подгруппа порядка p^m и $N = N_G(P)$ — нормализатор подгруппы P в группе G . Рассмотрим разложение группы G на двойные смежные классы по P и N :

$$G = Px_1N \cup Px_2N \cup \dots \cup Px_tN. \quad < 5 >$$

Отображение

$$\varphi_i : gx_ih \mapsto x_i^{-1}gx_ih, \quad g \in P, h \in N,$$

будет взаимно однозначным отображением Px_iN на $P^{x_i}N$. Теперь из $< 5 >$ получаем:

$$|G| = \sum_{i=1}^t |P^{x_i}N| = \sum_{i=1}^t \frac{|P^{x_i}| |N|}{|P^{x_i} \cap N|} = |N| \sum_{i=1}^t \frac{|P^{x_i}|}{|P^{x_i} \cap N|}.$$

Положим $|G : N| = \rho$. Элемент x_1 можно выбрать единичным, поэтому $Px_1N = P^{x_1}N = N$ и $P^{x_1} \cap N = P$. Теперь

$$\rho = 1 + \sum_{i=2}^t |P^{x_i}| / |P^{x_i} \cap N|. \quad < 6 >$$

Проверим, что под знаком суммы нет слагаемых равных 1. Допустим противное, т.е. что для некоторого $j \geq 2$ имеем равенство $|P^{x_j}| = |P^{x_j} \cap N|$. Это означает, что $P^{x_j} \leq N$ и подгруппа N содержит две подгруппы P и P^{x_j} порядка p^m . По (3) существует элемент $y \in N$ такой, что $P = P^{x_j y}$. Но тогда $x_j y \in N$, а так как $y \in N$, то и $x_j \in N$. Но это возможно только при $j = 1$, противоречие. Значит, допущение неверно и в равенстве $< 6 >$ под знаком суммы все слагаемые отличны от единицы. Поскольку каждое слагаемое есть степень простого p , то из равенства $< 6 >$ получаем сравнение $\rho \equiv 1 \pmod{p}$. По (3) все подгруппы порядка p^m группы G сопряжены между собой, а по следствию 5 число подгрупп, сопряженных с P равно ρ . Поскольку $P \leq N$, то ρ делит s .

Силовской p -подгруппой конечной группы G называют такую p -подгруппу, индекс которой не делится на p . Непосредственно из теоремы получаем

СЛЕДСТВИЕ. Пусть конечная группа G имеет порядок $p^m s$, где p — простое число и p не делит s . Тогда:

- (1) существует силовская p -подгруппа и её порядок равен p^m ;
- (2) каждая p -подгруппа содержится в некоторой силовской p -подгруппе;
- (3) любые две силовские p -подгруппы сопряжены;
- (4) число силовских p -подгрупп сравнимо с единицей по модулю p и делит s . $\square$

ТЕОРЕМА 1.65. Для конечной группы G и её силовской p -подгруппы P справедливы следующие утверждения:

- (1) если $K \triangleleft G$, то $P \cap K$ — силовская p -подгруппа в K , а PK/K — силовская p -подгруппа в G/K ;

$$(2) N_{G/K}(PK/K) = N_G(P)K/K;$$

(3) если $K_1 \triangleleft G$ и $K_2 \triangleleft G$, то

$$K_1K_2 \cap P = (K_1 \cap P)(K_2 \cap P)$$

и

$$K_1P \cap K_2P = (K_1 \cap K_2)P;$$

(4) пусть $p_1, p_2, \dots, p_n$ — все простые делители порядка группы G , $p_i \neq p_j$ при $i \neq j$, и пусть $P_1, P_2, \dots, P_n$ — соответствующие им силовские подгруппы. Тогда

$$G = \langle P_1 \cup P_2 \cup \dots \cup P_n \rangle,$$

а если $n = 2$, то $G = P_1P_2$.

(1) Так как $|P| = p^m$ и p не делит $|G : P|$, то $P \cap K$ — p -группа, а из того, что

$$|PK| = |P| |K| / |P \cap K|,$$

следует

$$|PK : P| = |K : K \cap P|.$$

Из теоремы 1.39 получаем, что

$$|G : P| = |G : PK| |PK : P|$$

и $|K : K \cap P|$ не делится на p . Значит $K \cap P$ — силовская p -подгруппа в K .

Поскольку $|PK/K| = |P/P \cap K|$, то PK/K — p -группа, а так как

$$|G/K : PK/K| = |G : PK| = |G : P| / |PK : P|$$

не делится на p , то PK/K — силовская p -подгруппа в G/K .

(2) Для $x \in N_G(P)$ получаем

$$(x^{-1}K)(PK/K)(xK) = P^xK/K = PK/K,$$

т.е. $N_G(P)K/K \leq N_{G/K}(PK/K)$. Обратно, если $yK \in N_{G/K}(PK/K)$, то $P^yK = PK$. Теперь P и P^y — силовские подгруппы в PK , которые по следствию 7 сопряжены в PK , т.е. существует элемент $ak \in PK$, $a \in P$, $k \in K$, такой, что $P^y = P^{ak} = P^k$. Теперь $yk^{-1} \in N_G(P)$ и $y \in N_G(P)K$, т.е.

$$N_{G/K}(PK/K) \leq N_G(P)K/K.$$

(3) Если

$$ab \in (K_1 \cap P)(K_2 \cap P), \quad a \in K_1 \cap P, \quad b \in K_2 \cap P,$$

то $ab \in K_1K_2 \cap P$ и

$$(K_1 \cap P)(K_2 \cap P) \leq K_1K_2 \cap P.$$

Если $M \leq G$, то пусть $|M|_p$ означает наивысшую степень p , делящую порядок M . По следствию 7 $|M|_p$ — порядок силовской p -подгруппы из M . Из (1) следует, что

$$|K_i \cap P| = |K_i|_p, \quad i = 1, 2; \quad |K_1K_2 \cap P| = |K_1K_2|_p.$$

Поэтому

$$\begin{aligned} |(K_1 \cap P)(K_2 \cap P)| &= |K_1|_p |K_2|_p / |K_1 \cap K_2|_p = \\ &= |K_1K_2|_p = |K_1K_2 \cap P| \end{aligned}$$

и

$$(K_1 \cap P)(K_2 \cap P) = K_1K_2 \cap P.$$

Если

$$ab \in (K_1 \cap K_2)P, \quad a \in K_1 \cap K_2, \quad b \in P,$$

то

$$ab \in (K_1 \cap P)(K_2 \cap P) \quad \text{и} \quad (K_1 \cap K_2)P \leq K_1P \cap K_2P.$$

Обратно, пусть

$$a_1b_1 = a_2b_2 \in K_1P \cap K_2P,$$

где $a_1 \in K_1, a_2 \in K_2, b_1$ и $b_2 \in P$. Тогда

$$a_2^{-1}a_1 = b_2b_1^{-1} \in K_1K_2 \cap P.$$

Поскольку уже доказано, что

$$K_1K_2 \cap P = K_2K_1 \cap P = (K_2 \cap P)(K_1 \cap P),$$

то $a_2^{-1}a_1 = c_2c_1$, где

$$c_2 \in K_2 \cap P, c_1 \in K_1 \cap P.$$

Теперь

$$a_1c_1^{-1} = a_2c_2 \in K_1 \cap K_2 \quad \text{и} \quad a_1b_1 = a_1c_1^{-1}c_1b_1 \in (K_1 \cap K_2)P.$$

Следовательно,

$$K_1P \cap K_2P = (K_1 \cap K_2)P.$$

(4) Пусть

$$H = \langle P_1 \cup P_2 \cup \dots \cup P_n \rangle.$$

Тогда $|P_i|$ делит $|H|$ для каждого $i = 1, 2, \dots, n$ и поэтому

$$|G| = |P_1| |P_2| \dots |P_n|$$

делит $|H|$, т.е. $H = G$. Для $n = 2$ по теореме 1.42 имеем $|G| = |P_1P_2|$, откуда $G = P_1P_2$.

ЛЕММА 1.66. (ФРАТТИНИ) Если K — нормальная подгруппа конечной группы G и P — силовская p -подгруппа из K , то $G = N_G(P)K$.

Пусть g — произвольный элемент из G . Так как $P \leq K \triangleleft G$, то $P^g \leq K^g = K$ и по следствию 7 подгруппы P и P^g сопряжены в K . Поэтому, существует элемент $k \in K$ такой, что $P = P^{gk}$, откуда

$$gk \in N_G(P) \quad \text{и} \quad g \in N_G(P)k^{-1} \subseteq N_G(P)K.$$

Таким образом, $G = N_G(P)K$.

ЛЕММА 1.67. Каждая подгруппа конечной группы, содержащая нормализатор некоторой силовской подгруппы, самонормализуема.

Пусть P — силовская подгруппа группы G и H — подгруппа группы G , содержащая $N_G(P)$. Так как $H \triangleleft N_G(H)$, то по лемме Фраттини

$$N_G(H) = HN_G(P) = H.$$

ЛЕММА 1.68. Пусть P — p -подгруппа конечной группы G , $N \triangleleft G$ и p не делит $|N|$. Тогда

$$N_{G/N}(PN/N) = N_G(P)N/N.$$

Ясно, что

$$N_G(P)N/N \leq N_{G/N}(PN/N).$$

По условию подгруппа P является силовской подгруппой в PN . Пусть

$$N_{G/N}(PN/N) = A/N.$$

Тогда $PN \triangleleft A$ и по лемме Фраттини $A = N_G(P)N$.

ПРИМЕР 1.25. Симметрическая группа S_6 степени 6 имеет порядок $6! = 2^4 \cdot 3^2 \cdot 5$. По теореме Силова S_6 содержит подгруппы порядков $2, 2^2, 2^3, 2^4, 3, 3^2, 5$. Силовская 2-подгруппа имеет порядок 2^4 , силоvская 3-подгруппа имеет порядок 3^2 и силоvская 5-подгруппа имеет порядок 5. $\square$

ПРИМЕР 1.26. Группа порядка 15 циклическая.

Пусть G — группа порядка 15. В группе G имеется подгруппа P порядка 3 и подгруппа Q порядка 5. По следствию 7 число силоvских 3-подгрупп имеет вид $1 + 3k$ для некоторого неотрицательного целого k и делит 5. Поэтому в группе имеется только одна подгруппа порядка 3. Так как любые две силоvские 3-подгруппы сопряжены, то $P \triangleleft G$. Аналогично, число силоvских 5-подгрупп равно $1 + 5t$ и делит 3. Поэтому $Q \triangleleft G$. Так как $P = \langle x \rangle$ и $Q = \langle y \rangle$ — циклические подгруппы простых порядков, то группа $G = \langle x \rangle \langle y \rangle$ по теореме 1.42. Теперь для любых $a \in P, b \in Q$ имеем:

$$\begin{aligned} aba^{-1}b^{-1} &= (aba^{-1})b^{-1} \in Q^{a^{-1}}Q = Q, \\ aba^{-1}b^{-1} &= a(ba^{-1}b^{-1}) \in PP^{b^{-1}} = P, \end{aligned}$$

поэтому

$$aba^{-1}b^{-1} \in P \cap Q = 1, aba^{-1}b^{-1} = 1$$

и $ab = ba$. Следовательно, группа G абелева. Теперь ясно, что $G = \langle xy \rangle$ — циклическая группа. $\square$

ГЛАВА 2. ГОМОМОРФИЗМЫ И ПРОИЗВЕДЕНИЯ ГРУПП

2.1. Гомоморфизмы групп

Пусть G и Γ — мультипликативные группы. Отображение $\varphi : G \rightarrow \Gamma$ называется *гомоморфизмом* группы G в группу Γ , если

$$\varphi(xy) = \varphi(x)\varphi(y) \quad < 1 >$$

для любых x и $y \in G$.

Если M — подмножество группы G , то

$$\varphi(M) = \{\varphi(m) \mid m \in M\}$$

— образ M при гомоморфизме φ , а $\varphi(G)$ — образ гомоморфизма φ . Образ гомоморфизма φ также обозначают через $\text{Im}\varphi$.

Ядром гомоморфизма φ называется множество

$$\text{Ker}\varphi = \{x \in G \mid \varphi(x) = \varepsilon\},$$

где ε — единичный элемент группы Γ . Другими словами, в ядре собраны все элементы группы G , переходящие при отображении φ в единичный элемент группы Γ , т.е. $\text{Ker}\varphi = \varphi^{-1}(\{\varepsilon\})$.

ЛЕММА 2.1. Пусть $\varphi : G \rightarrow \Gamma$ — гомоморфизм группы G в группу Γ . Тогда:

(1) *единичный элемент e группы G переходит в единичный элемент ε группы Γ , т.е. $\varphi(e) = \varepsilon$;*

(2) *обратный элемент переходит в обратный, т.е. $\varphi(a^{-1}) = \varphi(a)^{-1}$ для всех $a \in G$;*

(3) *образ гомоморфизма является подгруппой группы Γ , т.е. $\text{Im}\varphi \leq \Gamma$;*

(4) *ядро гомоморфизма является нормальной подгруппой группы G , т.е. $\text{Ker}\varphi \triangleleft G$;*

(5) *тогда и только тогда $\varphi(g) = \varphi(h)$, где $g, h \in G$, когда $gh^{-1} \in \text{Ker}\varphi$.*

(1) Предположим, что $\varphi(e) = \varepsilon_1 \in \Gamma$. Так как ε — единица группы Γ , то $\varepsilon_1\varepsilon = \varepsilon_1$. Применяя $<1>$ к равенству $ee = e$, получаем, $\varepsilon_1\varepsilon_1 = \varepsilon_1$. Теперь $\varepsilon_1\varepsilon = \varepsilon_1\varepsilon_1$, откуда $\varepsilon = \varepsilon_1 = \varphi(e)$ — единица группы Γ .

(2) Так как $e = aa^{-1} = a^{-1}a$, то

$$\varepsilon = \varphi(e) = \varphi(a)\varphi(a^{-1}) = \varphi(a^{-1})\varphi(a)$$

и $\varphi(a^{-1}) = \varphi(a)^{-1}$.

(3) Если α и $\beta \in \text{Im}\varphi$, то существуют элементы a и $b \in G$ такие, что $\varphi(a) = \alpha$, $\varphi(b) = \beta$. Так как G — группа, то $ab \in G$ и $a^{-1} \in G$. Отсюда

$$\alpha\beta = \varphi(a)\varphi(b) = \varphi(ab) \in \text{Im}\varphi$$

и

$$\alpha^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \text{Im}\varphi,$$

т.е. $\text{Im}\varphi$ — подгруппа группы Γ .

(4) Если a и $b \in \text{Ker}\varphi$, то $\varphi(a) = \varepsilon = \varphi(b)$. Поэтому

$$\varphi(ab) = \varphi(a)\varphi(b) = \varepsilon, \quad \text{т.е.} \quad ab \in \text{Ker}\varphi.$$

Далее,

$$\varphi(a^{-1}) = \varphi(a)^{-1} = \varepsilon, \quad \text{т.е.} \quad a^{-1} \in \text{Ker} \varphi.$$

Значит, $\text{Ker} \varphi$ — подгруппа группы G .

Для произвольных элементов $g \in G$, $a \in \text{Ker} \varphi$ имеем:

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(g)^{-1}\varepsilon\varphi(g) = \varepsilon.$$

Поэтому $g^{-1}ag \in \text{Ker} \varphi$ и по теореме 1.51, с. 38, подгруппа $\text{Ker} \varphi$ нормальна в G .

(5) Пусть $g, h \in G$ и $\varphi(g) = \varphi(h)$. Тогда

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = \varepsilon \quad \text{и} \quad gh^{-1} \in \text{Ker} \varphi.$$

Обратно, если $gh^{-1} \in \text{Ker} \varphi$, то

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = \varepsilon$$

и $\varphi(g) = \varphi(h)$.

Гомоморфизм $\varphi : G \rightarrow \Gamma$ называется *мономорфизмом*, если $\text{Ker} \varphi = \{\varepsilon\}$. Из леммы 2.1 следует, что гомоморфизм φ является мономорфизмом тогда и только тогда, когда отображение φ — инъекция.

Если $\text{Im} \varphi = \Gamma$, то гомоморфизм $\varphi : G \rightarrow \Gamma$ называется *эпиморфизмом*. Ясно, что в этом случае φ — сюръекция.

Гомоморфизм, который одновременно является мономорфизмом и эпиморфизмом, будет *изоморфизмом*.

ЛЕММА 2.2. Пусть $\varphi : G \rightarrow \Gamma$ — гомоморфизм группы G в группу Γ . Тогда:

(1) если $H \leq G$, то $\varphi(H) \leq \Gamma$;

(2) если $H \triangleleft G$, то $\varphi(H) \triangleleft \text{Im} \varphi$;

(3) если подмножества T и S сопряжены в G , то $\varphi(T)$ и $\varphi(S)$ сопряжены в $\text{Im} \varphi$.

Элементарная проверка.

ТЕОРЕМА 2.3. (ОСНОВНАЯ ТЕОРЕМА О ГОМОМОРФИЗМЕ) При гомоморфизме групп факторгруппа по ядру изоморфна образу, т.е. если $\varphi : G \rightarrow \Gamma$ — гомоморфизм, то $G/\text{Ker} \varphi \simeq \text{Im} \varphi$.

Так как $K = \text{Ker} \varphi \triangleleft G$, то факторгруппа G/K существует. Поставим в соответствие элементу aK группы G/K элемент $\varphi(a)$ из группы $\text{Im} \varphi$, т.е. положим $f(aK) = \varphi(a)$. Если $aK = bK$, то $b^{-1}a \in K$ и $\varphi(b^{-1}a) = \varepsilon$. Поэтому $\varphi(a) = \varphi(b)$ и $f(aK) = f(bK)$. Таким образом, соответствие f не зависит от выбора представителя смежного класса и каждому aK ставится в соответствие единственный элемент $\varphi(a)$. Следовательно, $f : aK \mapsto \varphi(a)$ является отображением группы G/K в группу $\text{Im} \varphi$.

Так как

$$f((aK)(bK)) = f(abK) = \varphi(ab) = \varphi(a)\varphi(b) = f(aK)f(bK),$$

то f — гомоморфизм.

Если $\varphi(a)$ — произвольный элемент из $\text{Im} \varphi$, то $\varphi(a) = f(aK)$, т.е. f — сюръекция.

Если $f(aK) = f(bK)$, то $\varphi(a) = \varphi(b)$, поэтому $\varphi(a^{-1}b) = \varepsilon$ и $a^{-1}b \in \text{Ker} \varphi = K$, т.е. $aK = bK$. Следовательно, f — инъекция и f — изоморфизм групп G/K и $\text{Im} \varphi$.

ТЕОРЕМА 2.4. Пусть H — нормальная подгруппа группы G . Тогда для любой подгруппы A пересечение $A \cap H$ является нормальной подгруппой в подгруппе A , а отображение

$$\varphi : aH \mapsto a(A \cap H)$$

является изоморфизмом групп AH/H и $A/A \cap H$.

Произведение AH — подгруппа группы G по лемме 1.53, с. 39. Так как единичный элемент e группы G содержится в A и в H , то AH содержит H и A . Кроме того, H будет нормальной подгруппой в AH , и можно рассматривать факторгруппу AH/H . Пересечение $A \cap H$ является нормальной подгруппой в A по лемме 1.53, с. 39. Поэтому можно рассматривать факторгруппу $A/A \cap H$.

Отображение

$$\varphi : aH \mapsto a(A \cap H)$$

будет взаимно однозначным отображением множества AH/H на $A/A \cap H$, причем

$$\begin{aligned} \varphi((a_1H)(a_2H)) &= \varphi(a_1a_2H) = a_1a_2(A \cap H) = \\ &= a_1(A \cap H)a_2(A \cap H) = \varphi(a_1H)\varphi(a_2H). \end{aligned}$$

Следовательно, φ — изоморфизм.

Теорему о соответствии, см. теорему 1.59, с. 42, дополняет следующая

ТЕОРЕМА 2.5. Если N и H — нормальные подгруппы группы G , причем $H \leq N$, то G/N изоморфна $G/H/N/H$.

По теореме 1.59 подгруппа N/H нормальна в G/H и факторгруппа $G/H/N/H$ состоит из смежных классов $gH(N/H)$, где gH — элемент из группы G/H . Рассмотрим отображение $\varphi : G/H \rightarrow G/N$, определяемое равенством $\varphi(gH) = gN$. Это отображение будет эпиморфизмом. Если $gH \in \text{Ker} \varphi$, то $\varphi(gH) = gN = N$ и $g \in N$, поэтому $\text{Ker} \varphi = N/H$. По теореме о гомоморфизме группы $G/H/N/H$ и G/N изоморфны.

ПРИМЕР 2.1. Пусть G — произвольная группа, а K — её произвольная нормальная подгруппа. Отображение $\varphi : g \mapsto gK$ группы G в факторгруппу G/K будет эпиморфизмом с ядром K . $\square$

ПРИМЕР 2.2. Пусть $\mathbb{Z}$ — аддитивная группа целых чисел, G — мультипликативная группа и a — фиксированный элемент из G . Рассмотрим отображение $\varphi : k \mapsto a^k$ из группы $\mathbb{Z}$ в группу G . Так как

$$\varphi(k+l) = a^{k+l} = a^k a^l = \varphi(k)\varphi(l),$$

то φ — гомоморфизм. Образ

$$\text{Im} \varphi = \{\varphi(k) \mid k \in \mathbb{Z}\} = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle$$

совпадают с циклической подгруппой, порожденной элементом a . Ядро

$$\text{Ker} \varphi = \{k \mid \varphi(k) = e\} = \{a^k = e\}$$

состоит из тех целых чисел k , для которых $a^k = e$. По теореме 1.21, с. 22, все эти числа кратны порядку элемента a , т.е. $\text{Ker} \varphi = \{a \mid \mathbb{Z}\}$. По основной теореме о гомоморфизмах $\mathbb{Z}/\{a \mid \mathbb{Z}\} \simeq \langle a \rangle$. $\square$

ПРИМЕР 2.3. Пусть S_n — симметрическая группа степени n , а $\Gamma = \{-1, 1\}$ — мультипликативная группа. Рассмотрим отображение $\text{sgn} : \tau \mapsto \text{sgn} \tau$. Четным перестановкам ставится в соответствие 1, а число (-1)

ставится в соответствии нечетным перестановкам. Поскольку знак произведения перестановок равен произведению знаков, т.е. $\text{sgn}(\tau\delta) = \text{sgn}\tau\text{sgn}\delta$, то требование $\langle 1 \rangle$ выполняется, и sgn — гомоморфизм. Ядро этого гомоморфизма состоит из четных перестановок, поэтому $\text{Ker}\text{sgn} = A_n$ — знакопеременная группа. Так как sgn — сюръекция, то $\text{Im}\text{sgn} = \Gamma$ и $S_n/A_n \simeq \Gamma$. $\square$

ПРИМЕР 2.4. Зададим отображение $\det : A \mapsto \det A$, которое каждой невырожденной матрице $A \in GL(n, P)$, где P — поле, ставит в соответствии её определитель. Так как определитель произведения двух матриц равен произведению определителей, т.е. $\det AB = \det A \det B$, то требование $\langle 1 \rangle$ выполняется, и отображение $\det$ — гомоморфизм группы $GL(n, P)$ в мультипликативную группу $P^\#$. Каждое число $a \in P^\#$ будет определителем матрицы

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

поэтому $\text{Im}\det = P^\#$, т.е. $\det$ — эпиморфизм. Ядро

$$\text{Ker}\det = \{A \in GL(n, P) \mid \det A = 1\}$$

состоит из матриц с единичным определителем, поэтому ядро $\text{Ker}\det = SL(n, P)$ — специальная линейная группа, а по лемме 2.1 подгруппа $SL(n, P)$ нормальна в $GL(n, P)$. По теореме о гомоморфизме факторгруппа $GL(n, P)/SL(n, P)$ изоморфна мультипликативной группе $P^\#$. $\square$

2.2. Автоморфизмы

Напомним, что изоморфное отображение группы на себя называется *автоморфизмом* группы. Два автоморфизма φ и ψ группы G считаются равными, если они одинаково действуют на элементах группы, т.е. если $\varphi(x) = \psi(x)$ для всех $x \in G$. Если автоморфизмы φ и ψ различны, то существует элемент $y \in G$ такой, что $\varphi(y) \neq \psi(y)$. Совокупность $\text{Aut}G$ всех автоморфизмов группы G с операцией

$$(\varphi\psi)(x) = \varphi(\psi(x))$$

для всех $x \in G$ является группой, см. теорему 1.34, с. 29.

ПРИМЕР 2.5. Пусть G — абелева группа и $\alpha : x \mapsto x^{-1}$. Тогда α — автоморфизм группы G . $\square$

ПРИМЕР 2.6. Пусть $\mathbb{C}^\#$ — мультипликативная группа ненулевых комплексных чисел. Тогда отображение $a + bi \mapsto \overline{a + bi} = a - bi$ является автоморфизмом группы $\mathbb{C}^\#$. $\square$

ПРИМЕР 2.7. Пусть G — абелева группа порядка n и m — натуральное число. Если m и n взаимно просты, то отображение $\beta : g \mapsto g^m$, $g \in G$, является автоморфизмом группы G . В частности, если G — абелева группа нечетного порядка, то отображение $g \mapsto g^2$ — автоморфизм группы G .

Действительно, т.к. группа G абелева, то $(ab)^m = a^m b^m$ для всех $a, b \in G$. Поэтому отображение $\beta : g \mapsto g^m$ — гомоморфизм группы G в G .

Если $a^m = e$ для некоторого $a \in G$, то порядок элемента a делит m по теореме 1.21, с. 22. Но $|a|$ делит n по теореме Лагранжа, а числа m и n взаимно просты. Следовательно, из равенства $a^m = e$ следует, что $a = e$ и β — инъекция. Поэтому β — автоморфизм группы G . $\square$

При автоморфизмах сохраняются многие свойства групп. Отметим некоторые в следующей лемме. Если $H \subseteq G$ и $\varphi \in \text{Aut}G$, то $\varphi(H) = \{\varphi(h) \mid h \in H\}$ — образ подмножества H при автоморфизме φ .

ЛЕММА 2.6. Пусть G — группа, H и $K \leq G$, $x \in G$ и $\varphi \in \text{Aut}G$. Тогда:

- (1) $|x| = |\varphi(x)|$;
- (2) $C_G(\varphi(x)) = \varphi(C_G(x))$;
- (3) $\varphi(H) \simeq H$;
- (4) если $H \leq K$, то $\varphi(H) \leq \varphi(K)$ и $|K : H| = |\varphi(K) : \varphi(H)|$;
- (5) если $H \triangleleft K$, то $\varphi(H) \triangleleft \varphi(K)$ и $K/H \simeq \varphi(K)/\varphi(H)$;
- (6) $N_G(\varphi(H)) = \varphi(N_G(H))$; $C_G(\varphi(H)) = \varphi(C_G(H))$.

Все утверждения леммы легко получаются из соответствующих определений.

Внутренние автоморфизмы. Пусть G — группа и $g \in G$. Зададим отображение

$$i_g : x \mapsto gxg^{-1} \quad \langle 1 \rangle$$

для всех $x \in G$. Если $gxg^{-1} = gyg^{-1}$, то $x = y$ и i_g — инъекция. Так как для любого $h \in G$ имеем $i_g(g^{-1}hg) = h$, то i_g — биекция. Кроме того,

$$i_g(xy) = g(xy)g^{-1} = gxg^{-1}gyg^{-1} = i_g(x)i_g(y)$$

и i_g — автоморфизм группы G .

Аutomорфизм i_g группы G , определяемый формулой $\langle 1 \rangle$, называется *внутренним автоморфизмом* группы G , порожденным элементом g . Совокупность всех внутренних автоморфизмов группы G обозначается через $\text{Inn}G$. Таким образом,

$$\text{Inn}G = \{i_g : x \mapsto gxg^{-1} \mid g, x \in G\}.$$

ТЕОРЕМА 2.7. (1) $\text{Inn}G \triangleleft \text{Aut}G$;

(2) $\text{Inn}G \simeq G/Z(G)$.

(1) Пусть i_g и $i_h \in \text{Inn}G$, $g, h \in G$. Тогда

$$\begin{aligned} i_g i_h(x) &= i_g(i_h(x)) = i_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = \\ &= (gh)x(gh)^{-1} = i_{gh}(x). \end{aligned}$$

Таким образом, $i_g i_h = i_{gh}$ и умножение определено на $\text{Inn}G$. Для единичного элемента e группы G внутренний автоморфизм i_e будет тождественным отображением, т.е. единичным элементом в $\text{Inn}G$. Поэтому из равенства $i_g i_h = i_{gh} = i_e$ следует, что $h = g^{-1}$ и $(i_g)^{-1} = i_{g^{-1}} \in \text{Inn}G$. Оба требования критерия подгруппы выполняются, следовательно, $\text{Inn}G$ — подгруппа группы $\text{Aut}G$.

Пусть $\varphi \in \text{Aut}G$, $i_g \in \text{Inn}G$. Тогда для любого $x \in G$ имеем:

$$\begin{aligned} (\varphi^{-1} i_g \varphi)(x) &= (\varphi^{-1} i_g)(\varphi(x)) = \varphi^{-1}(g\varphi(x)g^{-1}) = \\ &= \varphi^{-1}(g)\varphi^{-1}(\varphi(x))\varphi^{-1}(g^{-1}) = \varphi^{-1}(g)x(\varphi^{-1}(g))^{-1} = \end{aligned}$$

$$= i_{\varphi^{-1}(g)}(x), \text{ т.е. } \varphi^{-1}i_g\varphi = i_{\varphi^{-1}(g)} \in \text{Inn}G$$

и $\text{Inn}G$ — нормальная подгруппа группы $\text{Aut}G$.

(2) Определим отображение $f : G \rightarrow \text{Inn}G$ следующим образом: $f : g \mapsto i_g$, для всех $g \in G$. Тогда

$$f(gh) = i_{gh} = i_g i_h = f(g)f(h)$$

и f — гомоморфизм группы G в $\text{Inn}G$. Ясно, что f — сюръекция, то есть $\text{Im}f = \text{Inn}G$. Найдем ядро.

$$\begin{aligned} \text{Ker}f &= \{g \in G \mid f(g) = i_e\} = \\ &= \{g \in G \mid gxg^{-1} = x \text{ для всех } x \in G\} = Z(G). \end{aligned}$$

Применяя основную теорему о гомоморфизмах групп получаем, что $G/Z(G) \simeq \text{Inn}G$.

ТЕОРЕМА 2.8. Пусть G — группа и H — её подгруппа. Тогда $C_G(H) \triangleleft N_G(H)$ и $N_G(H)/C_G(H)$ изоморфна подгруппе группы автоморфизмов H .

Для каждого $g \in N_G(H)$ ограничение i_g^0 внутреннего автоморфизма i_g группы G на подгруппе H будет автоморфизмом группы H . Рассмотрим отображение $f : g \mapsto i_g^0$ для всех $g \in N_G(H)$. Это отображение f является гомоморфизмом группы $N_G(H)$ в $\text{Aut}H$, ядро которого

$$\begin{aligned} \text{Ker}f &= \{g \in N_G(H) \mid ghg^{-1} = h \text{ для всех } h \in H\} = \\ &= C_{N_G(H)}(H) = C_G(H). \end{aligned}$$

Теперь остается только применить основную теорему о гомоморфизмах групп.

Характеристические подгруппы. Пусть H — подгруппа группы G и α — автоморфизм группы G . Если $\alpha(H) = H$ для всех $\alpha \in \text{Aut}G$, то H называют *характеристической* подгруппой группы G и пишут $H \text{ char } G$. В каждой группе G единичная подгруппа и вся группа являются характеристическими подгруппами. Если в группе G нет других (отличной от единичной подгруппы и всей группы) характеристических подгрупп, то группа называется *характеристически простой*.

ЛЕММА 2.9. Каждая подгруппа конечной циклической группы характеристическая.

В циклических группах подгруппа фиксированного порядка единственна, см. следствие 3, с. 24. Поэтому, если G — циклическая группа и $H \leq G$, то из условия $|H| = |\alpha(H)|$ следует, что $\alpha(H) = H$ и $H \text{ char } G$.

ПРИМЕР 2.8. Простые группы являются характеристически простыми. $\square$

ЛЕММА 2.10. Пусть $H \leq G$. Тогда:

- (1) если $H \text{ char } G$, то $H \triangleleft G$;
- (2) если $H \text{ char } G$, то $C_G(H) \text{ char } G$;
- (3) если H и $K \text{ char } G$, то $HK \text{ char } G$ и $H \cap K \text{ char } G$;
- (4) если $H \leq K \leq G$, $H \text{ char } G$ и $K/H \text{ char } G/H$, то $K \text{ char } G$.

(1) Пусть $H \text{ char } G$. Тогда $i_g(H) = H$ для всех $g \in G$. Так как $i_g(H) = gHg^{-1}$, то из равенства $gHg^{-1} = H$ для всех $g \in G$ следует, что $H \triangleleft G$.

(2) Пусть $H \text{ char } G$ и $\alpha \in \text{Aut}G$. Если $g \in C_G(H)$, $h \in H$, то $gh = hg$ для всех $h \in H$, поэтому $\alpha(g)\alpha(h) = \alpha(h)\alpha(g)$, а т.к. $\alpha(H) = H$, то $\alpha(g) \in C_G(H)$ и $C_G(H) \text{ char } G$.

Доказательство утверждений (3) и (4) осуществляется непосредственной проверкой.

ЛЕММА 2.11. Пусть $H \leq K \leq G$. Тогда:

(1) если $H \text{ char } K$, $K \text{ char } G$, то $H \text{ char } G$;

(2) если $H \text{ char } K$, $K \triangleleft G$, то $H \triangleleft G$.

(1) Для любого $\alpha \in \text{Aut}G$ из условия $K \text{ char } G$ следует, что $\alpha(K) = K$. Ограничение $\alpha|_K$ автоморфизма α на K будет автоморфизмом K , а так как $H \text{ char } K$, то $\alpha|_K(H) = \alpha(H) = H$ и $H \text{ char } G$.

(2) Так как $K \triangleleft G$, то $i_g(K) = K$. Ограничение i_g^0 внутреннего автоморфизма i_g группы G на K будет автоморфизмом K , а так как $H \text{ char } K$, то $i_g^0(H) = i_g(H) = H$ и $H \triangleleft G$.

Холловой подгруппой конечной группы называют подгруппу, порядок и индекс которой взаимно просты. Силовая подгруппа всегда будет холловой.

ЛЕММА 2.12. Пусть N — холлова нормальная подгруппа конечной группы G . Тогда N — характеристическая подгруппа и если M — подгруппа, порядок которой делит порядок N , то $M \leq N$.

Докажем вначале второе утверждение. Пусть $M \leq G$ и порядок M делит порядок N . Так как MN — подгруппа группы G , то её порядок делит порядок группы G . Но

$$|MN| = |M| |N| / |M \cap N|,$$

поэтому

$$|MN| / |N| = |M| / |M \cap N|$$

делит $|G/N|$. Так как $|M/M \cap N|$ делит $|N|$, а числа $|N|$ и $|G/N|$ взаимно просты, то $|M| = |M \cap N|$ и $M \leq N$. Второе утверждение доказано.

Если $\alpha \in \text{Aut}G$, то $\alpha(N)$ — подгруппа, порядок которой равен порядку N . По доказанному имеем $\alpha(N) = N$ и $N \text{ char } G$.

СЛЕДСТВИЕ. Нормальная силовская подгруппа конечной группы является характеристической подгруппой. $\square$

Центральные автоморфизмы. Автоморфизм α группы G называется *центральным* автоморфизмом, если α перестановочен с каждым внутренним автоморфизмом группы G , т.е. если $\alpha i_g = i_g \alpha$ для всех $g \in G$.

ТЕОРЕМА 2.13. Автоморфизм α является центральным тогда и только тогда, когда $g^{-1}\alpha(g) \in Z(G)$ для всех $g \in G$.

Пусть α — центральный автоморфизм группы G . Тогда $\alpha i_g = i_g \alpha$ для всех $g \in G$. Если x — произвольный элемент группы G , то

$$\alpha i_g(x) = \alpha(gxg^{-1}) = \alpha(g)\alpha(x)\alpha(g)^{-1} = i_g\alpha(x) = g\alpha(x)g^{-1}.$$

Поэтому

$$g^{-1}\alpha(g)\alpha(x) = \alpha(x)g^{-1}\alpha(g)$$

и $g^{-1}\alpha(g) \in Z(G)$.

Обратно, пусть α — автоморфизм группы G и пусть $g^{-1}\alpha(g) \in Z(G)$ для всех $g \in G$. Тогда для любого $x \in G$ имеем:

$$g^{-1}\alpha(g)\alpha(x) = \alpha(x)g^{-1}\alpha(g),$$

$$\alpha(g)\alpha(x)\alpha(g)^{-1} = g\alpha(x)g^{-1},$$

$$\alpha i_g(x) = i_g\alpha(x),$$

т.е. α — центральный автоморфизм.

СЛЕДСТВИЕ. *Группа с единичным центром не имеет нетождественных центральных автоморфизмов.* $\square$

СЛЕДСТВИЕ. *Если $Z(G) = E$, то $C_{\text{Aut}G} \text{Inn}G = E$.*

Множество центральных автоморфизмов группы G совпадает с $C_{\text{Aut}G} \text{Inn}G = E$. Теперь утверждение вытекает из предыдущего следствия.

2.3. Эндоморфизмы и операторы

Гомоморфное отображение группы в себя называется *эндоморфизмом* группы. Таким образом, эндоморфизм φ группы G переводит элемент $x \in G$ в некоторый элемент $\varphi(x) \in G$, причем $\varphi(xy) = \varphi(x)\varphi(y)$ для любых $x, y \in G$. Множество всех эндоморфизмов группы G обозначают через $\text{End}G$. Два эндоморфизма φ и ψ группы G считаются равными если они одинаково действуют на элементах группы, т.е. если $\varphi(x) = \psi(x)$ для всех $x \in G$. Если эндоморфизмы φ и ψ различны, то существует элемент $y \in G$ такой, что $\varphi(y) \neq \psi(y)$.

Отображение $x \mapsto e$ для любого $x \in G$ является эндоморфизмом, здесь e — единичный элемент группы G . Этот эндоморфизм называется *нулевым*. Эндоморфизм $x \mapsto x$ называют *единичным* или *тождественным*.

ЛЕММА 2.14. *Множество $\text{End}G$ всех эндоморфизмов группы G с операцией*

$$\varphi\psi(x) = \varphi(\psi(x)), \quad \text{для всех } x \in G,$$

является полугруппой с единичным элементом

$$\varepsilon : x \mapsto x.$$

Пусть φ и $\psi \in \text{End}G$. Так как

$$\begin{aligned} \varphi\psi(xy) &= \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) = \\ &= \varphi(\psi(x))\varphi(\psi(y)) = (\varphi\psi)(x)(\varphi\psi)(y), \end{aligned}$$

то $\varphi\psi$ — эндоморфизм группы G . Поскольку умножение отображений ассоциативно, то $\text{End}G$ — полугруппа. Далее, $\varphi\varepsilon(x) = \varphi(x)$ и $\varepsilon\varphi(x) = \varphi(x)$, поэтому $\varphi\varepsilon = \varepsilon\varphi = \varphi$ для всех $\varphi \in \text{End}G$ и ε — единичный элемент в полугруппе $\text{End}G$.

Понятие гомоморфизма, введённое для групп, распространяется и на полугруппы. Отображение $\varphi : P_1 \rightarrow P_2$ (мультипликативной) полугруппы P_1 в (мультипликативную) полугруппу P_2 называется *гомоморфизмом*, если $\varphi(xy) = \varphi(x)\varphi(y)$ для всех $x, y \in P_1$. Если гомоморфизм $\varphi : P_1 \rightarrow P_2$ является биекцией, то он называется *изоморфизмом* полугрупп P_1 и P_2 . Факт изоморфизма полугрупп P_1 и P_2 обозначают так: $P_1 \simeq P_2$.

Эндоморфизмы и автоморфизмы циклических групп. Обозначим через $(\mathbb{Z}, \cdot)$ мультипликативную полугруппу целых чисел, а через $(\mathbb{Z}_n, \cdot)$ — мультипликативную полугруппу классов вычетов по модулю n .

ТЕОРЕМА 2.15. (1) Если $\langle g \rangle$ — бесконечная циклическая группа, то $\text{End}\langle g \rangle \simeq (\mathbb{Z}, \cdot)$.

(2) Если $\langle g \rangle$ — конечная циклическая группа порядка n , то $\text{End}\langle g \rangle \simeq (\mathbb{Z}_n, \cdot)$.

По теореме 1.20, с. 22, циклическая подгруппа $\langle g \rangle$, порожденная элементом g , состоит из всевозможных целых степеней элемента g , т.е.

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}.$$

Обозначим через φ_k , $k \in \mathbb{Z}$, эндоморфизм группы $\langle g \rangle$, для которого $g^i \mapsto g^{ik}$. Пусть φ — произвольный эндоморфизм группы $\langle g \rangle$. Тогда $\varphi(g) \in \langle g \rangle$, поэтому $\varphi(g) = g^m$ для некоторого целого m . Если g^i — произвольный элемент из $\langle g \rangle$, то

$$\varphi(g^i) = (\varphi(g))^i = g^{mi} \quad \text{и} \quad \varphi = \varphi_m.$$

Таким образом, каждый эндоморфизм группы $\langle g \rangle$ имеет вид $\varphi_k : g^i \mapsto g^{ik}$, где $k \in \mathbb{Z}$, поэтому

$$\text{End}\langle g \rangle = \{\varphi_k \mid k \in \mathbb{Z}\}.$$

Так как

$$(\varphi_s \varphi_t)g^i = \varphi_s(\varphi_t(g^i)) = \varphi_s(g^{ti}) = g^{sti} = \varphi_{st}(g^i),$$

то $\varphi_s \varphi_t = \varphi_{st}$ и отображение $\alpha : k \mapsto \varphi_k$ будет эпиморфизмом полугруппы $(\mathbb{Z}, \cdot)$ на полугруппу $\text{End}\langle g \rangle$.

(1) Пусть $\langle g \rangle$ — бесконечная группа. Тогда $g^s \neq g^t$ при $s \neq t$, поэтому $\varphi_s \neq \varphi_t$ и отображение $\alpha : k \mapsto \varphi_k$ будет изоморфизмом полугрупп $(\mathbb{Z}, \cdot)$ и $\text{End}\langle g \rangle$.

(2) Пусть $\langle g \rangle$ — конечная группа порядка n . Тогда

$$\langle g \rangle = \{g^0 = e, g, g^2, \dots, g^{n-1}\}$$

по теореме 1.21, с. 22. Если $\varphi_s = \varphi_t$, то

$$\varphi_s(g) = g^s = \varphi_t(g) = g^t, \quad g^{s-t} = e$$

и $s - t$ делится на n по теореме 1.21, с. 22. Поэтому отображение

$$\beta : \bar{k} \mapsto \varphi_k, \quad \bar{k} = k + n\mathbb{Z} \in \mathbb{Z}_n,$$

будет изоморфизмом полугрупп $(\mathbb{Z}_n, \cdot)$ и $\text{End}\langle g \rangle$.

ТЕОРЕМА 2.16. (1) Если $\langle g \rangle$ — бесконечная циклическая группа, то $\text{Aut}\langle g \rangle$ — группа порядка 2.

(2) Если $\langle g \rangle$ — конечная циклическая группа порядка n , то $\text{Aut}\langle g \rangle$ изоморфна группе всех обратимых элементов полугруппы $(\mathbb{Z}_n, \cdot)$.

(3) Группа автоморфизмов циклической группы абелева.

(4) Группа автоморфизмов группы простого порядка p является циклической группой порядка $p - 1$.

(1) Из всех эндоморфизмов φ_k бесконечной циклической группы $\langle g \rangle$ только два эндоморфизма

$$\varphi_1 : g \mapsto g; \quad \varphi_{-1} : g \mapsto g^{-1}$$

будут автоморфизмами.

(2) Пусть X — множество всех обратимых элементов полугруппы $(\mathbb{Z}_n, \cdot)$. Если $\varphi \in \text{Aut}\langle g \rangle$, то φ — обратимый элемент, поэтому $\varphi \in X$. Если $\psi \in X$, то ψ — биекция, поэтому $\psi \in \text{Aut}\langle g \rangle$ и $\text{Aut}\langle g \rangle = X$.

(3) Так как $(\mathbb{Z}, \cdot)$ и $(\mathbb{Z}_n, \cdot)$ — абелевы полугруппы, то в обоих случаях группа $\text{Aut}\langle g \rangle$ абелева.

(4) Если p — простое число, то кольцо классов вычетов $\mathbb{Z}_p$ является полем, поэтому его мультипликативная группа $(\mathbb{Z}_p^\#, \cdot)$ циклическая порядка $(p - 1)$. По (2) $\text{Aut}\langle g \rangle \simeq (\mathbb{Z}_p^\#, \cdot)$.

Операторы. Пусть даны группа G , множество Ω и отображение $f : \Omega \rightarrow \text{End}G$, переводящее элемент $\alpha \in \Omega$ в элемент $f(\alpha) \in \text{End}G$. Так как $f(\alpha)$ — эндоморфизм группы G , то каждый элемент $x \in G$ под действием эндоморфизма $f(\alpha)$ перейдет в элемент $f(\alpha)(x) \in G$. Условимся вместо $f(\alpha)(x)$ писать $\alpha(x)$. Ясно, что $\alpha(xy) = \alpha(x)\alpha(y)$ для всех $x, y \in G$.

В этой ситуации множество Ω называют *областью операторов* группы G , элементы из Ω — *операторами* группы G , а саму группу G — Ω -*группой* или *группой с областью операторов* Ω . Операторы действуют на группе G также, как и соответствующие им эндоморфизмы. Заметим, что различные операторы могут не отличаться по действию на группе G , поскольку им может соответствовать один и тот же эндоморфизм.

Если H — подмножество группы G и $\alpha \in \Omega$, то

$$\alpha(H) = \{\alpha(h) \mid h \in H\}$$

— образ множества H под действием оператора α . Очевидно, что если H — подгруппа группы G , то и $\alpha(H)$ — подгруппа.

Подгруппа H называется Ω -*допустимой* или просто Ω -*подгруппой*, если $\alpha(H) \subseteq H$ для всех $\alpha \in \Omega$. Ясно, что пересечение Ω -подгрупп Ω -группы вновь является Ω -подгруппой. Если H — Ω -подгруппа и $\alpha \in \Omega$, то ограничение $f(\alpha)|_H$ эндоморфизма $f(\alpha)$ на подгруппе H является эндоморфизмом подгруппы H , т.е. $f(\alpha)|_H \in \text{End}H$. Это позволяет считать Ω областью операторов любой Ω -подгруппы группы G .

ПРИМЕР 2.9. Пусть Ω — непустое множество и отображение $f : \Omega \rightarrow \text{End}G$ действует так: $f(\alpha) = \varepsilon$, где $\varepsilon : g \mapsto g$ — тождественный эндоморфизм группы G . В этой ситуации $f(\Omega) = \langle \varepsilon \rangle$ — единичная подгруппа в $\text{Aut}G \leq \text{End}G$ и $\alpha(g) = f(\alpha)(g) = \varepsilon(g) = g$. Поэтому каждая подгруппа группы G будет Ω -допустимой. $\square$

ПРИМЕР 2.10. Пусть A — непустое подмножество группы G . Превратим A в область операторов группы G с помощью отображения $f : a \mapsto i_a$, $a \in A$. Здесь $i_a : g \mapsto aga^{-1}$ — внутренний автоморфизм группы G , порожденный элементом a . Таким образом, $f(A) \subseteq \text{Inn}G \leq \text{End}G$. Если H — A -допустимая подгруппа из группы G , то $aHa^{-1} \subseteq H$ для всех $a \in A$, т.е. $a \in N_G(H)$. Таким образом, A -допустимыми подгруппами будут те подгруппы X из группы G , для которых $A \subseteq N_G(X)$. При $A = Z(G)$ все подгруппы будут $Z(G)$ -допустимыми. $\square$

ПРИМЕР 2.11. Положим в предыдущем примере $A = G$. Тогда $f(G) = \text{Inn}G \leq \text{End}G$. Поэтому G -допустимыми подгруппами будут нормальные подгруппы и только они.

□

ПРИМЕР 2.12. Если в качестве Ω взять группу $\text{Aut}G$ всех автоморфизмов группы G , то $\text{Aut}G$ -допустимыми подгруппами будут характеристические подгруппы и только они. □

Если H — Ω -подгруппа группы G и $H \triangleleft G$, то факторгруппа G/H становится Ω -группой, если положить $\alpha(gH) = \alpha(g)H$ для $g \in G$ и $\alpha \in \Omega$. Ω -аналогом теоремы 1.59, с. 42, является следующая

ТЕОРЕМА 2.17. Пусть H — нормальная Ω -подгруппа Ω -группы G . Тогда:

(1) если U — Ω -подгруппа и $H \leq U$, то U/H — Ω -подгруппа факторгруппы G/H ;

(2) каждая Ω -подгруппа факторгруппы G/H имеет вид V/H , где V — Ω -подгруппа группы G и $H \leq V$. □

Пусть G — неединичная группа с областью операторов Ω . Если в группе G нет Ω -допустимых нетривиальных нормальных подгрупп (т.е. отличных от единичной подгруппы и всей группы), то группа G называется Ω -простой. Ω -аналогом теоремы 1.61, с. 43, является следующая

ТЕОРЕМА 2.18. (1) Если H — максимальная нормальная Ω -подгруппа неединичной Ω -группы G , то факторгруппа G/H является Ω -простой группой.

(2) Если H — нормальная Ω -подгруппа Ω -группы G и факторгруппа G/H Ω -простая, то H — максимальная нормальная Ω -подгруппа Ω -группы G . □

Пусть G и Γ — группы с одной и той же областью операторов Ω . Гомоморфизм $\varphi : G \rightarrow \Gamma$ называется Ω -гомоморфизмом, если

$$\alpha(\varphi(g)) = \varphi(\alpha(g)) \quad < 1 >$$

для всех $g \in G$, $\alpha \in \Omega$.

ЛЕММА 2.19. Пусть G и Γ — группы с одной и той же областью операторов Ω и $\varphi : G \rightarrow \Gamma$ — Ω -гомоморфизм. Тогда:

(1) ядро

$$\text{Ker}\varphi = \{x \in G \mid \varphi(x) = \varepsilon\},$$

где ε — единица группы Γ , является нормальной Ω -подгруппой группы G ;

(2) образ $\varphi(H)$ любой Ω -подгруппы H из G является Ω -подгруппой группы Γ ;

(3) образ

$$\text{Im}\varphi = \varphi(G) = \{\varphi(g) \mid g \in G, \}$$

Ω -гомоморфизма φ является Ω -подгруппой группы Γ .

Элементарная проверка.

Ω -гомоморфизм $\varphi : G \rightarrow \Gamma$ называется:

Ω -эпиморфизмом, если $\text{Im}\varphi = \Gamma$;

Ω -мономорфизмом, если $\text{Ker}\varphi = E$;

Ω -изоморфизмом, если φ является одновременно Ω -эпиморфизмом и Ω -мономорфизмом. В этом случае говорят, что группы G и Γ Ω -изоморфны и пишут $G \simeq_{\Omega} \Gamma$. Обратим внимание на то, что если $\varphi : G \rightarrow \Gamma$ есть Ω -мономорфизм, то $\varphi : G \rightarrow \text{Im}\varphi$ — Ω -изоморфизм.

ТЕОРЕМА 2.20. При любом Ω -гомоморфизме $\varphi : G \rightarrow \Gamma$ группы $G/\text{Ker}\varphi$ и $\text{Im}\varphi$ Ω -изоморфны.

По теореме 2.3, с. 52, отображение

$$f : g\text{Ker}\varphi \mapsto \varphi(g)$$

является изоморфизмом группы $G/\text{Ker}\varphi$ и группы $\text{Im}\varphi$. Надо только проверить выполнимость равенства $\langle 1 \rangle$ для отображения f . Если $\alpha \in \Omega$, то

$$\begin{aligned} f(\alpha(g\text{Ker}\varphi)) &= f(\alpha(g)\text{Ker}\varphi) = \\ &= \varphi(\alpha(g)) = \alpha(\varphi(g)) = \alpha(f(g\text{Ker}\varphi)). \end{aligned}$$

ТЕОРЕМА 2.21. Если N и H — нормальные Ω -подгруппы Ω -группы G , причем $H \leq N$, то N/H — нормальная Ω -подгруппа факторгруппы G/H и имеет место Ω -изоморфизм

$$(G/H)/(N/H) \simeq {}_{\Omega}G/N.$$

Из теоремы 2.17 вытекает, что N/H — нормальная Ω -подгруппа Ω -факторгруппы G/H . По теореме 2.5, с. 53, отображение $\varphi : G/H \rightarrow G/N$, определяемое равенством $\varphi(gH) = gN$, является эпиморфизмом. Так как

$$\varphi(\alpha(gH)) = \varphi(\alpha(g)H) = \alpha(g)N = \alpha(gN) = \alpha(\varphi(gH)),$$

то φ — Ω -эпиморфизм. Если $gH \in \text{Ker}\varphi$, то $\varphi(gH) = gN = N$ и $g \in N$, поэтому $\text{Ker}\varphi = N/H$. По теореме 2.20 группы $G/H/N/H$ и G/N Ω -изоморфны.

ТЕОРЕМА 2.22. Пусть H — нормальная Ω -подгруппа Ω -группы G . Тогда для любой Ω -подгруппы A пересечение $A \cap H$ является нормальной Ω -подгруппой в подгруппе A , а отображение

$$\varphi : aH \mapsto a(A \cap H)$$

является Ω -изоморфизмом Ω -групп AH/H и $A/A \cap H$.

Ввиду теоремы 2.4, с. 53, надо только проверить выполнимость равенства $\langle 1 \rangle$ для отображения φ . Если $\alpha \in \Omega$, то

$$\begin{aligned} \alpha(\varphi(aH)) &= \alpha(a(A \cap H)) = \\ &= (\alpha(a))(A \cap H) = \varphi(\alpha(a)H) = \varphi(\alpha(aH)). \end{aligned}$$

2.4. Композиционные ряды

Цепочка подгрупп

$$E = A_0 < A_1 < \dots < A_{i-1} < A_i \dots < A_{a-1} < A_a = G$$

называется *рядом* длины a неединичной группы G и обозначается через $(A_i)_{i=0,\dots,a}$.

Ряд $(A_i)_{i=0,\dots,a}$ называется

нормальным, если $A_i \triangleleft G$ для всех i ;

субнормальным, если $A_{i-1} \triangleleft A_i$ для всех i .

Ясно, что каждый нормальный ряд является субнормальным.

Пусть $(A_i)_{i=0,\dots,a}$ — субнормальный ряд конечной группы G . Факторгруппы A_i/A_{i-1} , $i = 1, \dots, a$ называются *факторами* ряда, числа $|A_i/A_{i-1}|$

— индексами ряда. Нормальный ряд $(A_i)_{i=0,\dots,a}$ конечной группы G называется *главным*, если подгруппа A_{i-1} является максимальной нормальной подгруппой группы G , содержащейся в A_i , $i = 1, \dots, a$. Ясно, что в этом случае *главный* фактор A_i/A_{i-1} является минимальной нормальной подгруппой группы G/A_{i-1} для каждого $i = 1, \dots, a$.

Субнормальный ряд $(A_i)_{i=0,\dots,a}$ конечной группы G называется *композиционным*, если подгруппа A_{i-1} является максимальной нормальной подгруппой в A_i , $i = 1, \dots, a$. Композиционные факторы A_i/A_{i-1} по теореме 1.61, с. 43, являются простыми группами.

Ряд $E = E$ считается композиционным и главным рядом единичной группы E , а число 0 — длиной этого ряда.

ПРИМЕР 2.13. Пусть G — группа порядка $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ и $(A_i)_{i=0,\dots,a}$ — ее композиционный ряд. Предположим, что все композиционные факторы A_i/A_{i-1} абелевы. Тогда по теореме 1.38, с. 32, все композиционные факторы имеют простые порядки. Поэтому число композиционных факторов порядка p_i равно a_i , $a = a_1 + a_2 + \dots + a_k$ и $|G| = \prod_{i=1}^a |A_i/A_{i-1}|$. $\square$

Пусть G — конечная группа с областью операторов Ω . Ряд $(A_i)_{i=0,\dots,a}$, состоящий из Ω -подгрупп, называется Ω -*рядом*. Субнормальный Ω -ряд $(A_i)_{i=0,\dots,a}$ называется Ω -*композиционным*, если A_{i-1} является максимальной нормальной Ω -допустимой подгруппой в A_i , $i = 1, \dots, a$. Ясно, что Ω -композиционные факторы A_i/A_{i-1} по теореме 2.18 являются Ω -простыми группами.

ПРИМЕР 2.14. Пусть $\Omega = \langle \varepsilon \rangle$ — единичная подгруппа в $\text{Aut}G$, см. пример 2.9. Тогда Ω -композиционный ряд является композиционным рядом конечной группы G . $\square$

ПРИМЕР 2.15. Если $\Omega = G$, то G -допустимые подгруппы группы G — это в точности её нормальные подгруппы, см. пример 2.11. Поэтому G -композиционный ряд будет главным рядом группы G . $\square$

ПРИМЕР 2.16. Если $\Omega = \text{Aut}G$, то $\text{Aut}G$ -допустимые подгруппы группы G — это в точности её характеристические подгруппы, см. пример 2.12. Поэтому $\text{Aut}G$ -композиционный ряд состоит из характеристических подгрупп и $\text{Aut}G$ -композиционные факторы являются $\text{Aut}G$ -простыми группами. $\square$

Пусть G — конечная Ω -группа. Будем говорить, что два Ω -композиционных ряда $(A_i)_{i=0,1,\dots,a}$ и $(B_i)_{i=0,1,\dots,b}$ группы G *изоморфны*, если $a = b$ и существует биекция

$$\tau : \{A_i/A_{i-1} \mid i = 1, \dots, a\} \rightarrow \{B_i/B_{i-1} \mid i = 1, \dots, b\}$$

такая, что $\tau(A_i/A_{i-1}) \simeq_{\Omega} B_i/B_{i-1}$.

ТЕОРЕМА 2.23. (ЖОРДАН, ГЕЛЬДЕР) Любые два Ω -композиционных ряда конечной Ω -группы G изоморфны.

Применим индукцию к порядку группы. Пусть $(A_i)_{i=0,1,\dots,a}$ и $(B_i)_{i=0,1,\dots,b}$ — два Ω -композиционных ряда Ω -группы G . Ясно, что $G \neq 1$. Тогда $N = B_{b-1}$ — максимальная нормальная Ω -подгруппа Ω -группы G , поэтому $A_i \leq N$ или $A_i N = G$ для всех $i = 0, \dots, a$. Положим $A_i^* = A_i \cap N$ и зафиксируем наибольшее j для которого $A_j \leq N$. Тогда

$$A_j^* = A_j \triangleleft A_{j+1}^* < A_{j+1}.$$

Поскольку A_{j+1}/A_j — Ω -простая группа, то $A_j^* = A_j = A_{j+1}^*$ и

$$G/N = A_{j+1}N/N \simeq {}_{\Omega}A_{j+1}/A_{j+1} \cap N = A_{j+1}/A_j. \quad < 1 >$$

Для $k \geq j+2$ имеем

$$\begin{aligned} A_k^* \cap A_{k-1} &= A_k \cap N \cap A_{k-1} = A_{k-1}^* \\ A_k^*/A_{k-1}^* &\simeq {}_{\Omega}A_k^*A_{k-1}/A_{k-1} \triangleleft A_k/A_{k-1}. \end{aligned}$$

Поскольку A_k/A_{k-1} — Ω -простая группа, то

$$A_k^*/A_{k-1}^* \simeq {}_{\Omega}A_k/A_{k-1} \quad A_k^*/A_{k-1}^* = 1.$$

Если $A_k^*/A_{k-1}^* = 1$, то из равенств $NA_k = NA_{k-1} = G$ получаем:

$$\begin{aligned} G/N &= NA_k/N \simeq {}_{\Omega}A_k/A_k \cap N = A_k/A_k^*; \\ G/N &= NA_{k-1}/N \simeq {}_{\Omega}A_{k-1}/A_{k-1} \cap N = A_{k-1}/A_{k-1}^*, \end{aligned}$$

что приводит к равенству $A_k = A_{k-1}$, противоречие. Поэтому

$$A_k^*/A_{k-1}^* \simeq {}_{\Omega}A_k/A_{k-1} \quad k \geq j+2. \quad < 2 >$$

Теперь

$$\begin{aligned} 1 &= A_0^* < \dots < A_j^* < A_{j+2}^* < \dots < A_k^* = N, \\ 1 &= B_0 < \dots < B_{b-1} = N \end{aligned}$$

— два Ω -композиционных ряда Ω -группы N . По индукции $a-1 = b-1$ и существует биекция

$$\tau^* : \{A_i^*/A_{i-1}^* \mid i = 1, \dots, j, j+2, \dots, a\} \rightarrow \{B_i/B_{i-1} \mid i = 1, \dots, b-1\}$$

такая, что

$$\tau^*(A_i^*/A_{i-1}^*) \simeq {}_{\Omega}B_i/B_{i-1}.$$

Ввиду $<2>$

$$\tau^*(A_i/A_{i-1}) \simeq {}_{\Omega}B_i/B_{i-1}, \quad i \neq j+1,$$

а из $<1>$ следует, что

$$G/N = G/B_{b-1} \simeq {}_{\Omega}A_{j+1}/A_j.$$

В случае, когда $\Omega = \langle \varepsilon \rangle$ — единичная подгруппа в $\text{Aut}G$, см. пример 2.14, получаем

СЛЕДСТВИЕ. Любые два композиционных ряда конечной группы G изоморфны. $\square$

В случае, когда $\Omega = G$, см. пример 2.15, получаем

СЛЕДСТВИЕ. Любые два главных ряда конечной группы G изоморфны. $\square$

ЛЕММА 2.24. Пусть H и $K \triangleleft G$ и $K \leq H$. Тогда

$$C_G(H/K) = \langle g \in G \mid g^{-1}h^{-1}gh \in K, \quad h \in H \rangle$$

является нормальной подгруппой группы G и факторгруппа $G/C_G(H/K)$ изоморфна подгруппе группы $\text{Aut}(H/K)$.

Для каждого $g \in G$ зададим отображение

$$\gamma_g : Kh \mapsto Kghg^{-1}.$$

Если $Kghg^{-1} = Kfgf^{-1}$ для некоторых h и $f \in H$, то $gh(gf)^{-1} \in K$, а так как $K \triangleleft G$, то $hf^{-1} \in K$, поэтому $Kh = Kf$. Значит γ_g — биекция H/K на себя. Так как для любых $a, b \in G$

$$\gamma_a\gamma_b(Kh) = \gamma_a(Kbhb^{-1}) = Kabhb^{-1}a^{-1} = \gamma_{ab}(Kh),$$

то $\gamma_{ab} = \gamma_a \gamma_b$ и $\gamma_g \in \text{Aut}(H/K)$. Рассмотрим отображение $\delta : G \rightarrow \text{Aut}(H/K)$, при котором $\delta(g) = \gamma_g$. Поскольку

$$\delta(ab) = \gamma_{ab} = \gamma_a \gamma_b = \delta(a)\delta(b),$$

то δ — гомоморфизм группы G в $\text{Aut}(H/K)$ с ядром

$$\begin{aligned} \text{Ker} \delta &= \{g \in G \mid \gamma_g : Kh \mapsto Kghg^{-1} = Kh\} = \\ &= \{g \in G \mid ghg^{-1}h^{-1} \in K\} = C_G(H/K). \end{aligned}$$

По основной теореме о гомоморфизмах $G/C_G(H/K)$ изоморфна подгруппе из $\text{Aut}(H/K)$.

Введем обозначение:

$$\text{Aut}_G(H/K) = \{\gamma_g \mid g \in G\},$$

где $\gamma_g : Kh \mapsto Kghg^{-1}$. Тогда $\text{Aut}_G(H/K) = \text{Im} \delta$ и лемма 11.8 утверждает, что

$$G/C_G(H/K) \simeq \text{Aut}_G(H/K).$$

Если $K \triangleleft G$, $H \triangleleft G$, $K \leq H$ и H/K — минимальная нормальная подгруппа группы G/K , то H/K называют *главным фактором* конечной группы G . Ясно, что в этом случае имеется главный ряд конечной группы G , членами которого будут подгруппы K и H . Если $|H/K|$ есть степень простого числа p , то фактор H/K называют *p -главным фактором* группы G .

СЛЕДСТВИЕ. (1) Если H/K — главный фактор конечной группы G , то $C_G(H/K) \triangleleft G$ и $G/C_G(H/K) \simeq \text{Aut}_G(H/K)$.

(2) Если H/K — главный фактор порядка p конечной группы G , то $G/C_G(H/K)$ — циклическая группа порядка, делящего $(p-1)$.

(1) следует из леммы 11.8.

(2) По теореме 2.16, с. 59, группа автоморфизмов группы простого порядка p является циклической группой порядка $(p-1)$. Поэтому, если H/K — p -главный фактор группы G порядка p , то $G/C_G(H/K)$ — циклическая группа порядка, делящего $(p-1)$.

2.5. Прямые произведения

Пусть G — группа, A и B — ее подгруппы. Напомним, что произведение AB определяется как множество элементов ab , где $a \in A$, $b \in B$. Если $AB = G$, то говорят, что группа G является *произведением* своих подгрупп A и B . В этом случае каждый элемент $g \in G$ представим в виде $g = ab$, где $a \in A$, $b \in B$.

Произведение $G = AB$ называется *прямым*, если подгруппы A и B нормальны в G и $A \cap B = E$. Прямое произведение обозначают так: $G = A \times B$. Итак, группа G является *прямым произведением* своих подгрупп, если выполняются следующие требования:

$$G = AB; \quad A \cap B = E; \quad A \triangleleft G, \quad B \triangleleft G.$$

ТЕОРЕМА 2.25. Пусть группа G является прямым произведением своих подгрупп A и B . Тогда:

(1) каждый элемент $g \in G$ единственным образом представим в виде $g = ab$, где $a \in A$, $b \in B$;

(2) каждый элемент подгруппы A перестановочен с каждым элементом подгруппы B .

Обратно, если выполняются требования (1) и (2), то $A \cap B = E$, подгруппы A и B нормальны в G , и $G = A \times B$.

(1) Из равенства $G = AB$ следует, что каждый элемент $g \in G$ записывается в виде $g = ab$, где $a \in A$, $b \in B$. Если имеет место другая запись $g = a_1b_1$, $a_1 \in A$, $b_1 \in B$, то $ab = a_1b_1$, откуда $a^{-1}a_1 = bb_1^{-1} \in A \cap B = E$. Поэтому $a = a_1$, $b = b_1$ и каждый элемент $g \in G$ однозначно записывается в виде $g = ab$.

(2) Рассмотрим произведение $g = a^{-1}b^{-1}ab$. Так как $A \triangleleft G$, то $b^{-1}ab \in A$ и $g \in A$. Так как $B \triangleleft G$, то $a^{-1}b^{-1}a \in B$ и $g \in B$. Но $A \cap B = E$, поэтому $a^{-1}b^{-1}ab = e$ и $ab = ba$. Итак, каждый элемент из A перестановочен с каждым элементом из B .

Пусть теперь выполняются требования (1) и (2). Из (1) следует, что $G = AB$. Элемент $d \in A \cap B$ можно записать в виде $d = ed$, где $e \in A$, $d \in B$, и в виде $d = de$, где $d \in A$, $e \in B$. Из однозначности представления элементов следует, что $d = e$, т.е. $A \cap B = E$.

Из (2) вытекает, что A и B — нормальные подгруппы. Итак, все требования прямого произведения выполняются, поэтому $G = A \times B$.

Теорема 2.25 позволяет дать следующее определение прямого произведения, эквивалентное начальному.

Группа G является *прямым произведением* своих подгрупп A и B , если:

— каждый элемент $g \in G$ единственным образом представим в виде $g = ab$, где $a \in A$, $b \in B$;

— каждый элемент подгруппы A перестановочен с каждым элементом подгруппы B .

Определение прямого произведения сформулировано для двух подгрупп. Для большего числа сомножителей определение выглядит так.

Группа G является *прямым произведением* своих подгрупп $A_1, A_2, \dots, A_n$, если выполняются следующие требования:

$$G = A_1 A_2 \dots A_n; \quad A_i \cap A_1 \dots A_{i-1} A_{i+1} \dots A_n = E; \\ A_i \triangleleft G; \quad i = 1, \dots, n.$$

В этом случае пишут

$$G = A_1 \times A_2 \times \dots \times A_n = \bigotimes_{i=1}^n A_i.$$

Это определение можно заменить следующим, ему эквивалентным. Группа G является *прямым произведением* своих подгрупп $A_1, A_2, \dots, A_n$, если:

— каждый элемент $g \in G$ единственным образом представим в виде $g = a_1 a_2 \dots a_n$, где $a_i \in A_i$, $i = 1, 2, \dots, n$;

— элементы из любых двух подгрупп A_i и A_j , $i \neq j$, перестановочны между собой.

Приведем свойства прямых произведений. Утверждения следующей леммы непосредственно вытекают из определений прямых произведений.

ЛЕММА 2.26. (1) Если $G = A \times B$,

$$A = A_1 \times \dots \times A_k, \quad B = A_{k+1} \times \dots \times A_n,$$

$$\text{то } G = A \times \dots \times A_k \times A_{k+1} \times \dots \times A_n.$$

(2) Если $G = A_1 \times \dots \times A_n$, то $G = A \times B$, где

$$A = A_1 \times \dots \times A_l, \quad B = A_{l+1} \times \dots \times A_n$$

для любого $l = 1, 2, \dots, n-1$. □

ЛЕММА 2.27. (1) Если

$$G = A \times B, \quad A_1 \leq A, \quad B_1 \leq B,$$

то $A_1 B_1 = A_1 \times B_1$.

(2) Если $G = A \times B$ и $A \leq H \leq G$, то $H = A \times (H \cap B)$.

(3) Если $G = A \times B$, $X \subseteq A$, то

$$C_G(X) = C_A(X) \times B, \quad N_G(X) = N_A(X) \times B.$$

(4) Если $G = A \times B$ и $A_1 \triangleleft A$, то $A_1 \triangleleft G$.

(5) Если $G = A \times B$, то $Z(G) = Z(A) \times Z(B)$.

(1) Из теоремы 2.25 следует, что подгруппы A_1 и B_1 перестановочны, поэтому $A_1 B_1$ — подгруппа группы G по теореме 1.41, с. 34. Ясно, что $A_1 \cap B_1 \leq A \cap B = E$. Кроме того, A_1 и B_1 нормальны в $A_1 B_1$, следовательно, $A_1 B_1 = A_1 \times B_1$.

(2) По тождеству Дедекинда имеем, что $H = A(H \cap B)$. Остается применить (1).

(3) Из теоремы 2.25 следует, что элементы из A перестановочны с элементами из B , поэтому $B \leq C_G(X)$ и

$$C_G(X) = (C_G(X) \cap A) \times B = C_A(X) \times B$$

по (2). Аналогично, $B \leq N_G(X)$ и

$$N_G(X) = (N_G(X) \cap A) \times B = N_A(X) \times B.$$

(4) Если $G = A \times B$ и $A_1 \triangleleft A$, то $N_G(A_1) \geq A$ и $A_1 \triangleleft G$ по (3).

(5) Ясно, что

$$Z(A)Z(B) = Z(A) \times Z(B) \leq Z(G).$$

Пусть $z = ab$ — произвольный элемент из $Z(G)$, $a \in A, b \in B$. Если $x \in A$, то

$$xa = xzb^{-1} = zb^{-1}x = ax$$

и $a \in Z(A)$. Если $y \in B$, то

$$yb = ya^{-1}z = a^{-1}zy = by$$

и $b \in Z(B)$. Таким образом, $z \in Z(A)Z(B)$ и $Z(G) \leq Z(A)Z(B)$. Поэтому, $Z(G) = Z(A) \times Z(B)$.

ЛЕММА 2.28. Если $G = A \times B$, то $G/A \simeq B$.

По теореме 2.25 каждый элемент группы G однозначно представим в виде ab , $a \in A, b \in B$. Поэтому $\varphi : ab \mapsto b$ будет отображением группы G в группу B . Так как

$$\varphi(a_1 b_1 a_2 b_2) = \varphi(a_1 a_2 b_1 b_2) = b_1 b_2 = \varphi(a_1 b_1) \varphi(a_2 b_2),$$

то φ — гомоморфизм. Ясно, что φ — сюръекция, поэтому $\text{Im } \varphi = B$. Если $ab \in \text{Ker } \varphi$, то $e = \varphi(ab) = b$ и $\text{Ker } \varphi = A$. По основной теореме о гомоморфизме G/A изоморфна B .

ТЕОРЕМА 2.29. Если $G = A \times B_1 = A \times B_2$, то существует центральный автоморфизм f группы G такой, что $f(B_1) = B_2$.

По теореме об изоморфизме, см. теорему 2.4, с. 53, отображение

$$\alpha_i : b_i \mapsto b_i A, \quad b_i \in B_i, \quad i = 1, 2,$$

является изоморфизмом группы B_i на факторгруппу G/A . Поэтому произведение $\alpha = \alpha_2^{-1} \alpha_1$ является изоморфизмом группы B_1 на B_2 . Для каждого $b \in B_1$ по построению изоморфизмов имеем: $bA = \alpha(b)A$, поэтому $b^{-1}\alpha(b) \in A$. Если a — произвольный элемент группы A , то B_1 и B_2 централизует a , поэтому

$$b^{-1}\alpha(b) \in Z(A) \leq Z(G).$$

Таким образом, $b^{-1}\alpha(b) \in Z(G)$ для всех $b \in B_1$. Так как каждый элемент $x \in G$ единственным образом представим в виде $x = ab$, где $a \in A$, $b \in B_1$, то соответствие $f : x \mapsto a\alpha(b)$ будет автоморфизмом группы G . Кроме того,

$$x^{-1}f(x) = b^{-1}a^{-1}a\alpha(b) = b^{-1}\alpha(b) \in Z(G),$$

т.е. f — центральный автоморфизм группы G по теореме 2.13, с. 57. Но действие f на B_1 совпадает с изоморфизмом α группы B_1 на группу B_2 , поэтому $f(B_1) = B_2$.

С учетом следствия 2, с. 58, получаем

СЛЕДСТВИЕ. Если $G = A \times B_1 = A \times B_2$ и $Z(G) = 1$, то $B_1 = B_2$. $\square$

СЛЕДСТВИЕ. Если $G = A \times B$, A и B — простые неабелевы подгруппы, то E , A , B и G — все нормальные подгруппы группы G .

Пусть C — нормальная подгруппа группы G и $C \notin \{E, A, B, G\}$. Так как A и B — простые группы, то $A \cap C = B \cap C = 1$. Теперь $CA/A \simeq C$ и изоморфна нормальной подгруппе факторгруппы $G/A \simeq B$. Поэтому, $C \simeq B$ и $G = A \times C$. Применяя следствие 5, получаем, что $C = B$. Противоречие.

ТЕОРЕМА 2.30. Пусть

$$G = \bigotimes_{i=1}^n G_i,$$

G_i — неабелева простая группа для всех i и $E \neq N \triangleleft G$. Тогда существует подмножество $J \subseteq \{1, \dots, n\}$ такое, что

$$N = \bigotimes_{j \in J} G_j.$$

Применим индукцию по n . Предположим, что $N \cap G_i = E$ для всех i . Тогда $NG_i = N \times G_i$ и $N \leq Z(G)$ по теореме 2.25. По лемме 2.27

$$Z(G) = \bigotimes_{i=1}^n Z(G_i),$$

а поскольку подгруппы G_i простые неабелевы, то $Z(G) = E$ и $N = E$, противоречие. Следовательно, без ущерба для доказательства можно считать, что $N \cap G_1 \neq E$. Так как $N \cap G_1 \triangleleft G_1$, то $G_1 \leq N$ и по лемме 2.27

$$N = G_1 \times (N \cap \bigotimes_{i=2}^n G_i).$$

Применим индукцию к группе $\bigotimes_{i=2}^n G_i$ и ее нормальной подгруппе

$$K = N \cap \bigotimes_{i=2}^n G_i.$$

По индукции существует подмножество $J_1 \subseteq \{2, \dots, n\}$ такое, что

$$K = \bigotimes_{j \in J_1} G_j.$$

Теперь

$$N = G_1 \times K = \bigotimes_{j \in J} G_j,$$

где $J = J_1 \cup \{1\}$.

Внешнее прямое произведение. Пусть теперь G_1 и G_2 — произвольные группы. На множестве

$$G_1 \times G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

определим операцию (умножение) следующим образом:

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

где $g_i, h_i \in G_i$. Множество $G_1 \times G_2$ превращается в группу с единичным элементом (e_1, e_2) , где e_i — единичный элемент группы G_i , и обратным элементом

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$

Группу $G_1 \times G_2$ называют *внешним прямым произведением групп* G_1, G_2 .

В группе $G = G_1 \times G_2$ имеются две подгруппы

$$G'_1 = \{(g_1, e_2) \mid g_1 \in G_1\}, \quad G'_2 = \{(e_1, g_2) \mid g_2 \in G_2\},$$

причем G'_1 изоморфна G_1 , а G'_2 изоморфна G_2 . Кроме того,

$$G'_1 \triangleleft G, \quad G'_2 \triangleleft G, \quad G'_1 \cap G'_2 = E$$

и $G = G'_1 \times G'_2$, т.е. группа G совпадает с прямым произведением своих подгрупп G'_1 и G'_2 .

ТЕОРЕМА 2.31. Если G_1 и G_2 — группы взаимно простых порядков, то

$$\text{Aut}(G_1 \times G_2) = \text{Aut}G_1 \times \text{Aut}G_2.$$

Пусть $f \in \text{Aut}(G_1 \times G_2)$. Так как G_1 и G_2 — характеристические подгруппы группы $G_1 \times G_2$ по лемме 2.12, с. 57, то ограничение $f_i = f|_{G_i}$ автоморфизма f на подгруппе G_i будет автоморфизмом группы G_i . Отображение $\alpha : f \mapsto (f_1, f_2)$ группы $\text{Aut}(G_1 \times G_2)$ во внешнее прямое произведение $\text{Aut}G_1 \times \text{Aut}G_2$ будет мономорфизмом.

Обратно, каждый элемент

$$(\varphi_1, \varphi_2) \in \text{Aut}G_1 \times \text{Aut}G_2$$

является образом при отображении α следующего автоморфизма группы G :

$$(g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2)).$$

Поэтому,

$$\text{Aut}(G_1 \times G_2) = \text{Aut}G_1 \times \text{Aut}G_2.$$

ТЕОРЕМА 2.32. Пусть группа $G = A \times B$ является прямым произведением своих подгрупп A и B , и пусть $A_1 \triangleleft A$, $B_1 \triangleleft B$. Тогда

$$A_1B_1 = A_1 \times B_1 \triangleleft G \text{ и} \\ G/(A_1 \times B_1) \simeq A/A_1 \times B/B_1.$$

Обратим внимание на то, что $A/A_1 \times B/B_1$ — внешнее произведение групп A/A_1 и B/B_1 . Из леммы 2.27 следует, что A_1 и B_1 — нормальные подгруппы группы G , поэтому A_1B_1 — нормальная подгруппа. Далее, $A_1B_1 = A_1 \times B_1$ по лемме 2.27. Зададим отображение

$$\varphi : ab \mapsto (aA_1, bB_1)$$

из группы G во внешнее прямое произведение $A/A_1 \times B/B_1$. Так как

$$\varphi(a_1b_1a_2b_2) = \varphi(a_1a_2b_1b_2) = (a_1a_2A_1, b_1b_2B_1) = \\ (a_1A_1, b_1B_1)(a_2A_1, b_2B_1) = \varphi(a_1b_1)\varphi(a_2b_2)$$

для всех $a_1, a_2 \in A$, $b_1, b_2 \in B$, то φ — гомоморфизм. Каждый элемент (cA_1, dB_1) , $c \in A$, $d \in B$ группы $A/A_1 \times B/B_1$ будет образом при отображении φ элемента $cd \in A \times B = G$, т.е. φ — эпиморфизм. Если $ab \in \text{Ker}\varphi$, то $e = \varphi(ab) = (aA_1, bB_1)$ и $a \in A_1$, $b \in B_1$. Таким образом,

$$\text{Ker}\varphi = A_1B_1 = A_1 \times B_1.$$

Теперь остается применить основную теорему о гомоморфизме.

Конструкция внешнего прямого произведения групп без труда переносится на случай любого конечного числа сомножителей.

Подпрямое произведение. Пусть группа $G = A_1 \times A_2$ является прямым произведением своих подгрупп A_i , $i = 1, 2$. По теореме 2.25 каждый элемент группы G единственным образом представим в виде

$$g = a_1a_2, \quad a_1 \in A_1, \quad a_2 \in A_2.$$

Поэтому отображение $\varphi_i : g \mapsto a_i$ с учетом теоремы 2.25 будет эпиморфизмом группы G на подгруппу A_i .

Эпиморфизм $\varphi_i : G \rightarrow A_i$ называют *проектированием* группы G на i -ю компоненту A_i . Ясно, что если H — подгруппа группы G , то $\varphi_i(H)$ — подгруппа группы A_i .

Подгруппу $\varphi_i(H)$ называют *проекцией* подгруппы H на A_i . Если подгруппа H такова, что $\varphi_i(H) = A_i$, $i = 1, 2$, то подгруппу H называют *подпрямым произведением* прямого произведения $G = A_1 \times A_2$.

ЛЕММА 2.33. (РЕМАК) Если N_1 и N_2 — нормальные подгруппы группы G , то факторгруппа $G/(N_1 \cap N_2)$ изоморфна подгруппе, являющейся подпрямым произведением прямого произведения $(G/N_1) \times (G/N_2)$.

Внешнее прямое произведение

$$(G/N_1) \times (G/N_2)$$

состоит из множества всех пар (aN_1, bN_2) с умножением

$$(aN_1, bN_2)(cN_1, dN_2) = (acN_1, bdN_2),$$

где $a, b, c, d \in G$. Зададим отображение

$$\varphi : g \mapsto (gN_1, gN_2)$$

для всех $g \in G$. Это отображение будет гомоморфизмом, т.к.

$$\varphi(gh) = (ghN_1, ghN_2) = (gN_1, gN_2)(hN_1, hN_2) = \varphi(g)\varphi(h),$$

$g, h \in G$. Ясно, что

$$\text{Im}\varphi = \{(gN_1, gN_2) \mid g \in G\}$$

и $\text{Im}\varphi$ есть подгруппа группы $(G/N_1) \times (G/N_2)$, которая является подпрямым произведением. Найдем ядро отображения φ .

$$\text{Ker}\varphi = \{g \in G \mid \varphi(g) = e\},$$

где e — единичный элемент прямого произведения $(G/N_1) \times (G/N_2)$. Но единичным элементом является пара (N_1, N_2) , поэтому

$$\varphi(g) = (gN_1, gN_2) = (N_1, N_2)$$

тогда и только тогда, когда $g \in N_1 \cap N_2$. Итак,

$$\text{Ker}\varphi = N_1 \cap N_2.$$

По основной теореме о гомоморфизмах

$$G/(N_1 \cap N_2) \simeq \text{Im}\varphi \leq (G/N_1) \times (G/N_2).$$

Разложение циклической группы в прямое произведение подгрупп. Группа, которая не может быть разложена в прямое произведение своих собственных подгрупп, называется *неразложимой*. Очевидно, неразложимыми будут все простые группы.

ПРИМЕР 2.17. Симметрическая группа S_3 степени 3 содержит единственную нетривиальную нормальную подгруппу $\langle(123)\rangle$, поэтому S_3 неразложима. $\square$

ТЕОРЕМА 2.34. *Множество всех подгрупп циклической примарной группы с бинарным отношением $\leq$ является линейно упорядоченным множеством. В частности, циклическая примарная группа является неразложимой группой.*

Пусть $\langle g \rangle$ — циклическая группа порядка p^n , где p — простое число. По теореме 1.24, с. 23, все её подгруппы исчерпываются циклическими подгруппами $\langle g^t \rangle$ порядка p^n/t для каждого натурального t , делящего p^n . Отсюда следует, что $t = p^m$, где $m = 0, 1, \dots, n$ и

$$\langle g^{p^0} \rangle = \langle g \rangle, \langle g^{p^1} \rangle, \langle g^{p^2} \rangle, \dots, \langle g^{p^{n-1}} \rangle, \langle g^{p^n} \rangle = E$$

— все подгруппы группы $\langle g \rangle$.

Пусть $\langle g^{p^k} \rangle$ и $\langle g^{p^l} \rangle$ — две произвольные подгруппы. Считаем, для определенности, что $k \leq l$. Тогда $l - k \geq 0$ и

$$(g^{p^k})^{p^{l-k}} = g^{p^l},$$

т.е. элемент g^{p^l} является степенью элемента g^{p^k} и

$$\langle g^{p^l} \rangle \leq \langle g^{p^k} \rangle.$$

Значит, в группе $\langle g \rangle$ из любых двух подгрупп всегда одна содержится в другой. Поэтому множество $\mathbf{S}(\langle g \rangle)$ всех подгрупп группы $\langle g \rangle$ с бинарным

отношением $\leq$ является линейно упорядоченным множеством. В частности, в циклической примарной группе нет двух неединичных подгрупп, имеющих единичное пересечение.

Следующая теорема показывает, что каждая циклическая группа составного порядка разложима в прямое произведение своих подгрупп.

ТЕОРЕМА 2.35. *Если $\langle g \rangle$ — циклическая группа порядка nm , где n, m — взаимно простые числа, то*

$$\langle g \rangle = \langle g^m \rangle \times \langle g^n \rangle.$$

Так как n и m взаимно простые числа, то существуют целые числа s и t такие, что $ns + mt = 1$. Теперь

$$g = g^{ns+mt} = (g^n)^s (g^m)^t,$$

т.е. $g \in \langle g^n \rangle \langle g^m \rangle$. Отсюда следует, что

$$\langle g \rangle = \langle g^m \rangle \langle g^n \rangle.$$

Ясно, что подгруппы $\langle g^m \rangle$ и $\langle g^n \rangle$ нормальны в $\langle g \rangle$. Пусть

$$g^k \in \langle g^m \rangle \cap \langle g^n \rangle, \quad \text{т.е.} \quad g^k = g^{mk_1} = g^{nk_2}.$$

Тогда $g^{mk_1 - nk_2} = e$ и mn делит $mk_1 - nk_2$ по теореме 1.21, с. 22. Но m и n взаимно просты, поэтому m делит k_2 , а n делит k_1 и $g^k = g^{mk_1} = e$. Это означает, что подгруппы $\langle g^n \rangle$ и $\langle g^m \rangle$ имеют единичное пересечение. Итак, все требования прямого произведения выполняются, значит

$$\langle g \rangle = \langle g^m \rangle \times \langle g^n \rangle.$$

СЛЕДСТВИЕ. *Всякая конечная циклическая группа является прямым произведением своих примарных неразложимых циклических подгрупп. Более точно, если $\langle g \rangle$ — циклическая группа порядка*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

где p_i — простые числа, $p_i \neq p_j$ при $i \neq j$, то

$$\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle, \quad \text{где} \quad \langle g_i \rangle = \langle g^{n/p_i^{\alpha_i}} \rangle$$

— циклическая подгруппа порядка $p_i^{\alpha_i}$, $i = 1, 2, \dots, k$.

Воспользуемся индукцией по k . По теореме 2.35 имеем

$$\langle g \rangle = \langle g^{p_2^{\alpha_2} \dots p_k^{\alpha_k}} \rangle \times \langle g^{p_1^{\alpha_1}} \rangle. \quad < 1 >$$

Подгруппа $\langle g^{p_2^{\alpha_2} \dots p_k^{\alpha_k}} \rangle$ имеет порядок $p_1^{\alpha_1}$ и по теореме 2.34 неразложима.

Группа $\langle g^{p_1^{\alpha_1}} \rangle$ имеет порядок $n_1 = p_2^{\alpha_2} \dots p_k^{\alpha_k}$ и к ней применима индукция. По индукции

$$\langle g^{p_1^{\alpha_1}} \rangle = \langle g_2 \rangle \times \dots \times \langle g_k \rangle, \quad < 2 >$$

где $g_i = g^{p_1^{\alpha_1} (n_1/p_i^{\alpha_i})} = g^{n/p_i^{\alpha_i}}$ — циклическая подгруппа порядка $p_i^{\alpha_i}$, $i = 2, 3, \dots, k$. Теперь из разложений $<1>$ и $<2>$ в силу леммы 2.26 получаем, что

$$\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle,$$

где

$$g_1 = g^{p_2^{\alpha_2} \dots p_k^{\alpha_k}} = g^{n/p_1^{\alpha_1}}.$$

ПРИМЕР 2.18. Пусть $G = \langle g \rangle$ — циклическая группа порядка 100. Так как $100 = 2^2 5^2$, то по теореме 2.35 группа $\langle g \rangle = \langle g^{5^2} \rangle \times \langle g^{2^2} \rangle$ является прямым произведением своих примарных подгрупп: $\langle g^{5^2} \rangle$ порядка 2^2 и $\langle g^{2^2} \rangle$ порядка 5^2 . По теореме 2.34 подгруппы $\langle g^{25} \rangle$ и $\langle g^4 \rangle$ неразложимы. $\square$

2.6. Минимальные нормальные подгруппы

Минимальной нормальной подгруппой группы G называют такую нормальную подгруппу N группы G , что $N \neq E$ и в N нет нетривиальных нормальных подгрупп группы G . Запись $N \cdot \triangleleft G$ означает, что N — минимальная нормальная подгруппа группы G . Таким образом, если $N \cdot \triangleleft G$, то $N \neq E$ и из условий $X \leq N$, $X \triangleleft G$ следует, что $X = E$ или $X = N$. Очевидно, что в каждой неединичной конечной группе имеется минимальная нормальная подгруппа.

Цоколем группы G называется подгруппа, являющаяся произведением всех минимальных нормальных подгрупп группы G . Цоколь группы G обозначают через $\text{Soc}G$. Таким образом,

$$\text{Soc}G = \prod_{N \cdot \triangleleft G} N.$$

ЛЕММА 2.36. Пусть $N \cdot \triangleleft G$. Тогда:

- (1) если $K \triangleleft G$, то либо $N \leq K$, либо $N \cap K = E$ и $NK = N \times K$;
- (2) если N абелева и $NH = G$ для некоторой собственной подгруппы H группы G , то $N \cap H = E$;
- (3) если $K \triangleleft G$ и $N \not\leq K$, то $NK/K \cdot \triangleleft G/K$.

(1) Пусть $N \not\leq K$. Тогда $N \cap K \triangleleft G$ по лемме 1.53, с. 39, и $N \cap K$ — собственная подгруппа в N . Поэтому $N \cap K = E$ и $NK = N \times K$.

(2) Поскольку $N \cap H \triangleleft H$ и $N \cap H \triangleleft N$, то $N \cap H \triangleleft G$ и $N \cap H = E$.

(3) Так как $N \not\leq K$, то NK/K — неединичная нормальная подгруппа группы G/K . Если X/K — минимальная нормальная подгруппа группы G/K из NK/K , то $X \neq K$, $X \triangleleft G$ и $X = (X \cap N)K$ по тождеству Дедекинда. Теперь $X \cap N \triangleleft G$, а из (1) следует, что $X \cap N = N$ и $X = NK$. Поэтому $X/K = NK/K \cdot \triangleleft G/K$.

ЛЕММА 2.37. Пусть $\mathcal{M}$ — некоторое множество минимальных нормальных подгрупп группы G и

$$M = \prod_{N \in \mathcal{M}} N.$$

Тогда:

- (1) если $K \triangleleft G$, то существуют подгруппы

$$N_1, N_2, \dots, N_k \in \mathcal{M}$$

такие, что

$$KM = K \times N_1 \times N_2 \times \dots \times N_k;$$

- (2) существуют подгруппы

$$N_1, N_2, \dots, N_m \in \mathcal{M}$$

такие, что

$$M = N_1 \times N_2 \times \dots \times N_m;$$

(3) если $\mathcal{M}$ — множество всех минимальных нормальных подгрупп группы G , то существуют подгруппы

$$N_1, N_2, \dots, N_s \in \mathcal{M}$$

такие, что

$$\text{Soc}G = N_1 \times N_2 \times \dots \times N_s.$$

(1) Если $N \in \mathcal{M}$ и $N \not\subseteq K$, то $NK = N \times K$ по лемме 2.36. Пусть $\{N_1, \dots, N_k\}$ — подмножество из $\mathcal{M}$ с наибольшим k , для которого

$$K\left(\prod_{i=1}^k N_i\right) = K \times N_1 \times \dots \times N_k.$$

Обозначим через

$$X = K \times N_1 \times \dots \times N_k.$$

Ясно, что $K \leq X \leq KM$. Если $X \neq KM$, то существует подгруппа $N \in \mathcal{M}$, для которой $N \not\subseteq X$. Но тогда по лемме 2.36 $XN = X \times N$ и

$$XN = K \times N_1 \times \dots \times N_k \times N,$$

что противоречит максимальнойности k . Поэтому допущение неверно и $X = KM$.

(2) Утверждение следует из (1) при $K = E$.

(3) В случае, когда $\mathcal{M}$ — множество всех минимальных нормальных подгрупп группы G подгруппа $M = \prod_{N \in \mathcal{M}} N$ совпадает с цоклем группы G . Поэтому требуемое утверждение вытекает из (2).

ТЕОРЕМА 2.38. (1) В каждой группе минимальная нормальная подгруппа характеристически простая.

(2) Характеристически простая группа является прямым произведением изоморфных простых групп.

(1) Пусть $N \cdot \triangleleft G$ и $K \text{ char } N$. По лемме 2.11, с. 57, подгруппа $K \triangleleft \triangleleft G$. Из минимальности N следует, что $K = E$ или $K = N$. Поэтому N — характеристически простая группа.

(2) Пусть G — характеристически простая группа и $N \cdot \triangleleft G$. Ясно, что $\alpha(N)$ — минимальная нормальная подгруппа группы G для любого $\alpha \in \text{Aut}G$. Пусть $\mathcal{M} = \{\alpha(N) \mid \alpha \in \text{Aut}G\}$ и

$$M = \prod_{K \in \mathcal{M}} K.$$

Так как

$$\beta(M) = \beta\left(\prod_{K \in \mathcal{M}} K\right) = \prod_{K \in \mathcal{M}} \beta(K) = M$$

для любого $\beta \in \text{Aut}G$, то M — характеристическая подгруппа группы G , поэтому $M = G$. По лемме 2.37 получаем, что

$$G = N_1 \times \dots \times N_m$$

для $\{N_1, \dots, N_m\} \subseteq \mathcal{M}$. Итак группа G является прямым произведением изоморфных подгрупп $N_1, \dots, N_m$. По свойствам прямых произведений

каждая нормальная в N_1 подгруппа будет нормальной подгруппой группы G . Из того, что N_1 — минимальная нормальная подгруппа в группе $G = N_1 \times \dots \times N_m$ следует по лемме 2.28, с. 67, что N_1 простая.

Элементарной абелевой p -группой называют группу, являющуюся прямым произведением подгрупп порядка p .

ТЕОРЕМА 2.39. Пусть $N \triangleleft G$ и $K \triangleleft N$. Тогда K — простая подгруппа и существуют элементы $g_1, \dots, g_m \in G$ такие, что $N = K^{g_1} \times \dots \times K^{g_m}$. Кроме того:

(1) если N абелева, то $|K| = p$ для некоторого простого p и N — элементарная абелева p -группа;

(2) если N неабелева, то каждая минимальная нормальная в N подгруппа принадлежит множеству $\{K^{g_1}, \dots, K^{g_m}\}$.

Пусть $\mathcal{M} = \{K^g \mid g \in G\}$ и

$$L = \prod_{X \in \mathcal{M}} X.$$

Ясно, что L является нормальной подгруппой группы G . Так как $K^g \leq N$ для всех $g \in G$, то $L \leq N$, поэтому $L = N$. Поскольку K^g — минимальная нормальная подгруппа в N , то по лемме 2.37 существуют элементы $g_1, \dots, g_m \in G$ такие, что $N = K^{g_1} \times \dots \times K^{g_m}$. Из леммы 2.27, с. 67, следует что подгруппа K простая.

(1) Пусть N абелева. По теореме 1.54, с. 40, подгруппа K имеет простой порядок. Пусть $|K| = p$. Тогда N — элементарная абелева p -группа порядка p^m .

(2) Пусть N неабелева. По теореме 2.30, с. 68, каждая минимальная нормальная в N подгруппа принадлежит множеству $\{K^{g_1}, \dots, K^{g_m}\}$.

СЛЕДСТВИЕ. Минимальная нормальная подгруппа группы либо элементарная абелева p -группа для некоторого простого p , либо является прямым произведением изоморфных простых неабелевых групп. $\square$

ЛЕММА 2.40. Пусть $N \triangleleft G$, $N \leq H \triangleleft G$. Если $K \triangleleft H$, $K \leq N$, то существуют элементы $g_1, \dots, g_n \in G$ такие, что

$$N = K^{g_1} \times \dots \times K^{g_n}.$$

Так как $K^g \leq N^g = N$ для любого $g \in G$, то $N = \langle K^g \mid g \in G \rangle$. Полагая $\mathcal{M} = \{K^g \mid g \in G\}$ из леммы 13.2(2) для группы H и ее нормальной подгруппы N получаем, что существуют элементы $g_1, \dots, g_n$ такие, что

$$N = K^{g_1} \times \dots \times K^{g_n}.$$

Подгруппа U называется субнормальной подгруппой группы G , если существуют подгруппы $U_0, U_1, \dots, U_s$ такие, что

$$U = U_0 \triangleleft U_1 \triangleleft \dots \triangleleft U_{s-1} \triangleleft U_s = G.$$

Запись $U \triangleleft \triangleleft G$ означает, что U — субнормальная подгруппа группы G . Очевидно, что каждая субнормальная подгруппа является членом некоторого субнормального ряда группы G .

ЛЕММА 2.41. Пусть $U \triangleleft \triangleleft G$. Тогда:

- (1) если $T \triangleleft \triangleleft U$, то $T \triangleleft \triangleleft G$;
- (2) если $V \leq G$, то $V \cap U \triangleleft \triangleleft V$;
- (3) если $V \triangleleft \triangleleft G$, то $U \cap V \triangleleft \triangleleft G$;

(4) если $N \triangleleft G$, то $UN/N \triangleleft \triangleleft G/N$.

(1) Очевидно.

(2) Пусть

$$U = U_0 \triangleleft U_1 \triangleleft \dots \triangleleft U_{s-1} \triangleleft U_s = G.$$

Так как $U_i \triangleleft U_{i+1}$, то

$$(V \cap U_{i+1}) \cap U_i = V \cap U_i \triangleleft V \cap U_{i+1}.$$

Поэтому

$$U \cap V = U_0 \cap V \triangleleft U_1 \cap V \triangleleft \dots \triangleleft U_{s-1} \cap V \triangleleft U_s \cap V = V$$

и $U \cap V \triangleleft \triangleleft V$.

(3) По (2) $U \cap V \triangleleft \triangleleft V$, а т.к. $V \triangleleft \triangleleft G$, то $U \cap V \triangleleft \triangleleft G$ по (1).

(4) Так как

$$UN/N = U_0N/N \triangleleft U_1N/N \triangleleft \dots \triangleleft U_{s-1}N/N \triangleleft U_sN/N = G/N,$$

то $UN/N \triangleleft \triangleleft G/N$.

ЛЕММА 2.42. Если $U \triangleleft \triangleleft G$, то $\text{Soc}G \leq N_G(U)$.

Пусть

$$U = U_0 \triangleleft U_1 \triangleleft \dots \triangleleft U_{n-1} \triangleleft U_n = G.$$

Воспользуемся индукцией по n . Если $n = 1$, то $U \triangleleft G$ и $\text{Soc}G \leq N_G(U) = G$. По индукции $\text{Soc}U_{n-1} \leq N_{U_{n-1}}(U) \leq N_G(U)$. Пусть N — произвольная минимальная нормальная подгруппа группы G . Если $N \leq U_{n-1}$, то $N \leq \text{Soc}U_{n-1}$ по лемме 13.6 и подгруппа $N \leq N_G(U)$. Если $N \not\leq U_{n-1}$, то $NU_{n-1} = N \times U_{n-1}$ по лемме 13.1 и опять $N \leq C_G(U) \leq N_G(U)$. Таким образом, в любом случае $N \leq N_G(U)$ и $\text{Soc}G \leq N_G(U)$ по определению цоколя.

ТЕОРЕМА 2.43. Если $\{U_i \mid i \in I\}$ — некоторое множество субнормальных подгрупп группы G , то

$$U = \langle U_i \mid i \in I \rangle \triangleleft \triangleleft G.$$

Воспользуемся индукцией по порядку группы G . Пусть $N \triangleleft G$. Тогда $U_iN/N \triangleleft \triangleleft G/N$ по лемме 13.7 и по индукции $UN/N \triangleleft \triangleleft G/N$. Согласно лемме 13.8 подгруппа $N \subseteq \bigcap_{i \in I} N_G(U_i)$ поэтому $U \triangleleft UN \triangleleft \triangleleft G$ и $U \triangleleft \triangleleft G$.

Из леммы 13.7(3) и теоремы 13.9 получаем

СЛЕДСТВИЕ. Совокупность всех субнормальных подгрупп группы G образует решетку. $\square$

ЛЕММА 2.44. Пусть

$$G = \bigotimes_{i=1}^m G_i,$$

G_i — неабелева простая группа для всех i и $E \neq N \triangleleft \triangleleft G$. Тогда существует подмножество $J \subseteq \{1, \dots, m\}$ такое, что

$$N = \bigotimes_{j \in J} G_j.$$

Пусть

$$N = N_0 \triangleleft N_1 \triangleleft \dots \triangleleft N_{n-1} \triangleleft N_n = G.$$

Воспользуемся индукцией по n . По теореме 2.30, с. 68, существует подмножество $J_1 \subseteq \{1, \dots, m\}$ такое, что

$$N_{n-1} = \bigotimes_{j \in J_1} G_j.$$

Теперь по индукции существует подмножество $J \subseteq J_1$ такое, что

$$N = \bigotimes_{j \in J} G_j.$$

ТЕОРЕМА 2.45. Пусть $H \triangleleft \triangleleft G$, $K \triangleleft \triangleleft G$ и $H \cap K = E$. Если H — неабелева простая подгруппа, то $\langle H \cup K \rangle = H \times K$.

Пусть $U = \langle H \cup K \rangle$ и пусть

$$\begin{aligned} H &= H_0 \triangleleft H_1 \triangleleft \dots \triangleleft H_{n-1} \triangleleft H_n = U; \\ K &= K_0 \triangleleft K_1 \triangleleft \dots \triangleleft K_{m-1} \triangleleft K_m = U. \end{aligned}$$

Воспользуемся индукцией по n . Если $n = 1$, то $H \triangleleft U$ и $U = [H]K$. Если $K \triangleleft U$, то $U = H \times K$. Пусть K не является нормальной подгруппой группы U . Тогда $m \geq 2$ и K — собственная подгруппа в K_1 . Так как $K_1 \triangleleft \triangleleft U$, то $E \neq K_1 \cap H \triangleleft \triangleleft H$. Из того, что H — простая неабелева группа следует, что $H \leq K_1$ и $HK = H \times K$.

Пусть теперь $n \geq 2$. Тогда $H \neq H^{k_1}$ для некоторого $k_1 \in K$ и $H \cap H^{k_1} = E$. Так как $H_{n-1} \triangleleft U$, то $\langle H \cup H^{k_1} \rangle \subseteq H_{n-1}$ и по индукции $\langle H \cup H^{k_1} \rangle = H \times H^{k_1}$.

Пусть

$$V = H \times H^{k_1} \times \dots \times H^{k_t}, \quad k_1, \dots, k_t \in K,$$

с наибольшим номером t . Ясно, что $V \triangleleft \triangleleft H_{n-1}$. Если $H^k \not\subseteq V$ для некоторого $k \in K$, то $V \cap H^k = E$ и $\langle V \cup H^k \rangle = V \times H^k$ по индукции. Противоречие с выбором t . Поэтому $H^k \subseteq V$ для всех $k \in K$ и $K \leq N_G(V)$. Следовательно, $U = VK$.

Если $V \cap K \neq E$, то по лемме 13.11

$$V \cap K = \bigotimes_{i \in I} H^{k_i}$$

для некоторого множества I , поэтому существует номер $j \in I$ такой, что $H^{k_j} \leq K$. Теперь $H \leq K$, что противоречит условию теоремы. Следовательно, $V \cap K = E$ и $U = [V]K$. Если $K \triangleleft U$, то $U = H \times K$. Пусть K не является нормальной подгруппой в группе U . Тогда K — собственная подгруппа в подгруппе K_1 , поэтому $K_1 \cap V \neq E$ и по лемме 13.11 существует множество J такое, что

$$V \cap K_1 = \bigotimes_{j \in J} H^{k_j}.$$

Так как $V \cap K_1 \triangleleft K_1$, то $(V \cap K_1)K = (V \cap K_1) \times K$ и для некоторого $H^{k_l} \leq V \cap K_1$ имеем $H^{k_l}K = H^{k_l} \times K$. Но $k_l \in K$, значит $H^{k_l} \times K = H \times K$.

ТЕОРЕМА 2.46. Пусть H — неабелева простая подгруппа группы G и

$H \triangleleft \triangleleft G$. Тогда $H^G \cdot \triangleleft G$ и существуют элементы $g_1, \dots, g_n$ такие, что

$$H^G = \bigotimes_{i=1}^n H^{g_i}.$$

Если $H \triangleleft G$, то теорема очевидна. Пусть H не является нормальной подгруппой группы G . Тогда существует элемент $g \in G$ такой, что $H \neq H^g$. По теореме 13.12 получаем, что $\langle H \cup H^g \rangle = H \times H^g$. Пусть

$$V = H^{g_1} \times H^{g_2} \times \dots \times H^{g_t}$$

с наибольшим номером t . Если $H^x \not\subseteq V$ для некоторого $x \in G$, то $V \cap H^x \triangleleft \triangleleft H^x$, а поскольку подгруппа H^x простая неабелева, то $V \cap H^x = E$ и $\langle V \cup H^x \rangle = V \times H^x$ по теореме 13.12. Противоречие с выбором t . Поэтому $H^x \subseteq V$ для всех $x \in G$ и $V = H^G \triangleleft G$. Предположим, что $V_1 \triangleleft G$, $V_1 \leq V$. Тогда по лемме 13.11

$$V_1 = \bigotimes_{i \in I} H^{g_i}$$

и $V = H^G \subseteq V_1$. Поэтому $V = V_1 \triangleleft G$.

СЛЕДСТВИЕ. Если H — неабелева простая подгруппа группы G и $H \triangleleft \triangleleft G$, то $H \leq \text{Soc} G$. $\square$

Аналогичное утверждение для абелевых простых субнормальных подгрупп неверно. Примером служит диэдральная группа порядка 8, см. теорему 14.6.

2.7. Полупрямые произведения

ТЕОРЕМА 2.47. Пусть K и H — группы и ψ — гомоморфизм группы K в $\text{Aut} H$. Тогда существует группа G , обладающая следующими свойствами:

- (1) группа G содержит подгруппы $H^* \simeq H$ и $K^* \simeq K$;
- (2) $G = H^* K^*$;
- (3) $H^* \cap K^* = E$;
- (4) $H^* \triangleleft G$.

Условимся образ элемента $h \in H$ при автоморфизме $\psi(k) \in \text{Aut} H$, $k \in K$, обозначать через $[\psi(k)h]$. Проверим, что множество $G = \{(k, h) \mid k \in K, h \in H\}$ с операцией

$$(k_1, h_1)(k_2, h_2) = (k_1 k_2, [\psi(k_2^{-1})h_1]h_2) \quad <1>$$

является искомой группой.

Так как $[\psi(k_2^{-1})h_1] \in H$, то операция $<1>$ определена на G . Проверим, что операция ассоциативна.

$$\begin{aligned} ((k_1, h_1)(k_2, h_2))(k_3, h_3) &= (k_1 k_2, [\psi(k_2^{-1})h_1]h_2)(k_3, h_3) = \\ &= (k_1 k_2 k_3, [\psi(k_3^{-1})([\psi(k_2^{-1})h_1]h_2)]h_3) = \\ &= (k_1 k_2 k_3, [(\psi(k_2 k_3)^{-1})h_1][\psi(k_3^{-1})h_2]h_3); \\ (k_1, h_1)((k_2, h_2)(k_3, h_3)) &= (k_1, h_1)(k_2 k_3, [\psi(k_3^{-1})h_2]h_3) = \end{aligned}$$

$$= (k_1 k_2 k_3, [\psi((k_2 k_3)^{-1}) h_1] [\psi(k_3^{-1}) h_2] h_3).$$

Таким образом операция $\langle 1 \rangle$ ассоциативна. Пусть e_K — единичный элемент группы K , а e_H — единичный элемент группы H . Так как

$$\begin{aligned} (k_1, h_1)(e_K, e_H) &= (k_1 e_K, [\psi(e_K^{-1}) h_1] e_H) = (k_1, h_1); \\ (e_K, e_H)(k_1, h_1) &= (e_K k_1, [\psi(k_1^{-1}) e_H] h_1) = (k_1, h_1), \end{aligned}$$

то (e_K, e_H) — единичный элемент G .

Проверим, что $(k, h)^{-1} = (k^{-1}, [\psi(k) h^{-1}])$.

$$\begin{aligned} (k, h)(k^{-1}, [\psi(k) h^{-1}]) &= (k k^{-1}, [\psi(k) h][\psi(k) h^{-1}]) = \\ &= (e_K, [\psi(k)(h h^{-1})]) = (e_K, e_H); \\ (k^{-1}, [\psi(k) h^{-1}])(k, h) &= (k^{-1} k, [\psi(k^{-1})[\psi(k) h^{-1}]] h) = \\ &= (e_K, [\psi(k^{-1}) \psi(k)(h^{-1})] h) = (e_K, e_H). \end{aligned}$$

Итак, G — группа. Рассмотрим два множества:

$$\begin{aligned} K^* &= \{(k, e_H) \mid k \in K\}; \\ H^* &= \{(e_K, h) \mid h \in H\}. \end{aligned}$$

Так как

$$\begin{aligned} (k_1, e_H)(k_2, e_H) &= (k_1 k_2, [\psi(k_2^{-1}) e_H] e_H) = (k_1 k_2, e_H) \in K^*; \\ (e_K, h_1)(e_K, h_2) &= (e_K e_K, [\psi(e_K^{-1}) h_1] h_2) = (e_K, h_1 h_2) \in H^*, \end{aligned}$$

то K^* и H^* — подгруппы группы G . Ясно, что отображения

$$k \mapsto (k, e_H), \quad h \mapsto (e_K, h)$$

являются изоморфизмами $K \simeq K^*$, $H \simeq H^*$. Из построения получаем, что $K^* \cap H^* = E$ и $G = K^* H^*$. Так как

$$\begin{aligned} (k, e_H)^{-1}(e_K, h)(k, e_H) &= (k^{-1}, e_H)(e_K, h)(k, e_H) = \\ &= (k^{-1}, [\psi(e_K^{-1}) e_H] h)(k, e_H) = (k^{-1}, h)(k, e_H) = \\ &= (k^{-1} k, [\psi(k^{-1}) h] e_H) = (e_K, [\psi(k^{-1}) h]) \in H^*, \end{aligned}$$

то $H^* \triangleleft G$.

Построенная в теореме 14.1 группа G называется *внешним полупрямым произведением* группы K и группы H относительно гомоморфизма ψ и обозначается через $G = K_\psi[H]$ или $G = [H]_\psi K$.

СЛЕДСТВИЕ. Внешнее полупрямое произведение $G = K_\psi[H]$ групп K и H относительно гомоморфизма $\psi : K \rightarrow \text{Aut} H$ является прямым произведением тогда и только тогда, когда ψ каждый элемент группы K переводит в тождественный автоморфизм группы H .

Если $G = K_\psi[H] = K \times H$, то операция $\langle 1 \rangle$ принимает вид:

$$(k_1, h_1)(k_2, h_2) = (k_1 k_2, h_1 h_2); \quad [\psi(k_2^{-1}) h_1] h_2 = h_1 h_2,$$

поэтому $\psi(k_2^{-1}) = \epsilon$ — тождественный автоморфизм группы H для любого $k_2 \in K$.

Обратно, если ψ каждый элемент группы K переводит в тождественный автоморфизм группы H , то из $\langle 1 \rangle$ следует, что

$$(k_1, h_1)(k_2, h_2) = (k_1 k_2, h_1 h_2)$$

и произведение $G = K_\psi[H]$ будет прямым.

ПРИМЕР 2.19. Пусть

$$K = \langle k \rangle, |K| = m, H = \langle h \rangle, |H| = n$$

— циклические группы порядков n и m . Выберем натуральное число r , для которого

$$r^m \equiv 1 \pmod{n} \quad \text{и} \quad r^l \not\equiv 1 \pmod{n}$$

при $0 < l < m$. Для каждого $i = 1, 2, \dots, m$ зададим отображение

$$\varphi_i : h^t \mapsto h^{tr^i}, \quad t = 1, \dots, n.$$

Так как

$$\begin{aligned} \varphi(h^{t_1}h^{t_2}) &= \varphi_i(h^{t_1+t_2}) = h^{(t_1+t_2)r^i} = \\ &= h^{t_1r^i}h^{t_2r^i} = \varphi_i(h^{t_1})\varphi_i(h^{t_2}), \end{aligned}$$

то φ_i — эндоморфизм группы H . Поскольку $\text{Ker} \varphi_i = \{h^t \mid h^{tr^i} = e\} = \{h^t \mid n \text{ делит } tr^i\} = \{h^t \mid n \text{ делит } t\} = \{e\}$, то φ_i — автоморфизм группы H . Заметим, что

$$\begin{aligned} (\varphi_i \varphi_j)(h^t) &= \varphi_i(\varphi_j(h^t)) = \\ \varphi_i(h^{tr^j}) &= h^{tr^j r^i} = h^{tr^{i+j}} = \varphi_{i+j}(h^t), \end{aligned}$$

т.е. $\varphi_i \varphi_j = \varphi_{i+j}$. Здесь сложение $i + j$ происходит по модулю n .

Теперь отображение $\psi : k^i \mapsto \varphi_i$ будет гомоморфизмом группы K в группу $\text{Aut} H$. По теореме 2.47 существует группа G , являющаяся полупрямым произведением групп K и H относительно ψ , т.е. $G = K_\psi[H]$. $\square$

ПРИМЕР 2.20. Положим в предыдущем примере $m = 2$. Тогда $r = n - 1$ и

$$\varphi_1 : h^t \mapsto h^{(n-1)t} = h^{-t}, \quad \varphi_2 : h^t \mapsto h^{t(n-1)^2} = h^t,$$

и φ_2 — тождественный автоморфизм. Группа

$$G = K_\psi[H] = \langle k \rangle_\psi[\langle h \rangle] = \langle k, h \mid k^2 = h^n = e, h^k = h^{-1} \rangle.$$

$\square$

Говорят, что группа G является *полупрямым произведением* своих подгрупп A и B , если выполняются следующие требования:

$$G = AB; \quad A \cap B = E; \quad B \triangleleft G.$$

Полупрямое произведение обозначают так: $G = A[B]$ или $G = [B]A$. Построенная в теореме 14.1 группа G является полупрямым произведением своих подгрупп K^* и H^* , т.е. $G = K^*[H^*]$.

ЛЕММА 2.48. Если $G = A[B]$, то

(1) каждый элемент $g \in G$ единственным образом представим в виде произведения $g = ab$, где $a \in A$, $b \in B$;

(2) если $a_1, a_2 \in A$ и $b_1, b_2 \in B$, то

$$(a_1 b_1)(a_2 b_2) = (a_1 a_2)(b_1^{a_2} b_2).$$

(1) Из равенства $G = AB$ следует, что каждый элемент $g \in G$ записывается в виде $g = ab$, где $a \in A$, $b \in B$. Если имеет место другая запись $g = a_1 b_1$, $a_1 \in A$, $b_1 \in B$, то $ab = a_1 b_1$, откуда $a^{-1} a_1 = b b_1^{-1} \in A \cap B = E$. Поэтому $a = a_1$, $b = b_1$ и каждый элемент $g \in G$ однозначно записывается в виде $g = ab$.

(2) $(a_1 b_1)(a_2 b_2) = a_1 a_2 a_2^{-1} b_1 a_2 b_2 = (a_1 a_2)(b_1^{a_2} b_2).$

Элемент порядка 2 называется *инволюцией*. *Диэдральной группой* называется группа, порожденная двумя различными инволюциями.

ТЕОРЕМА 2.49. Пусть G – группа. Тогда следующие утверждения эквивалентны:

- (1) группа G диэдральная;
- (2) группа $G = [A]B$, где

$$A = \langle a \rangle, \quad B = \langle b \rangle, \quad |B| = 2, \quad a^b = a^{-1}.$$

Пусть группа G диэдральная. Тогда существуют две инволюции i и j такие, что $G = \langle i, j \rangle$. Пусть $B = \langle j \rangle$, $a = ij$ и $A = \langle a \rangle$. Тогда

$$\begin{aligned} a^i &= (ij)^i = iijj = ji = (ij)^{-1} = a^{-1} \in A, \\ a^j &= (ij)^j = jijj = ji = (ij)^{-1} = a^{-1} \in A, \end{aligned}$$

поэтому $A \triangleleft G$ и $AB \leq G$. Так как $j \in B \leq AB$ и $aj = ijj = i \in AB$, то $G = \langle i, j \rangle = AB$. Если $E \neq A \cap B$, то $B \leq A$ и $i = j$ по следствию 3, с. 24, что противоречит определению диэдральной группы. Поэтому $A \cap B = E$ и $G = [A]B$.

Обратно, пусть группа $G = [A]B$, где

$$A = \langle a \rangle, \quad B = \langle b \rangle, \quad |B| = 2, \quad a^b = a^{-1}.$$

Тогда $abab = aa^{-1} = e$ и ab – инволюция. Так как $B = \langle b \rangle \leq \langle ab, b \rangle$ и $a = abb \leq \langle ab, b \rangle$, то $G \leq \langle ab, b \rangle$, т.е. $G = \langle ab, b \rangle$ – диэдральная группа.

Обычно диэдральную группу порядка $2n$ записывают так:

$$D_{2n} = \langle a, b \mid a^n = b^2 = e, \quad a^b = a^{-1} \rangle.$$

Отметим, что группа из примера 14.4 является диэдральной группой порядка $2n$.

Говорят, что группа G является *центральным произведением* своих подгрупп A и B , если выполняются следующие требования:

$$G = AB; \quad A \triangleleft G, \quad B \triangleleft G; \quad A \cap B \subseteq Z(G).$$

Очевидно, что прямое произведение двух подгрупп является центральным произведением. Кроме того, если $G = AB$ – центральное произведение, то

$$G/(A \cap B) = A/(A \cap B) \times B/(A \cap B)$$

будет прямым произведением.

ПРИМЕР 2.21. Над полем $\mathbb{Z}_5$ рассмотрим матрицы :

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}; \quad B = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}.$$

Так как $\det A = \det B = 1$, то A и $B \in SL(2, \mathbb{Z}_5)$. Вычислим порядки этих матриц. $A^2 = B^2 = 4E$; $A^4 = B^4 = E$;

$$A^3 = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix}; \quad B^3 = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}.$$

Итак, A и B – матрицы порядка 4 и

$$\langle A \rangle \cap \langle B \rangle = \langle 4E \rangle \subseteq Z(SL(2, \mathbb{Z}_5)).$$

Через Q обозначим группу, порожденную этими матрицами. Несложно проверить, что Q – группа порядка 8, являющаяся центральным произ-

ведением двух нормальных подгрупп $\langle A \rangle$ и $\langle B \rangle$. Так как

$$B^{-1}AB = B^3AB = A^3 = A^{-1},$$

то группу Q можно записать так:

$$Q = \langle A, B \mid A^4 = B^4 = E, A^2 = B^2, B^{-1}AB = A^{-1} \rangle.$$

Легко проверяются следующие свойства группы Q : $Z(Q) = \langle 4E \rangle$; все элементы из разности $Q \setminus Z(Q)$ имеют порядок 4; Q содержит единственную подгруппу порядка 2; каждая подгруппа нормальна. Группу Q называют *группой кватернионов*. Над полем комплексных чисел $\mathbb{C}$ матрицы

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}; \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

порождают подгруппу, изоморфную Q . □

2.8. Линейные группы

В примере 1.2, с. 14, введены полная линейная $GL(n, P)$ и специальная линейная $SL(n, P)$ группы степени n над полем P , а в примере 2.4, с. 54, показано, что $SL(n, P) \triangleleft GL(n, P)$ и факторгруппа $GL(n, P)/SL(n, P)$ изоморфна мультипликативной группе поля P .

Матрица, у которой ниже главной диагонали все элементы нули, а на диагонали все элементы единицы, называют *верхней унитреугольной* матрицей. Множество всех верхних унитреугольных матриц обозначают через $U(n, P)$. Очевидно, что $U(n, P)$ является группой.

Напомним, что характеристика конечного поля всегда простое число и если P — конечное поле характеристики p , то число элементов в поле P равно p^m , где m — некоторое натуральное число, т.е. $|P| = p^m$. Известно, что любые два конечных поля равных порядков изоморфны между собой.

Пусть поле P конечно и $|P| = p^m = q$. Если Q — другое поле порядка q , то поле Q изоморфно полю P . Этот факт доказывается в теории полей. Но отсюда следует, что группы $GL(n, P)$ и $GL(n, Q)$ изоморфны и вместо $GL(n, P)$ можно писать $GL(n, q)$. Аналогично, вместо $SL(n, P)$ будем писать $SL(n, q)$.

Заметим, что если $E_{p^n} = \langle a_1 \rangle + \dots + \langle a_n \rangle$ — элементарная абелева p -группа порядка p^n , записанная аддитивно, то можно рассматривать векторное пространство $V(n, p)$ над полем $\mathbb{Z}_p$ классов вычетов по простому модулю p , в котором аддитивной группой является группа E_{p^n} , а умножение на элементы из поля $\mathbb{Z}_p$ определяется по правилу: $[k]a = ka$, для любых $a \in E_{p^n}$ и

$$[k] = k + p\mathbb{Z} \in \mathbb{Z}_p.$$

При этом, очевидно,

$$\text{Aut}(E_{p^n}) = \text{Aut}V(n, p) = GL(n, p).$$

Таким образом, доказана

ТЕОРЕМА 2.50. *Элементарная абелева p -группа E_{p^n} порядка p^n изоморфна аддитивной группе векторного пространства $V(n, p)$ размерности n над полем $\mathbb{Z}_p$ из p элементов, а группа автоморфизмов $\text{Aut}E_{p^n}$ изоморфна полной линейной группе $GL(n, p)$.* □

ТЕОРЕМА 2.51. (1) $|GL(n, q)| = \prod_{i=0}^{n-1} (q^n - q^i)$;

(2) $|SL(n, q)| = q^{n-1} \prod_{i=0}^{n-2} (q^n - q^i)$.

(3) $|U(n, q)| = q^{n(n-1)/2}$.

(1) Пусть P — конечное поле порядка $q = p^m$, где p — простое число. Из элементов этого поля составляются строки невырожденных $n \times n$ -матриц. В каждой строке n элементов. Поэтому число всевозможных строк над полем P равно q^n . Подсчитаем теперь число всевозможных невырожденных $n \times n$ -матриц над полем P . Известно, что матрица является невырожденной тогда и только тогда, когда никакая строка этой матрицы не является линейной комбинацией остальных строк. Первая строка невырожденной матрицы может быть любой, кроме нулевой. Поэтому для первой строки существует $q^n - 1$ возможностей. Вторая строка может быть любой, непропорциональной первой строке. Коэффициентов пропорциональности столько, сколько элементов в поле P , т.е. q . Поэтому для второй строки существует $q^n - q$ возможностей. Третья строка невырожденной матрицы не должна быть линейной комбинацией первых двух строк. Очевидно, что число строк, являющихся линейной комбинацией двух строк, равно q^2 . Поэтому для третьей строки существует $q^n - q^2$ возможностей. И т.д. Наконец, последняя n -я строка не должна быть линейной комбинацией первых $(n-1)$ строк. Поэтому для последней строки существует $(q^n - q^{n-1})$ возможностей. Таким образом, число невырожденных матриц равно

$$(q^n - 1)(q^n - q) \dots (q^n - q^{n-1}) = \prod_{i=0}^{n-1} (q^n - q^i).$$

Это число равно порядку группы $GL(n, q)$.

(2) Так как $GL(n, P)/SL(n, P) \simeq P^\#$ и $|P^\#| = q - 1$, то

$$|SL(n, P)| = |GL(n, P)| / (q - 1) = \prod_{i=0}^{n-2} (q^n - q^i) q^{n-1}.$$

(3) В верхней унитарной матрице выше главной диагонали $(n^2 - n)/2$ мест. Поэтому $|U(n, q)| = q^{(n^2 - n)/2}$.

ТЕОРЕМА 2.52. Группа $U(n, p^m)$ является силовской p -подгруппой группы $GL(n, p^m)$ и группы $SL(n, p^m)$.

Пусть $q = p^m$, где p — простое число и $m \in \mathbb{N}$. Так как

$$|U(n, q)| = q^{n(n-1)/2}$$

и

$$\begin{aligned} |GL(n, q)| &= \prod_{i=0}^{n-1} (q^n - q^i) = q^{1+\dots+(n-1)} \prod_{i=0}^{n-1} (q^{n-i} - 1) = \\ &= q^{n(n-1)/2} \prod_{i=0}^{n-1} (q^{n-i} - 1), \end{aligned}$$

причем

$$\prod_{i=0}^{n-1} (q^{n-i} - 1)$$

не делится на p , то $U(n, q)$ — силовская p -подгруппа группы $GL(n, q)$.

Так как $U(n, q) \leq SL(n, q)$ и

$$|SL(n, q)| = |GL(n, q)| / (q - 1),$$

то $U(n, q)$ — силовская p -подгруппа группы $SL(n, q)$.

Обратим внимание, что в следующей теореме поле P произвольное.

ТЕОРЕМА 2.53. (1) *Центр группы $GL(n, P)$ состоит из скалярных матриц.*

(2) *Центр группы $SL(n, P)$ состоит из скалярных матриц с единичным определителем.*

(1) Через E_{ij} обозначим при $i = j$ единичную матрицу, а при $i \neq j$ — матрицу, которая получается из единичной добавлением единицы на пересечении i -й строки и j -го столбца. Так как $\det E_{ij} = 1$, то $E_{ij} \in SL(n, P)$. Пусть $B = (b_{ij})$ — произвольная матрица, перестановочная с каждой матрицей E_{ij} . Так как

$$BE_{ij} = \begin{pmatrix} b_{11} & \dots & b_{1j-1} & b_{1j} + b_{1i} & b_{1j+1} & \dots & b_{1n} \\ b_{21} & \dots & b_{2j-1} & b_{2j} + b_{2i} & b_{2j+1} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_{n1} & \dots & b_{nj-1} & b_{nj} + b_{ni} & b_{nj+1} & \dots & b_{nn} \end{pmatrix},$$

а

$$E_{ij}B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{i-11} & \dots & b_{i-1n} \\ b_{i1} + b_{j1} & \dots & b_{in} + b_{jn} \\ b_{i+11} & \dots & b_{i+1n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix},$$

то из равенства $BE_{ij} = E_{ij}B$ получаем, что

$$\begin{cases} b_{1j} + b_{1i} = b_{1j} \\ b_{2j} + b_{2i} = b_{2j} \\ \dots \\ b_{i-1j} + b_{i-1i} = b_{i-1j} \\ b_{ij} + b_{ii} = b_{ij} + b_{jj} \\ b_{i+1j} + b_{i+1i} = b_{i+1j} \\ \dots \\ b_{nj} + b_{ni} = b_{nj} \end{cases}$$

Отсюда следует, что

$$b_{1i} = b_{2i} = \dots = b_{(i-1)i} = b_{(i+1)i} = \dots = b_{ni} = 0,$$

а $b_{ii} = b_{jj}$. Таким образом, при $i, j = 1, \dots, n$ получаем, что B — скалярная матрица. Таким образом, если матрица B перестановочна с каждой матрицей E_{ij} , то B — скалярная матрица.

Если αE — скалярная матрица, $\alpha \in P^\#$, то $\alpha E \cdot A = A\alpha E$ для любой матрицы $A \in GL(n, P)$, поэтому $\alpha E \in Z(GL(n, P))$.

Обратно, если матрица $B \in Z(GL(n, P))$, то она перестановочна с каждой матрицей из $GL(n, P)$, в частности, с каждой матрицей E_{ij} , $i, j = 1, \dots, n$. Поэтому матрица B будет скалярной. Таким образом, $Z(GL(n, P)) = \{\alpha E \mid \alpha \in P^\#\}$.

(2) Из определения центра получаем, что

$$Z(GL(n, P)) \cap SL(n, P) \subseteq Z(SL(n, P)).$$

Обратно, если $B \in Z(SL(n, P))$, то матрица B перестановочна со всеми матрицами из $SL(n, P)$, в частности, с каждой матрицей E_{ij} , $i, j = 1, \dots, n$. Поэтому B — скалярная матрица и $B \in Z(GL(n, P))$. Отсюда следует, что

$$Z(SL(n, P)) \subseteq Z(GL(n, P)),$$

поэтому

$$Z(SL(n, P)) = Z(GL(n, P)) \cap SL(n, P).$$

СЛЕДСТВИЕ. (1) $|Z(GL(n, q))| = q - 1$;

(2) $|Z(SL(n, q))| = (n, q - 1)$.

(1) Так как $Z(GL(n, q))$ состоит из скалярных матриц, то число таких матриц равно числу ненулевых элементов поля P , поэтому это число равно $q - 1$.

(2) $Z(SL(n, q))$ состоит из скалярных матриц αE , $\alpha \in P^\#$, для которых $\alpha^n = 1$. Так как мультипликативная группа поля P циклическая, то число решений уравнения $\alpha^n = 1$ равно наибольшему общему делителю n и $q - 1$.

Факторгруппу $GL(n, q)/Z(GL(n, q))$ называют *проективной полной (общей) линейной группой* и обозначают через $PGL(n, q)$. Факторгруппу $SL(n, q)/Z(SL(n, q))$ называют *проективной специальной линейной группой* и обозначают через $PSL(n, q)$.

СЛЕДСТВИЕ. (1) $|PGL(n, q)| = |SL(n, q)| = q^{n-1} \prod_{i=0}^{n-2} (q^n - q^i)$;

(2) $|PSL(n, q)| = d^{-1} |SL(n, q)| =$

$$= d^{-1} q^{n-1} \prod_{i=0}^{n-2} (q^n - q^i), \text{ где } d = (n, q - 1).$$

Оба утверждения вытекают из теоремы 2.51 и следствия 8.

Для $n = 2$ получаем

СЛЕДСТВИЕ. (1) $|GL(2, q)| = (q^2 - 1)(q^2 - q)$;

(2) $|SL(2, q)| = q(q^2 - 1)$;

(3) $|PGL(2, q)| = q(q^2 - 1)$;

(4) $|PSL(2, q)| =$

$$= \begin{cases} 2^m(2^m - 1)(2^m + 1), & \text{при } q = 2^m; \\ (1/2)p^m(p^m - 1)(p^m + 1), & \text{при } q = p^m, p > 2. \end{cases}$$

ТЕОРЕМА 2.54. (1) $GL(2, 2^m) = Z(GL(2, 2^m)) \times SL(2, 2^m)$. В частности,

$$PGL(2, 2^m) \simeq SL(2, 2^m) = PSL(2, 2^m).$$

(2) При $p > 2$ группа $PGL(2, p^m)$ содержит нормальную подгруппу индекса 2, изоморфную $PSL(2, p^m)$.

(1) Ясно, что обе подгруппы $Z(GL(2, 2^m))$ и $SL(2, 2^m)$ нормальны в $GL(2, 2^m)$. По теореме 2.53

$$Z(GL(2, 2^m)) \cap SL(2, 2^m) = Z(SL(2, 2^m)).$$

Но если $D \in Z(SL(2, 2^m))$, то D — скалярная матрица с единичным определителем, т.е. $D = \gamma E$, $\gamma^2 = 1$. Так как $\gamma \in P^\#$ и $|P^\#| = 2^m - 1$ — нечетное число, то по теореме Лагранжа в мультипликативной группе поля P нет элементов порядка 2. Поэтому $\gamma = e$ и D — единичная матрица. Таким образом,

$$Z(SL(2, 2^m)) = Z(GL(2, 2^m)) \cap SL(2, 2^m) = E,$$

в частности, $SL(2, 2^m) = PSL(2, 2^m)$.

Так как

$$\begin{aligned} |Z(GL(2, 2^m)) \cdot SL(2, 2^m)| &= |Z(GL(2, 2^m))| \times \\ &\times |SL(2, 2^m)| = |GL(2, 2^m)|, \end{aligned}$$

то все требования прямого произведения выполняются и

$$GL(2, 2^m) = Z(GL(2, 2^m)) \times SL(2, 2^m).$$

Отсюда, в частности, следует, что

$$PGL(2, 2^m) = GL(2, 2^m)/Z(GL(2, 2^m)) \simeq SL(2, 2^m).$$

(2) Пусть $p > 2$ и $K = Z(GL(2, p^m)) \cdot SL(2, p^m)$. Ясно, что K — нормальная подгруппа группы $GL(2, p^m)$. По следствию 8

$$|Z(GL(2, p^m)) \cap SL(2, p^m)| = |Z(SL(2, p^m))| = 2.$$

Поэтому,

$$\begin{aligned} |K| &= \frac{|Z(GL(2, p^m))| \cdot |SL(2, p^m)|}{|Z(GL(2, p^m)) \cap SL(2, p^m)|} = \\ &= \frac{(p^m - 1)p^m(p^{2m} - 1)}{2} = \frac{|GL(2, p^m)|}{2}, \end{aligned}$$

т.е. индекс K в группе $GL(2, p^m)$ равен 2. Кроме того, $PGL(2, p^m) = GL(2, p^m)/Z(GL(2, p^m))$ содержит подгруппу

$$\begin{aligned} K/Z(GL(2, p^m)) &= Z(GL(2, p^m))SL(2, p^m)/Z(GL(2, p^m)) \simeq \\ &\simeq SL(2, p^m)/Z(GL(2, p^m)) \cap SL(2, p^m) = \\ &= SL(2, p^m)/Z(SL(2, p^m)) = PSL(2, p^m), \end{aligned}$$

которая имеет индекс 2.

Доказательство следующей теоремы можно найти в книге Хупперта [26], теорема II.8.27.

ТЕОРЕМА 2.55. Группа $PSL(2, p^m)$ содержит только следующие подгруппы:

(1) элементарные абелевы p -группы порядков $p, p^2, \dots, p^m$;

- (2) циклические группы порядка z , где z делит $(p^m \pm 1)/d$, $d = (2, p^m - 1)$;
- (3) диэдральные группы порядка $2z$, где число z как в (2);
- (4) A_4 при $p > 2$ или $p = 2$ и m четное;
- (5) S_4 при $p^{2m} \equiv 1 \pmod{16}$;
- (6) A_5 при $p = 5$ или $p^{2m} \equiv 1 \pmod{5}$;
- (7) полупрямое произведение элементарной абелевой группы порядка p^k с циклической группой порядка t , причем t делит $p^k - 1$ и t делит $(p^m - 1)/d$;
- (8) группы $SL(2, p^k)$ при k , делящем m , и $PGL(2, p^k)$ при $2k$, делящем m . □

ГЛАВА 3. АБЕЛЕВЫ И НИЛЬПОТЕНТНЫЕ ГРУППЫ

В этой главе и в последующих главах рассматриваются только конечные группы.

2.9. Строение конечных абелевых групп

В этом параграфе доказывается следующая

ТЕОРЕМА 2.56. *Конечная абелева группа является прямым произведением примарных циклических подгрупп. Любые два таких разложения имеют одинаковое число сомножителей каждого порядка.*

Вначале утверждение теоремы 16.1 докажем для примарных абелевых групп. Для этого потребуется следующая

ЛЕММА 2.57. *Если H — циклическая подгруппа наибольшего порядка примарной абелевой группы P , то существует подгруппа K такая, что $P = H \times K$.*

Доказательство. Пусть P — группа порядка p^n . Воспользуемся индукцией по n . Если $n = 1$, то P — циклическая группа, $H = P$ и $P = H \times E$ — требуемое разложение, т.е. при $n = 1$ лемма справедлива. Предположим, что лемма верна для всех p -групп порядка $< p^n$.

По теореме Силова в группе P имеются циклические подгруппы порядка p , поэтому $|H| \geq p$ и факторгруппа P/H имеет порядок $< p^n$, т.е. к P/H применима индукция. Предположим, что P/H — нециклическая группа. Выберем в ней циклическую подгруппу T/H наибольшего порядка. По индукции существует подгруппа S/H такая, что

$$P/H = T/H \times S/H.$$

Так как P/H нециклическая, а T/H циклическая, то $P/H \neq T/H$ и подгруппы T и S собственные в P . К ним также применима индукция, по которой

$$T = H \times T_1, \quad S = H \times S_1.$$

Из того, что

$$T/H \cap S/H = H/H$$

следует, что $T \cap S = H$ и $T_1 \cap S_1 = E$. Теперь,

$$P = TS = (H \times T_1)(H \times S_1) = H \times (T_1 S_1)$$

и лемма справедлива.

Пусть теперь факторгруппа P/H циклическая, $\langle gH \rangle = P/H$ и $|P/H| = p^a$. Тогда

$$(gH)^{p^a} = g^{p^a} H = H$$

и p^a — наименьшая степень элемента g , при которой $g^{p^a} \in H$. Ясно, что $P = H \langle g \rangle$.

Если $g^{p^a} = e$, то $\langle g \rangle \cap H = E$ и произведение $P = H \langle g \rangle$ будет прямым. Значит, $P = H \times \langle g \rangle$.

Пусть $g^{p^a} \neq e$. По выбору $H = \langle h \rangle$ — циклическая подгруппа группы P наибольшего порядка. Пусть $|H| = p^b$. Так как $g^{p^a} \in H$, то $g^{p^a} = h^t$, где

$0 < t < p^b$. Пусть $t = mp^c$ и простое число p не делит m . Элементы h и h^m имеют порядок p^b по лемме 1.23, с. 23, поэтому h^t имеет порядок p^{b-c} . Теперь

$$(g^{p^a})^{p^{b-c}} = (h^{p^c m})^{p^{b-c}} = (h^{p^{b-c}})^{mp^c} = e$$

и g — элемент порядка p^{a+b-c} . По выбору подгруппы H порядок элемента g не должен превышать порядок элемента h , т.е. $a + b - c \leq b$ и $c - a \geq 0$. Теперь число p^{c-a} натуральное и можно ввести элемент $f = gh^{-mp^{c-a}}$. Поскольку

$$f^{p^a} = (gh^{-mp^{c-a}})^{p^a} = g^{p^a} h^{-mp^c} = h^t h^{-t} = e,$$

то f — элемент порядка p^a . Кроме того, $fH = gh^{-mp^{c-a}}H = gH$. Поэтому $P = \langle f \rangle H$, а так как

$$p^a = |f| = |P : H|,$$

то $\langle f \rangle \cap H = E$ и $P = \langle f \rangle \times H$.

ТЕОРЕМА 2.58. *Конечная абелева примарная группа является прямым произведением своих циклических подгрупп. Если имеется два таких разложения*

$$P = P_1 \times P_2 \times \dots \times P_r = Q_1 \times Q_2 \times \dots \times Q_s,$$

то $r = s$ и при подходящей нумерации $|P_i| = |Q_i|$ для всех i .

Воспользуемся индукцией по $|P|$. Пусть теорема верна для всех абелевых p -групп порядка меньше, чем $|P|$. Выберем в P циклическую подгруппу P_1 наибольшего порядка p^{a_1} . Тогда $P = P_1 \times K$ по лемме 2.57. По индукции

$$K = P_2 \times \dots \times P_r$$

и первое утверждение теоремы доказано.

Для получения второго утверждения удобно множители расположить так, чтобы их порядки не возрастали, т.е.

$$\begin{aligned} P &= \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_r \rangle, \quad |g_i| = p^{a_i}, &< 1 > \\ a_1 &\geq a_2 \geq \dots \geq a_k \geq a_{k+1} = a_{k+2} = \dots = a_r = 1; \\ P &= \langle h_1 \rangle \times \langle h_2 \rangle \times \dots \times \langle h_s \rangle, \quad |h_i| = p^{b_i}, &< 2 > \\ b_1 &\geq b_2 \geq \dots \geq b_l \geq b_{l+1} = b_{l+2} = \dots = b_s = 1; \end{aligned}$$

Рассмотрим множество

$$P^p = \{x^p \mid x \in P\}$$

всех p -х степеней элементов из P . Так как P — абелева группа, то

$$x^p y^p = (xy)^p \in P^p, \quad (x^p)^{-1} = (x^{-1})^p \in P^p$$

и P^p — подгруппа. Кроме того, $P_i^p = \langle g_i^p \rangle$ — подгруппа индекса p в группе P_i , т.е. $|P_i^p| = p^{a_i-1}$.

В соответствии с разложениями $<1>$ и $<2>$ каждый элемент группы P представим в виде

$$x = g_1^{t_1} \dots g_r^{t_r} = h_1^{m_1} \dots h_s^{m_s},$$

поэтому

$$x^p = g_1^{pt_1} \dots g_k^{pt_k} = h_1^{pm_1} \dots h_l^{pm_l}$$

и

$$P^p = P_1^p \times P_2^p \times \dots \times P_k^p = Q_1^p \times Q_2^p \times \dots \times Q_l^p \quad < 3 >$$

— два разложения подгруппы P^p в прямые произведения циклических подгрупп. Так как $|P_i^p| = |P_i|/p$, то $|P^p| < |P|$ и к группе P^p применима индукция. Из $<3>$ заключаем, что $k = l$ и $|P_i^p| = |Q_i^p|$ для всех i . Теперь, $p^{a_i-1} = p^{b_i-1}$ и $a_i = b_i$ для всех $i = 1, 2, \dots, k$. Таким образом, $|P_i| = |Q_i|$ для $i = 1, 2, \dots, k$.

Пусть

$$p^d = |P_1 \times \dots \times P_k| = |Q_1 \times \dots \times Q_k|.$$

Тогда из $<1>$ и $<2>$ заключаем, что

$$\begin{aligned} |P| &= p^d |P_{k+1} \times \dots \times P_r| = \\ p^d p^{r-k} &= p^d |Q_{k+1} \times \dots \times Q_s| = p^d p^{s-k}. \end{aligned}$$

Поэтому $r = s$ и теорема полностью доказана.

ТЕОРЕМА 2.59. *Каждая конечная абелева группа является прямым произведением своих силовских подгрупп. Для каждого простого числа p силовская p -подгруппа в абелевой группе единственна.*

Пусть G — абелева группа порядка $n = p_1^{a_1} p_2^{a_2} \dots p_t^{a_t}$, где $p_1, p_2, \dots, p_t$ — попарно различные простые числа. По теореме Силова в группе G существуют силовские подгруппы $G_{p_1}, G_{p_2}, \dots, G_{p_t}$, соответствующие простым числам $p_1, p_2, \dots, p_t$. Силовские подгруппы нормальны в G , поскольку группа G абелева. Кроме того, порядки G_{p_1} и G_{p_2} взаимно просты, поэтому

$$G_{p_1} \cap G_{p_2} = E; \quad |G_{p_1} G_{p_2}| = |G_{p_1}| |G_{p_2}|.$$

Это означает, что $G_{p_1} G_{p_2} = G_{p_1} \times G_{p_2}$. Предположим, что для некоторого k уже доказали, что

$$G_{p_1} G_{p_2} \dots G_{p_k} = G_{p_1} \times G_{p_2} \times \dots \times G_{p_k}.$$

Тогда подгруппа $H = G_{p_1} \times \dots \times G_{p_k}$ имеет порядок $p_1^{a_1} \dots p_k^{a_k}$, а пересечение $H \cap G_{p_{k+1}}$ — подгруппа порядка делящего $|H|$ и $|G_{p_{k+1}}|$. Отсюда следует, что $H \cap G_{p_{k+1}} = E$. Так как H и $G_{p_{k+1}}$ — нормальные подгруппы, то $H G_{p_{k+1}} = H \times G_{p_{k+1}}$. Итак,

$$G_{p_1} \dots G_{p_{k+1}} = G_{p_1} \times \dots \times G_{p_{k+1}}.$$

Теперь согласно индукции, группа G разложима в прямое произведение своих силовских подгрупп.

Так как силовские p -подгруппы конечной группы сопряжены между собой, то для каждого простого p силовская p -подгруппа в абелевой группе единственна.

Доказательство теоремы 16.1. Утверждение теоремы 16.1 является следствием теоремы 16.4 и теоремы 16.3. Действительно, по теореме 16.4 каждая конечная абелева группа разлагается в прямое произведение своих силовских подгрупп. По теореме 16.3 каждая силовская подгруппа является прямым произведением своих циклических подгрупп. Поэтому каждая конечная абелева группа разложима в прямое произведение своих циклических примарных подгрупп.

В конечной абелевой группе G силовская p -подгруппа G_p единственна для каждого простого p . По теореме 16.3 любые два разложения подгруппы G_p в прямое произведение циклических подгрупп имеют одинаковое число множителей каждого порядка. Поэтому и любые два разложения группы G в прямое произведение примарных циклических подгрупп имеют одинаковое число множителей каждого порядка. $\square$

Вернемся к теореме 16.3. По теореме 1.31, с. 26, все циклические группы одного порядка изоморфны, поэтому циклическую группу можно задать её порядком.

Пусть абелева p -группа P порядка p^a разлагается в прямое произведение

$$P = P_1 \times P_2 \times \dots \times P_r \quad <4>$$

циклических подгрупп $P_1, P_2, \dots, P_r$ порядков $p^{a_1}, p^{a_2}, \dots, p^{a_r}$. Ясно, что

$$a = a_1 + a_2 + \dots + a_r.$$

Порядки $(p^{a_1}, p^{a_2}, \dots, p^{a_r})$ циклических множителей прямого произведения $<4>$ называют *инвариантами* абелевой p -группы P .

Если две абелевы группы P и Q имеют одинаковые инварианты $(p^{a_1}, p^{a_2}, \dots, p^{a_r})$, то

$$P = P_1 \times P_2 \times \dots \times P_r, \quad Q = Q_1 \times Q_2 \times \dots \times Q_r$$

и $|P_i| = |Q_i| = p^{a_i}$ для $i = 1, 2, \dots, r$. Поэтому существуют изоморфизмы $\varphi_i : P_i \rightarrow Q_i$, при которых элемент $g_i \in P_i$ отображается в элемент $\varphi_i(g_i) \in Q_i$. По свойствам прямых произведений любой элемент из P однозначно представим в виде $g_1 g_2 \dots g_r$, где $g_i \in P_i$. Поэтому отображение

$$\varphi(g_1 g_2 \dots g_r) = \varphi_1(g_1) \varphi_2(g_2) \dots \varphi_r(g_r)$$

будет изоморфизмом групп P и Q . Тем самым доказана следующая теорема.

ТЕОРЕМА 2.60. *Примарная абелева группа однозначно определяется своими инвариантами.* $\square$

Для построения произвольных, не обязательно примарных, абелевых групп порядка n поступают следующим образом. Выписывают все возможные инварианты каждой силовской подгруппы, а затем, комбинируя инвариантами силовских подгрупп получают все возможные абелевы группы порядка n .

ПРИМЕР 2.22. Перечислим все абелевы группы порядка 16.

Через C_n условимся обозначать циклическую группу порядка n . Группа порядка $16 = 2^4$ может обладать следующими инвариантами:

$$(2^4), (2^3, 2), (2^2, 2^2), (2^2, 2, 2), (2, 2, 2, 2),$$

которым соответствуют следующие группы:

$$C_{16}, C_8 \times C_2, C_4 \times C_4, C_4 \times C_2 \times C_2, \\ C_2 \times C_2 \times C_2 \times C_2.$$

Таким образом, абелевы группы порядка 16 могут быть одного из пяти указанных видов. $\square$

ПРИМЕР 2.23. Перечислим все абелевы группы порядка 1000.

Так как $1000 = 2^3 5^3$, то для силовских подгрупп возможны следующие ситуации. Силовская 2-подгруппа имеет порядок 2^3 , и она либо C_8 , либо $C_4 \times C_2$, либо $C_2 \times C_2 \times C_2$. Силовская 5-подгруппа имеет порядок 5^3 , и

она либо C_{125} , либо $C_{25} \times C_5$, либо $C_5 \times C_5 \times C_5$. Таким образом, абелева группа порядка 1000 может быть только одной из следующих групп:

$$\begin{aligned} & C_8 \times C_{125}, C_8 \times C_{25} \times C_5, C_8 \times C_5 \times C_5 \times C_5, \\ & C_4 \times C_2 \times C_{125}, C_4 \times C_2 \times C_{25} \times C_5, C_4 \times C_2 \times C_5 \times C_5, \\ & C_2 \times C_2 \times C_2 \times C_{125}, C_2 \times C_2 \times C_2 \times C_{25} \times C_5, \\ & C_2 \times C_2 \times C_2 \times C_5 \times C_5 \times C_5. \end{aligned}$$

□

2.10. Примарные группы

Напомним, что p -группой называют группу, порядок которой есть степень простого числа p . Ясно, что подгруппы и факторгруппы любой p -группы также являются p -группами. *Примарной* называют группу, которая является p -группой для некоторого простого p .

ТЕОРЕМА 2.61. *Центр неединичной примарной группы отличен от единицы.*

Пусть P — p -группа порядка p^n и

$$K_1, K_2, \dots, K_t$$

— все различные классы сопряженных элементов группы P , $K_i = \{g_i^x \mid x \in P\}$. По следствию 5, с. 37, число элементов в классе сопряженных с g_i элементов равно индексу централизатора элемента g_i , т.е.

$$|K_i| = |P : C_P(g_i)| = p^{a_i}.$$

Поэтому каждый элемент центра группы составляет отдельный класс и наоборот, если $|K_j| = 1$, то $g_j \in Z(P)$, где $Z(P)$ — центр группы P . Итак,

$$P = K_1 \cup K_2 \cup \dots \cup K_t,$$

где $K_i \cap K_j = \emptyset$ при $i \neq j$. Пусть $K_1 = \{e\}$. Тогда

$$p^n = 1 + p^{a_2} + \dots + p^{a_t}.$$

Отсюда следует, что существует $l > 1$ такое, что $a_l = 0$. Но тогда

$$1 = p^{a_l} = |P : C_P(g_l)|$$

и $g_l \in Z(P)$.

ТЕОРЕМА 2.62. *В примарной группе каждая собственная подгруппа отлична от своего нормализатора.*

Пусть P — p -группа и A — собственная подгруппа в P . Рассмотрим разложение группы P в двойные смежные классы по подгруппе A .

$$P = Ax_1A \cup Ax_2A \cup \dots \cup Ax_tA = A \cup (\cup_{i=2}^t Ax_iA). \quad <1>$$

Здесь $x_1 = e$. Используя теорему 1.42, с. 34, получаем

$$|Ax_iA| = |A^{x_i}A| = |A^{x_i}| |A| / |A^{x_i} \cap A|.$$

Из <1> получаем

$$|P| = |A| + \sum_{i=2}^t |A^{x_i}| |A| / |A^{x_i} \cap A|. \quad <2>$$

Введем обозначения: $|P| = p^n$, $|A| = p^a$. Тогда из <2> следует, что

$$p^{n-a} = 1 + \sum_{i=2}^t |A| / |A^{x_i} \cap A|.$$

Так как $p^{n-a} > 1$, то в правой части равенства под знаком суммы существуют слагаемые равные единице, т.е. существует номер $j \geq 2$ такой, что $|A| = |A^{x_j} \cap A|$. Это означает, что $A^{x_j} = A$ и $x_j \in N_P(A)$. Ввиду того, что $j \geq 2$ элемент x_j не принадлежит A и A — собственная подгруппа в $N_P(A)$.

СЛЕДСТВИЕ. В примарной группе все максимальные подгруппы нормальны и имеют простые индексы.

Пусть P — p -группа и $M < P$. По теореме 17.2 подгруппа M — собственная подгруппа в своем нормализаторе $N_P(M)$. Из максимальности M следует, что $N_P(M) = P$ и $M \triangleleft P$. По теореме о соответствии в факторгруппе P/M нет нетривиальных подгрупп (т.е. подгрупп отличных от единичной подгруппы и всей группы), поэтому по теореме Силова группа P/M имеет простой порядок.

ТЕОРЕМА 2.63. В примарной группе пересечение неединичной нормальной подгруппы с центром группы отлично от единицы.

Пусть P — p -группа и $A \triangleleft P$, $A \neq 1$. Требуется доказать, что $A \cap Z(P) \neq 1$. Если a — произвольный элемент из A , то $a^x \in A^x = A$ для любого элемента $x \in P$. Поэтому A состоит из классов сопряженных элементов группы P , т.е.

$$A = K_1 \cup K_2 \cup \dots \cup K_t,$$

где $K_i = a_i^P$. Можно положить, что $K_1 = \{e\}$. Поскольку

$$|K_i| = |P : C_P(a_i)|,$$

то считая $|A| = p^n$, $|K_i| = p^{n_i}$ получаем

$$p^n = 1 + \sum_{i=2}^t p^{n_i}.$$

Теперь ясно, что существует $j \geq 2$ такое, что $p^{n_j} = |K_j| = 1$ и $a_j \in Z(P)$.

СЛЕДСТВИЕ. Нормальная подгруппа простого порядка примарной группы содержится в центре группы. □

СЛЕДСТВИЕ. Минимальная нормальная подгруппа примарной группы имеет простой порядок и содержится в центре группы.

Пусть P — p -группа и $N \cdot \triangleleft P$. Так как $N \neq E$, то $N \cap Z(P) \neq E$, а поскольку $N \cap Z(P) \triangleleft P$, то $N \leq Z(P)$. В N существует элемент a простого порядка по теореме Силова. Поэтому $\langle a \rangle \triangleleft P$ и из условия $N \cdot \triangleleft P$ следует, что $N = \langle a \rangle$.

2.11. Нильпотентные группы

Группа называется *нильпотентной*, если все ее силовские подгруппы нормальны. В абелевой группе все подгруппы нормальны, поэтому каждая абелева группа нильпотентна. Примарная группа совпадает со своей силовской подгруппой, поэтому каждая примарная группа нильпотентна. В симметрической группе S_3 силовская 2-подгруппа $\langle (12) \rangle$ ненормальна, поэтому группа S_3 ненильпотентна.

ЛЕММА 2.64. *Нильпотентная группа является прямым произведением своих силовских подгрупп.*

Пусть G — нильпотентная группа и

$$|G| = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

где все простые числа p_i различны, и пусть P_i — силовская p_i -подгруппа группы G . Так как P_1 и $P_2 \triangleleft G$, то $P_1 P_2 \triangleleft G$, а поскольку $P_1 \cap P_2 = E$, то $P_1 P_2 = P_1 \times P_2$. Далее

$$(P_1 P_2) P_3 \triangleleft G, \quad P_1 P_2 \cap P_3 = E,$$

поэтому

$$(P_1 P_2) P_3 = P_1 \times P_2 \times P_3,$$

и т.д. Через n шагов с учетом теоремы 1.65, с. 47, получаем, что

$$G = P_1 P_2 \dots P_n = P_1 \times P_2 \times \dots \times P_n.$$

ЛЕММА 2.65. (1) *Подгруппа и факторгруппа нильпотентной группы нильпотентны.*

(2) *Прямое произведение нильпотентных групп является нильпотентной группой.*

(1) Пусть G — нильпотентная группа, $H \leq G$ и P_1 — силовская p -подгруппа группы H . Так как в любой группе силовские p -подгруппы сопряжены между собой, то в нильпотентной группе силовская p -подгруппа единственна для каждого простого p . Поэтому $P_1 \leq P \cap H$, где P — силовская p -подгруппа группы G . Из того, что $P \cap H$ — p -группа и $|H : P_1|$ не делится на p получаем, что $P_1 = P \cap H$. Но $P \triangleleft G$, поэтому $P_1 \triangleleft H$ и H нильпотентна.

Пусть $N \triangleleft G$. По теореме 1.65, с. 47, подгруппа PN/N — силовская в G/N и $PN/N \triangleleft G/N$ по теореме о соответствии. Поэтому G/N нильпотентна.

(2) Пусть

$$G = G_1 \times \dots \times G_n$$

и группа G_i нильпотентна для любого $i = 1, 2, \dots, n$. Пусть p — простое число и P_i — силовская p -подгруппа группы G_i . Так как $P_i \triangleleft G_i$ и в прямом произведении элементы из различных множителей перестановочны, то $P_i \triangleleft G$ и

$$P = P_1 \times \dots \times P_n \triangleleft G.$$

Кроме того, $|P| = \prod_{i=1}^n |P_i|$ и P — p -группа. Ясно, что

$$|G : P| = \prod_{i=1}^n |G_i : P_i|,$$

поэтому $|G : P|$ не делится на p и P — силовская p -подгруппа группы G .

Напомним, что $\pi(X)$ — множество всех простых делителей порядка группы X .

ТЕОРЕМА 2.66. (1) *Центр $Z(G)$ неединичной нильпотентной группы G отличен от единицы и $\pi(Z(G)) = \pi(G)$.*

(2) *В нильпотентной группе каждая собственная подгруппа отлична от своего нормализатора.*

(3) В нильпотентной группе G пересечение неединичной нормальной подгруппы N с центром группы отлично от единицы и $\pi(N) = \pi(N \cap Z(G))$.

(1) Пусть G — неединичная нильпотентная группа. По лемме 18.1 группа G есть прямое произведение своих силовских подгрупп. Но центр каждой силовской подгруппы отличен от E по теореме 17.1. Так как по лемме 2.27, с. 67, центр прямого произведения равен прямому произведению центров сомножителей, то $Z(G) \neq E$. Если $p \in \pi(G)$ и P — силовская p -подгруппа группы G , то $E \neq Z(P) \leq Z(G)$ и $p \in \pi(Z(G))$. Поэтому $\pi(Z(G)) = \pi(G)$.

(2) Пусть теперь G — нильпотентная группа и $H < G$. По лемме 18.1 группа

$$G = P_1 \times P_2 \times \dots \times P_n,$$

где P_i — силовская p_i -подгруппа, а по лемме 18.2 подгруппа

$$H = (H \cap P_1) \times (H \cap P_2) \times \dots \times (H \cap P_n),$$

где $H \cap P_i$ — силовская p_i -подгруппа из H . Так как H — собственная подгруппа в G , то существует номер j такой, что $H \cap P_j$ — собственная подгруппа в P_j . По теореме 17.2 подгруппа $N_{P_j}(H \cap P_j)$ содержит элемент x_j , не принадлежащий $H \cap P_j$. Теперь x_j не принадлежит H , но $x_j \in N_G(H)$.

(3) Пусть опять G — нильпотентная группа и $E \neq N \triangleleft G$. Пусть $p \in \pi(N)$ и P_1 — силовская p -подгруппа в N , а P — силовская подгруппа в G , содержащая P_1 . Так как G и N нильпотентны, то $P_1 \triangleleft N$, а $P \triangleleft G$. По лемме Фраттини

$$G = NN_G(P_1) = N_G(P_1),$$

т.е. $P_1 \triangleleft G$. Теперь $P_1 \triangleleft P$ и по теореме 17.4 пересечение $P_1 \cap Z(P) \neq E$. Так как центр группы G совпадает с прямым произведением центров силовских подгрупп, то

$$E \neq P_1 \cap Z(P) \leq N \cap Z(G)$$

и $p \in \pi(N \cap Z(G))$. Поэтому $\pi(N) \subseteq \pi(N \cap Z(G))$. Поскольку $N \cap Z(G) \leq Z(N)$, то

$$\pi(N \cap Z(G)) \subseteq \pi(Z(N)) = \pi(N).$$

Следовательно, $\pi(N) = \pi(N \cap Z(G))$.

СЛЕДСТВИЕ. В нильпотентной группе все максимальные подгруппы нормальны и имеют простые индексы.

Пусть G — нильпотентная группа и $M < \cdot G$. По теореме 18.3(2) подгруппа M — собственная подгруппа в своем нормализаторе $N_G(M)$. Из максимальной M следует, что $N_G(M) = G$ и $M \triangleleft G$. По теореме о соответствии в факторгруппе G/M нет нетривиальных подгрупп (т.е. подгрупп отличных от единичной подгруппы и всей группы), поэтому по теореме Силова группа G/M имеет простой порядок.

СЛЕДСТВИЕ. Минимальная нормальная подгруппа нильпотентной группы имеет простой порядок и содержится в центре группы.

Пусть N — минимальная нормальная подгруппа нильпотентной группы G . Так как $N \neq E$, то $N \cap Z(G) \neq E$ по теореме 18.3(3). Поскольку $N \cap Z(G) \triangleleft G$ и $N \cdot \triangleleft G$, то $N \leq Z(G)$. Теперь все подгруппы из N нормальны

в G . По теореме Силова в N существует подгруппа N_1 простого порядка. Так как $N_1 \triangleleft G$, то $N_1 = N$.

ТЕОРЕМА 2.67. *Для группы G следующие требования эквивалентны:*

- (1) G — нильпотентная группа;
- (2) G — прямое произведение своих силовских подгрупп;
- (3) каждая собственная подгруппа отлична от своего нормализатора;
- (4) все максимальные подгруппы нормальны;
- (5) все подгруппы группы G субнормальны.

Из (1) следует (2), (3) и (4) в силу леммы 18.1 и теоремы 18.3. Из (2) следует (1) по определению прямого произведения. Из (3) следует (4). Пусть выполняется (4), т.е. в группе G все максимальные подгруппы нормальны. Предположим, что группа G ненильпотентна. Тогда в G существует ненормальная силовская подгруппа P . Пусть M — максимальная подгруппа группы G , содержащая $N_G(P)$. По условию $M \triangleleft G$, а по лемме Фраттини $G = MN_G(P) = M$, противоречие. Значит допущение неверно и из (4) следует (1). Из (3) следует (5), а из (5) следует (3).

ЛЕММА 2.68. *Если N — максимальная абелева нормальная подгруппа нильпотентной группы G , то $C_G(N) = N$.*

Пусть $C = C_G(N)$ и предположим, что $N \neq C$. Тогда $N < C$ и C/N — неединичная нормальная по лемме 1.53, с. 39, подгруппа нильпотентной группы G/N . По теореме 18.3 $C/N \cap Z(G/N) \neq E$. Пусть $N < H \leq G$ и H/N — подгруппа простого порядка из $C/N \cap Z(G/N)$. Тогда $H \triangleleft G$ и по лемме 1.56, с. 41, подгруппа H абелева. Получили противоречие условию N — максимальная абелева нормальная подгруппа.

ЛЕММА 2.69. *Пусть $Z \leq Z(G)$. Тогда и только тогда группа G нильпотентна, когда факторгруппа G/Z нильпотентна.*

Если группа нильпотентна, то по лемме 18.2 факторгруппа G/Z нильпотентна. Обратно, пусть факторгруппа G/Z нильпотентна и P — силовская подгруппа группы G . Тогда PZ/Z — силовская подгруппа группы G/Z по лемме 1.65, с. 47, поэтому $PZ/Z \triangleleft G/Z$ и $PZ \triangleleft G$. По лемме Фраттини $G = N_G(P)Z$, а так как $Z \leq Z(G)$, то $P \triangleleft G$ и группа G нильпотентна.

Пусть G — неединичная группа. Введем следующие обозначения:

$$\begin{aligned} Z_0(G) &= E, \\ Z_1(G) &= Z(G), \\ Z_2(G)/Z_1(G) &= Z(G/Z_1(G)), \dots, \\ Z_i(G)/Z_{i-1}(G) &= Z(G/Z_{i-1}(G)), \dots \end{aligned}$$

Ясно, что

$$E = Z_0(G) \leq Z_1(G) \leq \dots \leq Z_{i-1}(G) \leq Z_i(G) \leq \dots$$

ТЕОРЕМА 2.70. *Тогда и только тогда неединичная группа G нильпотентна, когда существует натуральное число s такое, что $Z_s(G) = G$.*

У неединичной нильпотентной группы G центр $Z(G) = Z_1(G)$ отличен от единицы. Поэтому $E = Z_0(G) < Z_1(G)$. Группа $G/Z_1(G)$ нильпотентна по лемме 18.2. Если $G/Z_1(G) = E$, то $s = 1$. Если $G/Z_1(G) \neq E$, то

$$Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \neq E$$

и $E = Z_0(G) < Z_1(G) < Z_2(G)$. Таким образом, получаем цепочку подгрупп

$$E = Z_0(G) < Z_1(G) < \dots < Z_{i-1}(G) < Z_i(G) < \dots$$

Поэтому существует натуральное c , для которого $Z_c(G) = G$.

Обратно, пусть G — неединичная группа и $Z_c(G) = G$ для некоторого натурального c . Воспользуемся индукцией по c . Если $c = 1$, то

$$Z(G) = Z_1(G) = G$$

и группа G абелева. Пусть

$$Z(G) = Z_1(G) \neq G.$$

Для факторгруппы $G/Z_1(G)$ получаем, что

$$Z_{c-1}(G/Z_1(G)) = G/Z_1(G),$$

поэтому группа $G/Z_1(G)$ нильпотентна по индукции. Теперь группа G нильпотентна по лемме 18.8.

Итак, каждая неединичная нильпотентная группа обладает *возрастающим центральным рядом*

$$\begin{aligned} E = Z_0(G) < Z_1(G) < \dots < Z_{i-1}(G) < Z_i(G) < \dots \\ < Z_{c-1}(G) < Z_c(G) = G, \end{aligned}$$

где

$$Z_0(G) = E, \quad Z_1(G) = Z(G), \dots,$$

$$Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)), \quad i = 1, \dots, c.$$

Число c называется *степенью нильпотентности* группы G и обозначается через $c(G)$. Для единичной группы полагают $c(E) = 0$.

Очевидно, что $c(G) = 1$, когда группа $G \neq E$ и G абелева, а $c(G) = 2$, когда группа G неабелева, но факторгруппа $G/Z(G)$ абелева.

2.12. Подгруппа Фраттини

В единичной группе E нет собственных подгрупп. В неединичной группе всегда существует собственная подгруппа, например подгруппа E . Собственная подгруппа M неединичной группы G называется *максимальной* подгруппой, если M не содержится ни в какой другой подгруппе, отличной от всей группы G , т.е. если из условия $M \leq H \leq G$ следует, что $M = H$ или $H = G$. Для максимальной подгруппы M неединичной группы G используется запись $M < \cdot G$.

ЛЕММА 2.71. Пусть $M < \cdot G$ и $K \triangleleft G$. Тогда:

- (1) если $\alpha \in \text{Aut} G$, то $\alpha(M) < \cdot G$;
- (2) если $K \leq M$, то $M/K < \cdot G/K$;
- (3) если K не содержится в M , то $MK = G$;
- (4) если $\bar{U}$ — максимальная подгруппа факторгруппы $\bar{G} = G/K$, то существует $U < \cdot G$ такая, что $K \leq U$ и $\bar{U} = U/K$;
- (5) если $M \triangleleft G$, то индекс подгруппы M в группе G является простым числом.

Все утверждения проверяются непосредственно с привлечением теоремы о соответствии.

Подгруппой Фраттини неединичной группы называется пересечение всех её максимальных подгрупп. Подгруппа Фраттини неединичной группы G обозначается через $\Phi(G)$. Таким образом,

$$\Phi(G) = \bigcap_{M < G} M.$$

Для единичной группы E полагают $\Phi(E) = E$.

Если $H \leq G$, то пересечение всех подгрупп, сопряженных с H , называется *ядром подгруппы H* в группе G и обозначается через $\text{Core}_G(H)$.

ЛЕММА 2.72. Пусть $H \leq G$. Тогда справедливы следующие утверждения:

- (1) $\text{Core}_G(H)$ — наибольшая нормальная подгруппа группы G , содержащаяся в подгруппе H ;
- (2) $\Phi(G) = \bigcap_{M < G} \text{Core}_G(M)$;
- (3) $\Phi(G) \text{ char } G$, в частности, $\Phi(G) \triangleleft G$.

(1) По определению

$$\text{Core}_G(H) = \bigcap_{x \in G} H^x.$$

Поэтому $\text{Core}_G(H) \triangleleft G$. Если $K \triangleleft G$ и $K \leq H$, то $K^x = K \leq H^x$ для любого $x \in G$ и $K \leq \text{Core}_G(H)$. Поэтому, $\text{Core}_G(H)$ — наибольшая нормальная подгруппа группы G , содержащаяся в H .

(2) Так как подгруппа, сопряжённая максимальной подгруппе, будет также максимальной подгруппой, то

$$\begin{aligned} \Phi(G) &= \bigcap_{M < G} M = \bigcap_{M < G} (\bigcap_{x \in G} M^x) = \\ &= \bigcap_{M < G} \text{Core}_G(M). \end{aligned}$$

(3) Из леммы 19.1(1) следует, что $\Phi(G) \text{ char } G$, поэтому $\Phi(G) \triangleleft G$.

ТЕОРЕМА 2.73. Подгруппа Фраттини является нормальной нильпотентной подгруппой.

Из леммы 19.2(3) следует, что $\Phi(G) \triangleleft G$. Пусть P — силовская подгруппа в $\Phi(G)$. Предположим, что P ненормальна в G . Тогда $N_G(P)$ — собственная в G подгруппа и можно выбрать максимальную подгруппу M группы G , содержащую $N_G(P)$. Теперь $P \leq N_G(P) \leq M$, а по лемме Фраттини

$$G = \Phi(G)N_G(P) \leq M.$$

Противоречие. Значит допущение неверно и $P \triangleleft G$. Итак, все силовские подгруппы из $\Phi(G)$ нормальны в G . Поэтому $\Phi(G)$ нильпотентна.

Элемент $x \in G$ называется *необразующим элементом группы G* , если для любого подмножества T группы G из условия $\langle T, x \rangle = G$ следует, что $\langle T \rangle = G$.

ТЕОРЕМА 2.74. Подгруппа Фраттини группы G состоит из всех необразующих элементов группы G . В частности, если факторгруппа $G/\Phi(G)$ циклическая, то группа G циклическая.

Обозначим через X — множество всех необразующих элементов группы G . Пусть $x \in X$ и предположим, что x не содержится в $\Phi(G)$. Тогда существует максимальная подгруппа M группы G , не содержащая элемент x . Теперь $M \neq G$, а $\langle M, x \rangle = G$, что противоречит тому, что x — необразующий элемент. Поэтому, допущение неверно, и $X \subset \Phi(G)$.

Пусть теперь $y \in \Phi(G)$ и допустим, что существует такое подмножество $T \subset G$, что $\langle T \rangle \neq G$, а $\langle T, y \rangle = G$. Пусть H — максимальная подгруппа группы G , содержащая подгруппу $\langle T \rangle$. Так как $y \in \Phi(G) \leq H$,

то $G = \langle T, y \rangle \leq H$, противоречие. Поэтому допущение неверно и y — необразующий элемент группы G .

Пусть факторгруппа $G/\Phi(G)$ циклическая. Тогда $G/\Phi(G) = \langle g\Phi(G) \rangle$ для некоторого элемента $g \in G$. Поскольку $G = \langle g, \Phi(G) \rangle$, то $G = \langle g \rangle$ и группа G циклическая.

СЛЕДСТВИЕ. Если $H \leq G$ и $H\Phi(G) = G$, то $H = G$. □

СЛЕДСТВИЕ. Пусть $K \triangleleft G$. Тогда и только тогда в группе G существует собственная подгруппа H такая, что $G = KH$, когда подгруппа K не содержится в подгруппе Фраттини $\Phi(G)$.

Если в группе G существует собственная подгруппа H такая, что $G = KH$ и $K \subseteq \Phi(G)$, то по теореме 19.4

$$G = \langle K, H \rangle = \langle H \rangle = H,$$

противоречие. Обратно, если $K \not\subseteq \Phi(G)$, то существует максимальная подгруппа M , не содержащая K . Поэтому $KM = G$.

Пусть K — подгруппа группы G . Подгруппа H называется *добавлением* к подгруппе K , если $KH = G$ и $KH_1 \neq G$ для любой подгруппы H_1 из H , отличной от H . Понятно, что любая нормальная подгруппа обладает по крайней мере одним добавлением.

ЛЕММА 2.75. Тогда и только тогда подгруппа H является добавлением к нормальной подгруппе K в группе G , когда $HK = G$ и $H \cap K \subseteq \Phi(H)$.

Пусть H — добавление к подгруппе K . Допустим, что $H \cap K$ не содержится в подгруппе Фраттини $\Phi(H)$. Тогда существует максимальная подгруппа H_1 группы H такая, что $H \cap K$ не содержится в H_1 . Так как $H \cap K \triangleleft H$, то

$$H_1(H \cap K) = H; \quad G = HK = H_1(H \cap K)K = H_1K,$$

противоречие с определением добавления. Поэтому допущение неверно и $H \cap K \leq \Phi(H)$.

Обратно, пусть

$$HK = G; \quad H \cap K \leq \Phi(H).$$

Предположим, что H не является добавлением к подгруппе K . Тогда существует максимальная подгруппа H_1 в группе H такая, что $H_1K = G$. По тождеству Дедекинда

$$H = H_1(H \cap K) \leq H_1\Phi(H) = H_1,$$

противоречие. Поэтому допущение неверно и подгруппа H является добавлением к подгруппе K .

ТЕОРЕМА 2.76. Пусть $K \triangleleft G$. Тогда:

- (1) $\Phi(K) \leq \Phi(G)$;
- (2) $\Phi(G)K/K \leq \Phi(G/K)$;
- (3) если $K \leq \Phi(G)$, то $\Phi(G)/K = \Phi(G/K)$;
- (4) если $A \leq G$ и $K \leq \Phi(A)$, то $K \leq \Phi(G)$.

(1) Так как $\Phi(K) \text{ char } K$, то $\Phi(K) \triangleleft G$. Предположим, что $\Phi(K) \not\subseteq \Phi(G)$. Тогда существует максимальная подгруппа M такая, что $\Phi(K)M = G$. По тождеству Дедекинда

$$K = \Phi(K)(K \cap M),$$

а по следствию 19.5 $K = K \cap M$, т.е. $K \leq M$. Теперь $\Phi(K) \leq M$, противоречие. Поэтому допущение неверно и $\Phi(K) \leq \Phi(G)$.

(2) Утверждение вытекает из леммы 19.1(4).

(3) Пусть $K \leq \Phi(G)$. Тогда K содержится в каждой максимальной подгруппе группы G и из леммы 19.1(4) вытекает это утверждение.

(4) Пусть $A \leq G$ и $K \leq \Phi(A)$. Предположим, что K не содержится в $\Phi(G)$. Тогда существует максимальная подгруппа M группы G , не содержащая K . По тождеству Дедекинда

$$A = A \cap G = A \cap MK = (A \cap M)K.$$

Так как $K \leq \Phi(A)$, то по следствию 19.5 $A = A \cap M$, т.е. $A \leq M$. Теперь $K \leq M$, что противоречит предположению. Поэтому предположение неверно и $K \leq \Phi(G)$.

ТЕОРЕМА 2.77. $\Phi(G_1 \times G_2) = \Phi(G_1) \times \Phi(G_2)$.

Пусть $G = G_1 \times G_2$. Так как $G_1 \triangleleft G$ и $G_2 \triangleleft G$, то по теореме 19.8(1)

$$\Phi(G_1) \times \Phi(G_2) \subseteq \Phi(G).$$

Пусть

$$G/(\Phi(G_1) \times \Phi(G_2)) = G^*.$$

По теореме 19.8(3)

$$\Phi(G)/(\Phi(G_1) \times \Phi(G_2)) = \Phi(G^*).$$

Ясно, что $G^* = G_1^* \times G_2^*$, где

$$G_1^* \simeq G_1/\Phi(G_1); \quad G_2^* \simeq G_2/\Phi(G_2).$$

Опять по теореме 19.8(3) $\Phi(G_1^*) = \Phi(G_2^*) = E$. Так как пересечение максимальных подгрупп группы G^* , содержащих подгруппу G_1^* (или подгруппу G_2^*) равно 1 и $G_1^* \cap G_2^* = E$, то $\Phi(G^*) = E$. Поэтому

$$\Phi(G) = \Phi(G_1) \times \Phi(G_2).$$

ТЕОРЕМА 2.78. Пусть $D \triangleleft K \triangleleft G$, $D \leq \Phi(G)$ и $D \triangleleft G$. Если K/D нильпотентна, то K нильпотентна.

Пусть P — силовская p -подгруппа группы K . По теореме 1.65, с. 47, PD/D — силовская p -подгруппа факторгруппы K/D , а т.к. K/D нильпотентна, то $PD/D \triangleleft K/D$. Поскольку $PD/D \text{ char } K/D$, то

$$PD/D \triangleleft G/D; \quad PD \triangleleft G.$$

По лемме Фраттини $G = N_G(P)D$, а из следствия 19.5 вытекает, что $G = N_G(P)$ и $P \triangleleft G$. Теперь $P \triangleleft K$ и K нильпотентна.

СЛЕДСТВИЕ. Если $G/\Phi(G)$ нильпотентна, то G нильпотентна.

Утверждение вытекает из теоремы 19.10 при $D = \Phi(G)$ и $K = G$.

Теперь рассмотрим подгруппу Фраттини примарной группы.

ЛЕММА 2.79. Пусть G — p -группа. Тогда:

- (1) факторгруппа $G/\Phi(G)$ — элементарная абелева p -группа;
- (2) если $K \triangleleft G$ и G/K — элементарная абелева группа, то $\Phi(G) \subseteq K$;
- (3) $\Phi(G)$ является наименьшей нормальной подгруппой группы G , факторгруппа по которой элементарная абелева p -группа;
- (4) если $|G/\Phi(G)| = p^n$, то существуют элементы $x_1, \dots, x_n \in G$ такие, что $G = \langle x_1, \dots, x_n \rangle$.

(1) В p -группах максимальные подгруппы нормальны и имеют индекс p , см. следствие 10, с. 93. Пусть $\{M_i \mid i = 1, \dots, m\}$ — множество всех максимальных подгрупп группы G . Так как факторгруппа

$$G/\Phi(G) = G/\cap_{i=1}^m M_i$$

по лемме 2.33, с. 70, изоморфна подгруппе прямого произведения $\prod_{i=1}^m G/M_i$ групп G/M_i порядка p , то $G/\Phi(G)$ элементарная абелева.

(2) Пусть

$$\{H_i/K \mid i = 1, \dots, k\}$$

— множество всех максимальных подгрупп факторгруппы G/K . По условию факторгруппа G/K элементарная абелева, поэтому

$$\cap_{i=1}^k (H_i/K) = E; \quad K = \cap_{i=1}^k H_i.$$

Теперь

$$\Phi(G) = \cap_{X < G} X \subseteq \cap_{i=1}^k H_i = K.$$

(3) Утверждение вытекает из (1) и (2).

(4) Так как $G/\Phi(G)$ — элементарная абелева p -группа порядка p^n , то

$$G/\Phi(G) = \langle x_1\Phi(G) \rangle \times \dots \times \langle x_n\Phi(G) \rangle$$

для некоторых $x_1, \dots, x_n \in G$. Теперь $G = \langle x_1, \dots, x_n, \Phi(G) \rangle$ и $G = \langle x_1, \dots, x_n \rangle$ по теореме 19.4.

Литература

1. Белоногов В.А. Задачник по теории групп. — М.: Наука, 2000. 239 с.
2. Богопольский О.В. Введение в теорию групп. — Москва–Ижевск: Институт компьютерных исследований, 2002. 148 с.
3. Ведерников В.А. Элементы теории классов групп. Учебное пособие по спецкурсу. — Смоленск: Смоленский гос. пед. ин-т, 1988. 95 с.
4. Горенштейн Д., Конечные простые группы: Введение в их классификацию. — М.: Мир, 1985. 352 с.
5. Каморников С.Ф., Селькин М.В. Подгрупповые функторы и классы конечных групп. — Минск: Беларуская навука, 2003. 254 с.
6. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. — М.: Наука, 1982. 288 с.
7. Кондратьев А.С., Махнев А.А., Старостин А.И. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. Т.24. (Итоги науки и техники. ВИНТИ АН СССР). М., 1986. С.3–120.
8. Кострикин А.И. Конечные группы. — В сб.: Алгебра. Топология. Геометрия, 1964. (Итоги науки. Серия: Математика. ВИНТИ АН СССР). М., 1966. С.7–46.
9. Мазуров В.Д. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. Т.14. (Итоги науки и техники. ВИНТИ АН СССР). М., 1976. С.5–56.
10. Монахов В.С. Введение в теорию групп. Тексты лекций по курсу "Алгебра и теория чисел". — Минск: Белорусский гос. ун-т, 1990. 72 с.
11. Нерешенные вопросы теории групп. Коуровская тетрадь. — Новосибирск: Новосиб. гос. ун-т, 2002. 172 с.
12. Селькин М.В. Максимальные подгруппы в теории классов конечных групп. — Мн.: Беларуская навука, 1997. 144 с.
13. Скиба А.Н. Алгебра формаций. — Мн.: Беларуская навука, 1997. 240 с.
14. Скиба А.Н. Решетки и универсальные алгебры. Учебное пособие. — Гомель: Гомельский гос. ун-т, 2002. 255 с.
15. Холл Ф. Теория групп. — М.: ИЛ, 1962. 468 с.
16. Чунихин С. А. Подгруппы конечных групп.— Минск: Наука и техника, 1964. 158 с.
17. Чунихин С.А. Краткий курс теории групп. — 1969. 276 с.

18. Чунихин С.А., Шеметков Л.А. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. (Итоги науки и техники. ВИНТИ АН СССР). М., 1971. С.7–70.
19. Шеметков Л.А. Формации конечных групп. — М.: Наука, 1978. 272 с.
20. Шеметков Л.А. Классические факторизации групп и колец. Учебное пособие. — Гомель: Гомельский гос. ун-т, 1979. 64 с.
21. Шеметков Л.А. Основы теории групп. Спецкурс для студентов математического факультета Гомельского госуниверситета. — 1979. 134 с.
22. Шеметков Л.А., Скиба А.Н. Формации алгебраических систем. — М.: Наука, 1989. 253 с.
23. Doerk K., Hawkes T. Finite soluble groups. — Walter de Gruyter. Berlin, New York, 1992. 889 p.
24. Gaschütz W. Lectures of subgroups of Sylow type in finite soluble groups. Notes on pure mathematics; № 11. — Canberra, Australian National University, 1979. 100 p.
25. Guo W. The Theory of Classes of Groups. — Science Press-Kluwer Academic Publishers, Beijing-New York-Dordrecht-Boston-London, 2000. 258 p.
26. Huppert B. Endliche Gruppen I. — Berlin, Heidelberg, New York, 1967. 793 s.
27. Huppert B., Blackburn N. Finite groups, II. — Berlin–Heidelberg–New York: Springer, 1982. 531 p.
28. Huppert B., Blackburn N. Finite groups, III. — Berlin–Heidelberg–New York: Springer, 1982. 454 p.
29. Kurzweil H., Stellmacher B., Theorie der endlichen Gruppen. Eine Einführung. — Springer-Verlag, Berlin–Heidelberg–New York, 1998. 341 s.
30. Robinson D.J.S. A course in the theory of groups. — Springer-Verlag, Berlin–Heidelberg–New York, 1982. 481 p.
31. Wehrfritz B.A.F. Finite groups. A second course on group theory. — World scientific: Singapore–New Yersey–London–Hong Kong, 1999. 123 p.

Предметный указатель

- p -группа, 45
 - абелева
 - элементарная, 74
- автоморфизм, 29, 54
 - центральный, 57
 - внутренний, 55
- центр, 20
- централизатор, 19
- цокль группы, 73
- добавление, 99
- элемент
 - единичный, 8
 - необразующий, 98
 - обратный, 8
 - сопряженный, 11
- эндоморфизм, 58
 - нулевой, 58
 - тождественный или единичный, 58
- эпиморфизм, 52
- фактор
 - главный, 62
 - композиционный, 63
 - ряда, 62
- факторгруппа, 41
- гомоморфизм, 51
- группа, 9
 - абелева, 9
 - циклическая, 22
 - бесконечная, 23
 - конечная, 23
 - диэдральная, 80
 - конечная, 9
 - кватернионов, 82
 - линейная
 - общая, 14
 - полная, 14
 - специальная, 14
 - нильпотентная, 93
 - примарная, 45, 92
 - проективная, 85
 - простая, 40
 - симметрическая, 15
 - знакопеременная, 15
- индекс
 - подгруппы, 31
- инволюция, 80
- изоморфизм, 26
 - рядов, 63
- класс
 - смежный
 - двойной, 33
 - левый, 30
 - правый, 30
 - сопряженных элементов, 11
- матрица
 - перестановки, 27
 - верхняя унитарная, 82
- гомоморфизм, 52
- нормализатор, 36
- образ
 - гомоморфизма, 51
- операция
 - ассоциативная, 8
 - бинарная, 8
 - коммутативная, 8
- оператор, 60
- перестановка, 14
- подгруппа, 17
 - Фраттини, 98
 - циклическая, 21
 - допустимая, 60
 - единичная, 17
 - характеристическая, 56
 - характеристически простая, 56
 - холлова, 57
 - максимальная, 97
 - максимальная нормальная, 43
 - нетривиальная, 17
 - нормальная, 38
 - минимальная, 73
 - порожденная множеством, 18
 - силовская, 47
 - собственная, 17
 - сопряженная, 18
 - субнормальная, 75
 - тривиальная, 17
- подмножество
 - сопряженное, 18
- полугруппа, 8
- порядок
 - элемента, 22
 - группы, 9
- преобразование
 - аффинное прямой, 15
- произведение
 - центрального, 81
 - подгрупп, 34
 - подпрямое, 70
 - полупрямое, 80
 - внешнее, 79
 - прямое, 65
 - внешнее, 69
- решетка
 - подгрупп, 19
- ряд, 62
 - центральный, 97
 - нормальный, 62
 - субнормальный, 62
- ступень
 - нильпотентности, 97

трансверсаль
 левая, 31
 правая, 31
ядро
 гомоморфизма, 51
 подгруппы, 98

Содержание

Содержание

Условные обозначения	5
Глава 1. Группы и их подгруппы	8
1 Группы, примеры групп	8
Алгебраическая операция	8
Группа и ее начальные свойства	9
Классы сопряженных элементов	11
Примеры	14
2 Подгруппы	17
Подгруппа группы	17
Подгруппа, порожденная множеством	18
Решетка подгрупп	19
Централизатор	19
Центр группы	20
Примеры	21
3 Циклические группы	21
Порядок элемента	22
Подгруппы циклических групп	23
Критерий подгруппы конечной группы	24
Примеры	24
4 Изоморфизм групп	26
Изоморфизм циклических групп	26
Матрица перестановки	27
Вложение конечных групп в симметрическую группу и в полную линейную группу	28
Аutomорфизмы групп	29
Примеры	29
5 Смежные классы	30
Трансверсаль	31
Двойные смежные классы	33
Произведение подгрупп	33
Нормализатор	36
Примеры	38
6 Нормальные подгруппы и факторгруппы	38
Простая группа	40
Факторгруппа	40
Факторгруппы циклических групп	41
Теорема о соответствии	42
Решетка нормальных подгрупп	42
Максимальная нормальная подгруппа	43
Подгруппа наименьшего простого индекса	43
Примеры	43
7 Силовские подгруппы конечных групп	44
Силовские подгруппы	47
Лемма Фраттини	49
Примеры	50
Глава 2. Гомоморфизмы и произведения групп	51

1	Гомоморфизмы групп	51
	Мономорфизм, эпиморфизм	52
	Основная теорема о гомоморфизме	52
	Теоремы о изоморфизме	52
	Примеры	53
2	Автоморфизмы	54
	Примеры автоморфизмов	54
	Внутренние автоморфизмы	55
	Характеристические подгруппы	56
	Центральные автоморфизмы	57
3	Эндоморфизмы и операторы	58
	Эндоморфизмы и автоморфизмы циклических групп	59
	Операторы	60
4	Композиционные ряды	62
	Субнормальные и нормальные ряды	62
	Ω -композиционный ряд	63
	Теорема Жордана–Гельдера	63
5	Прямые произведения	65
	Прямое произведение двух групп	65
	Прямое произведение нескольких групп	66
	Внешнее прямое произведение	69
	Подпрямое произведение	70
	Разложение циклической группы в прямое произведение подгрупп	71
6	Минимальные нормальные подгруппы	73
	Цоколь группы	73
	Субнормальные подгруппы	75
	Решетка субнормальных подгрупп	76
	Свойства простых неабелевых субнормальных подгрупп	77
7	Полупрямые произведения	78
	Внешнее полупрямое произведение	78
	Полупрямое произведение	80
	Диэдральная группа	80
	Центральное произведение	81
8	Линейные группы	82
	Порядки линейных групп	82
	Разложение линейных групп	85
	Подгруппы $PSL(2, p^m)$	86
	Глава 3. Абелевы и нильпотентные группы	88
9	Строение конечных абелевых групп	88
	Циклическая подгруппа наибольшего порядка примарной абелевой группы	88
	Инварианты абелевой p -группы	91
	Примеры	91
10	Примарные группы	92
	Центр примарной группы	92
	Нормализаторы подгрупп	92
	Нормальные подгруппы примарной группы	93
11	Нильпотентные группы	93
	Свойства нильпотентной группы	93
	Условия, эквивалентные определению нильпотентной группы	96
	Центральный ряд	96

Содержание

12 Подгруппа Фраттини	97
Свойства подгруппы Фраттини	98
Необразующие элементы	98
Подгруппа Фраттини прямого произведения	100
Подгруппа Фраттини примарных групп	100
Литература	102
Предметный указатель	104

Учебное издание

МОНАХОВ ВИКТОР СТЕПАНОВИЧ

Введение в теорию конечных групп и их классов. Учебное пособие

Подписано в печать 24.04.2003. Формат $60 \times 84 \frac{1}{16}$. Бумага офсетная. Печать офсетная. Усл. п. л. 18,6 Уч.-изд. л. 20. Тираж 250 экз. Заказ № 234.

Отпечатано на полиграфической технике УО “ТГУ им. Ф.Скорины”
Лицензия ЛВ № 357 от 12 февраля 1999.
246019 г.Гомель, ул.Советская 104