Монахов Виктор Степанович, доктор физико-математических наук, профессор кафедры алгебры и геометрии Гомельского государственного университета имени Франциска Скорины. Научные работы по теории конечных групп и теории графов. Восполнил пробел в классической теореме Бернсайда 1905 г. о нормальных подгруппах бипримарных групп; разработал методику исследования строения конечных факторизуемых групп; получил новую информацию о существовании подгрупп Шмидта в конечных группах; исследовал зависимость инвариантов конечных разрешимых групп от индексов максимальных подгрупп. Автор ряда методических пособий по вопросам преподавания математики в вузах.

УДК 512.542
ББК
М 77
Р е ц е н з е н т ы: кафедра высшей алгебры Белорусского государственного университета; доктор физико-математических наук, профессор *Э.М.Пальчик*

Монахов В.С.

М77 Введение в теорию конечных групп и их классов: учебное пособие / В.С.Монахов – Мн.: Выш. шк., 2005. – 202 с.
ISBN 985-06-1114-6

Рассмотрены основы теории групп и основы теории классов конечных групп: формаций, классов Шунка, классов Фиттинга.

Изложение материала проводится на высоком научно-методическом уровне, в то же время пособие вполне доступно для самостоятельного изучения. Вводимые понятия иллюстрируются разнообразными примерами.

Для студентов, аспирантов и преподавателей физико-математических специальностей вузов.

УДК 512.542

ISBN 985-06-1114-6

Предисловие

Теория групп — один из центральных разделов современной алгебры, активно разрабатываемый в Беларуси в настоящее время в научных школах Минска, Гомеля, Витебска, Новополоцка, Могилева и Мозыря. Однако учебных изданий в Республике Беларусь, посвященных основам теории конечных групп, до сих пор не было.

Данная книга — расширенная запись лекций по теории конечных групп, читаемых автором на математическом факультете Гомельского государственного университета им. Ф. Скорины начиная с 1986/87 учебного года в рамках специализации "Алгебра и теория чисел". Для понимания достаточно знать начальные разделы вузовской алгебры: матрицы, отображения, перестановки, поля, векторные пространства.

Книга состоит из пяти глав. Материалы первых трех глав полностью охватывают ту часть типовой программы университетского курса "Алгебра и теория чисел которая касается теории групп. В связи с этим данное учебное пособие может быть рекомендовано студентам-математикам при изучении курса "Алгебра и теория чисел". Четвертая и пятая главы могут оказаться полезными аспирантам специальности 01.01.06 — математическая логика, алгебра и теория чисел при подготовке к сдаче кандидатского экзамена.

При подборе материала автор использовал методики построения текстов лекций по теории групп С.А.Чунихина и Л.А.Шеметкова, а также отдельные фрагменты книг Гашюца [6] и Хупперта [7].

Более углубленно изучить различные разделы теорию конечных групп и их классов читатель может по монографиям и обзорным статьям, указанным в списках литературы.

Автор выражает искреннюю благодарность члену–корреспонденту НАН Беларуси профессору Л.А.Шеметкову и профессору В.А.Ведерникову за многочисленные полезные советы, способствующие улуч-

шению качества излагаемого материала. Автор также благодарен рецензентам — коллективу кафедры высшей алгебры Белорусского государственного университета, возглавляемому профессором О.И.Тавгенем, профессору этой кафедры О.В.Мельникову, заведующему кафедрой прикладной математики Полоцкого государственного университета профессору Э.М.Пальчику — за конструктивные замечания, и кандидату физико-математических наук И.В.Близнецу — за помощь в подготовке рукописи книги к изданию.

Автор

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
$\mathbb{Z}_p$ — поле классов вычетов по простому модулю p
$\{\alpha \mid \beta\}$ — множество всех α для которых выполняется β
π — некоторое множество простых чисел
π' — дополнение к π во множестве всех простых чисел
G — группа
$|G|$ — порядок группы G
e — единичный элемент группы G
E — единичная подгруппа и единичная группа
$\pi(G)$ — множество всех простых делителей порядка группы G
$Z(G)$ — центр группы G
$\Phi(G)$ — подгруппа Фраттини группы G
$F(G)$ — подгруппа Фиттинга группы G
G' — коммутант группы G
$C_G(H)$ — централизатор подгруппы H в группе G
$N_G(H)$ — нормализатор подгруппы H в группе G
$Aut\ G$ — группа всех автоморфизмов группы G
$Inn\ G$ — группа всех внутренних автоморфизмов группы G
$H \leq G$ — H — подгруппа группы G
$H < G$ — H — собственная подгруппа группы G
$M < \cdot\ G$ — M — максимальная подгруппа группы G
$H \triangleleft G$ — H — нормальная подгруппа группы G
$H \triangleleft\triangleleft G$ — H — субнормальная подгруппа группы G
$H \cdot\!\triangleleft\ G$ — H — минимальная нормальная подгруппа группы G
$|G : H|$ — индекс подгруппы H в группе G
$\pi(G : H) = \pi(|G : H|)$
$A \times B$ — прямое произведение подгрупп A и B
$[A]B$ — полупрямое произведение нормальной подгруппы A и подгруппы B
$\langle \ldots \rangle$ — подгруппа, порождённая некоторым множеством элементов или подгрупп
$[x, y] = x^{-1}y^{-1}xy$ — коммутатор элементов $x, y \in G$

$A^x = x^{-1}Ax$ — множество, сопряженное с множеством A посредством элемента x

$A \simeq B$ — группы A и B изоморфны

E_{p^n} — элементарная абелева группа порядка p^n

D_n — диэдральная группа порядка n

Q_8 — группа кватернионов порядка 8

Z_n — циклическая группа порядка n

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

$\mathfrak{G}$ — класс всех конечных групп

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

$\mathfrak{N}$ — класс всех нильпотентных групп

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

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

$\square$ — начало доказательства теоремы, леммы, следствия, а также решения примера

$\boxtimes$ — окончание доказательства теоремы, леммы, следствия, а также решения примера

1. ГРУППЫ И ИХ ПОДГРУППЫ

1.1. Группы. Примеры групп

Бинарной алгебраической операцией на множестве X называют отображение декартова квадрата $X \times X$ в X. Если $\varphi : \ X \times X \to X$ — 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 следующих символов: $+, \cdot, \oplus, \circ, \otimes, *$ и т.д. Если вместо φ условимся писать $\circ$, то вместо $c = \varphi(a, b)$ следует писать $c = a \circ b$.

Наиболее часто используются две формы записи операции: аддитивная и мультипликативная. При *аддитивной форме записи* операцию называют *сложением* и вместо $c = a \circ b$ пишут $c = a + b$. При *мультипликативной форме записи* операцию называют *умножением* и вместо $c = a \circ b$ пишут $c = a \cdot b$ или $c = ab$. В дальнейшем, при изложении теории, будем использовать мультипликативную форму записи.

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), которая удовлетворяет следующим двум требованиям: операция определена на P, т.е. $ab \in P$ для всех $a, b \in P$; 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. Тогда $e_1e_2 = e_1$, поскольку e_2 — единичный элемент, и $e_1e_2 = e_2$, так как 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 их произведение. Для $n \leq 4$ составим следующие произведения:

a_1 при $n = 1$;

a_1a_2 при $n = 2$;

$(a_1a_2)a_3, a_1(a_2a_3)$ при $n = 3$;

$((a_1a_2)a_3)a_4, (a_1(a_2a_3))a_4, a_1((a_2a_3)a_4), a_1(a_2(a_3a_4))$,

$(a_1a_2)(a_3a_4)$ при $n = 4$.

Поскольку операция ассоциативна, то $(a_1a_2)a_3 = a_1(a_2a_3)$. Для $n = 4$, используя свойство ассоциативности, легко проверить, что все пять произведений совпадают.

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

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

при любых k и l, $1 \leq k$, $l \leq n-1$. По предположению индукции произведения внутри скобок вычисляются однозначно. Пусть $k > l$. Тогда $(a_1 \dots a_k)(a_{k+1} \dots a_n) = ((a_1 \dots a_l)(a_{l+1} \dots a_k))(a_{k+1} \dots a_n) = (a_1 \dots a_l) \times ((a_{l+1} \dots a_k)(a_{k+1} \dots a_n)) = (a_1 \dots a_l)(a_{l+1} \dots a_n)$. ☒

Теорема 1.2 позволяет использовать в полугруппах знак кратного умножения:

$$a_1a_2 = \prod_{i=1}^{2} a_i, \quad a_1a_2a_3 = \prod_{i=1}^{3} a_i, \quad \dots, \quad a_1a_2...a_n = \prod_{i=1}^{n} a_i.$$

В частности, при $a_1 = a_2 = \dots = a_n = a$ произведение $aa \dots a$ обозначают через a^n и называют n-*й степе-*

нью элемента a. Следствием теоремы 1.2 являются равенства:

$$a^n a^m = a^{n+m}, \quad (a^n)^m = a^{nm}, \tag{1.1}$$

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 $(ab)^n = a^n b^n$ для всех натуральных n, что легко проверяется индукцией по n.

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

1) операция определена на G, т.е. $ab \in G$ для всех $a, b \in G$;

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.*

Лемма 1.4. *Если a, b — элементы группы G, то $(a^{-1})^{-1} = a$ и $(ab)^{-1} = b^{-1}a^{-1}$.*

□ Первое равенство очевидно. Так как $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$, $(b^{-1}a^{-1})(ab) =$

$b^{-1}(a^{-1}a)b = b^{-1}eb = e$, то справедливо и второе равенство. ⊠

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

$$a^{-n} = (a^n)^{-1} \tag{1.2}$$

для всех $n \in \mathbb{N}$.

Лемма 1.5. *Если a — элемент группы G и $s \in \mathbb{Z}$, то $(a^s)^{-1} = (a^{-1})^s = a^{-s}$.*

□ 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 формуле (1.2). Если $s = 0$, то $(a^s)^{-1} = e = (a^{-1})^s = a^{-s}$. Если $s < 0$, то

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

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

Лемма 1.6. *Для любых целых s, t и любого $a \in G$ справедливы равенства: $a^s a^t = a^{s+t}$, $(a^s)^t = a^{st}$.*

□ Для натуральных показателей данные равенства уже получены в формулах (1.1). Если один из показателей — нуль, то равенства также справедливы. Пусть s и t — отрицательные числа. Используя леммы 1.4, 1.5 и формулы (1.1) получаем:

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

$(a^s)^t = (a^{-|s|})^t = ((a^{|s|})^{-1})^t = (a^{|s|})^{-t} = (a^{|s|})^{|t|} = a^{|s||t|} = a^{st}$. Если $s < 0$, $t > 0$, $t \geq |s|$, то

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

Если $s < 0$, $t > 0$, $|s| \geq t$, то

$$a^s a^t = a^{-|s|} a^t = \underbrace{a^{-1} \dots a^{-1}}_{|s|} \underbrace{a \dots a}_{t} = (a^{-1})^{|s|-t} = a^{t+s}.$$

Далее если $s < 0$, $t > 0$, $|s| \geq t$ или $t \geq |s|$, то $(a^s)^t =$

$$\underbrace{a^s \dots a^s}_{t} = \underbrace{\underbrace{(a^{-1} \dots a^{-1})}_{|s|} \dots \underbrace{(a^{-1} \dots a^{-1})}_{|s|}}_{t \text{ скобок}} = (a^{-1})^{|s|t} = a^{st}.$$

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 этого уравнения, 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 $a, b \in P$. 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 $x_ca = b$. Умножим справа обе части равенства на a^{-1}. 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 $g, f \in P$. 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 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 множество всех элементов группы G, сопряженных с элементом a. Это множество a^G называется *классом сопряженных с a элементов.* Ясно, что если G абелева, то $a^G = \{a\}$ для всех $a \in G$.

Лемма 1.9. *Пусть G — группа, элементы $a, b, x, y \in G$. Тогда*

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

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

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

4) $(a^x)^k = (a^k)^x$ для любого целого k;

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

6) группа G является объединением непересекающихся классов сопряженных элементов.

□ 1–4. Утверждения очевидны.

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

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

Если $c = a^z \in a^G$, то $c = b^{yx^{-1}z} \in b^G$ и $a^G \subseteq b^G$. Аналогично $b^G \subseteq a^G$, 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, согласно утверждению 5, группа G распадается на

непересекающиеся классы сопряженных элементов. $\boxtimes$

Все приведенные определения и полученные результаты легко переносятся (с соответствующим изменением терминологии как указано далее в таблице 1.1) на множества с аддитивной формой записи операции.

Приведем примеры числовых групп. 1. Множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ с операцией сложения — абелевы группы. Все требования определения группы проверяются без труда.

2. Множество $\mathbb{N}$ со сложением не является группой, так как в $\mathbb{N}$ нет нулевого и противоположных элементов. Однако, $\mathbb{N}$ со сложением — коммутативная полугруппа.

3. Множество $\{-1, 1\}$ с умножением — конечная абелева группа порядка 2.

4. 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. Множества $\mathbb{Z}^{\#} = \mathbb{Z} \setminus \{0\}$ и $\mathbb{N}$ с умножением — полугруппы, но не группы.

Приведем примеры матричных групп. 1. 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 имеют обратные, то $M(n, P)$ не является группой.

2. 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*.

3. Матрицы с единичными определителями образуют группу $SL(n, P) = \{A \in GL(n, P) \mid \det A = 1\}$, которая называется *специальной линейной группой степени n над P*.

Приведем примеры групп перестановок. 1. Пусть $X = \{1, 2, \ldots, n\}$. 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, указывая образы всех элементов:

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

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

Таблица 1.1.

Мультипликативная запись операции	*Аддитивная запись операции*
умножение	сложение
произведение ab, $\prod_{i=1}^{n} a_i = a_1 a_2 \ldots a_n$	сумма $a+b$, $\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n$
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 $n > 0$, $a^n = \underbrace{a \ldots a}_{n \text{ раз}}$	кратное na при $n > 0$, $na = \underbrace{a + \ldots + a}_{n \text{ раз}}$
степень a^n при $n < 0$, $a^n = \underbrace{a^{-1} \ldots a^{-1}}_{-n \text{ раз}}$	кратное na при $n < 0$, $na = \underbrace{(-a) + \ldots + (-a)}_{-n \text{ раз}}$
$a^n = e$ при $n = 0$	$na = 0$ при $n = 0$
$a^n a^m = a^{n+m}$, $n, m \in \mathbb{Z}$	$na + ma = (n+m)a$, $n, m \in \mathbb{Z}$
$(a^n)^m = a^{nm},\ n, m \in \mathbb{Z}$	$m(na) = (mn)a,\ n, m \in \mathbb{Z}$
$(ab)^n = a^n b^n,\ n \in \mathbb{Z}$, если $ab = ba$	$n(a+b) = na + nb,\ n \in \mathbb{Z}$, если $a + b = b + a$

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

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

Произведение $\delta\tau$ двух перестановок δ и τ находим как произведение отображений: $\delta\tau(k) = \delta(\tau(k)),\quad k = 1, 2, \ldots, n$. Легко проверить, что множество S_n всех перестановок степени n с операцией умножения 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.

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

Таблица умножения элементов группы S_3 приведена на обложке.

Приведем примеры групп функций. 1. Четыре функции

$$f_1(x) = x, \quad f_2(x) = -x, \quad f_3(x) = \frac{1}{x}, \quad f_4(x) = -\frac{1}{x}$$

с операцией умножения образуют группу. Составим таблицу умножения этих функций.

Таблица 1.2.

	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 $f_i f_j$ указывается на пересечении строки f_i и столбца f_j. Например,

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

поэтому $f_2 f_3 = f_4$.

Из табл. 1.2 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 обратным для себя. Таким образом, множество $\{f_1, f_2, f_3, f_4\}$ с умножением является конечной абелевой группой порядка 4.

2. *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 $A_1(\mathbb{R})$. Согласно операции умножения 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 $\varphi_{a,b}$.

Пример 1.1. Перечислить все классы сопряженных элементов симметрической группы

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

□ Вычислим $(12)^x$, где x "пробегает" элементы из S_3. Ясно, что $(12)^\varepsilon = (12)$ и $(12)^{(12)} = (12)$. Далее,

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

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

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

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

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

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

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

Таким образом, в S_3 имеется только три класса сопряженных элементов и $S_3 = \varepsilon^{S_3} \cup (12)^{S_3} \cup (123)^{S_3}$.

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. Можно записать перестановку 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:

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

Следовательно,

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

т.е. сопряженные перестановки имеют одинаковое число циклов каждой длины. Обратно, если перестановки

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

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

имеют одинаковое число циклов каждой длины, то

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

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

Рассмотрим симметрическую группу степени 4. Запись (...)(.) обозначает любую перестановку в S_4, распадающуюся на циклы длиной 3 и 1. В S_4 возможны следующие разложения: (.)(.)(.)(.), (.)(.)(..), (.)(...), (..)(..), (....). На основании теоремы 1.10, группа S_4 имеет пять классов сопряженных элементов.

1.2. Подгруппы

Подмножество H группы G называется *подгруппой*, если H — группа относительно той же операции, которая определена на G. Запись $H \leq G$ означает, что H — подгруппа группы G, а $H < G$, что $H \leq G$ — собственная подгруппа группы G, т.е. $H \leq G$ и $H \neq G$.

Теорема 1.11. *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 $h_1, h_2 \in H$.*

$\square$ Пусть H — подгруппа группы G, т. е. H — группа относительно той же операции, которая определена на 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 $e_1e = ee_1 = e_1$, поскольку e_1 — элемент из G. В G для e_1 имеется обратный элемент e_1^{-1}, т.е. $e_1^{-1}e_1 = e_1e_1^{-1} = e$. 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 $ee_1 = e$, откуда $e_1 = e$. Таким образом, единицы подгруппы H и группы G совпадают.

Поскольку H — подгруппа, то для каждого $h \in H$ существует в H обратный элемент h^{-1}, т.е. такой элемент, что $h^{-1}h = hh^{-1} = e_1 = e$. Это означает, что h^{-1} является обратным элементом в G.

Обратно, пусть $h_1h_2 \in H$ и $h_1^{-1} \in H$ для всех $h_1, h_2 \in H$. Тогда на H определена алгебраическая операция. 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. $\boxtimes$

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 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.

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 для любого $x \in G$.*

$\square$ 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 $t_1t_2 = h_1^xh_2^x = (h_1h_2)^x \in H^x$, так как $h_1h_2 \in H$. Кроме того, $t_1^{-1} = (x^{-1}h_1x)^{-1} = x^{-1}h_1^{-1}x \in H^x$, поскольку $h_1^{-1} \in H$. Условия теоремы 1.11 выполняются, следовательно, H^x — подгруппа. $\boxtimes$

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 $d_1, d_2 \in D$, то $d_1, d_2 \in H_\alpha$ для всех $\alpha \in I$. Значит, $d_1 d_2 \in H_\alpha$ и $d_1 d_2 \in D$. Если $d \in D$, то $d \in H_\alpha$ и $d^{-1} \in H_\alpha$ для всех $\alpha \in I$. Следовательно, $d^{-1} \in D$ и D — подгруппа группы G согласно теореме 1.11. ⊠

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 получаем равенство $\langle\emptyset\rangle = E$, а также следующее утверждение:

Лемма 1.15. *Подгруппа, порожденная непустым множеством T, является наименьшей подгруппой, содержащей множество T.*

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

Теорема 1.16. *Пусть T — непустое подмножество группы G. Тогда подгруппа $\langle T\rangle$ состоит из всех конечных произведений элементов из T и им обратных, 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 $u, v \in F$. 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, $u^{-1} = (t_1 \cdots t_n)^{-1} = t_n^{-1} \cdots t_1^{-1} \in F$, поскольку $t_i^{-1} \in \{T \cup T^{-1}\}$. Условия теоремы 1.11 выполняются, поэтому F — подгруппа.

Подгруппа F содержит подмножество T, значит, F встречается среди подгрупп, участвующих в пересечении $\bigcap_{T\subseteq H\leq G} H$, поэтому $\langle T\rangle \subseteq F$.

Проверим обратное включение. По определению
$$\langle T\rangle = \bigcap_{T\subseteq H\leq G} H.$$
Если H — подгруппа и $T \subseteq H$, то $T^{-1} \subseteq H$ и $F \subseteq H$ по теореме 1.11. Поэтому $F \subseteq \langle T\rangle$ и $\langle T\rangle = F$.

Решетка подгрупп. Пусть $\mathbf{S}(G)$ обозначает множество всех подгрупп группы G с бинарным отношением $\leq$. Две подгруппы A и B 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 $\{A, B\}$. Из теоремы 1.16 получаем, что $\langle A\cup B\rangle$ будет точной верхней гранью множества $\{A, B\}$. Таким образом, доказана

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

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 $C_G(T)$.

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

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 $C_G(T^x) = C_G(T)^x$.

$\square$ 1. Пусть $x, y \in C_G(T)$. Тогда для любого элемента $t \in T$ получаем, что $xt = tx$, $yt = ty$. Поэтому $xyt = xty = txy$, $xy \in C_G(T)$. Умножив обе части равенства $xt = tx$ на x^{-1} слева, получим: $t = x^{-1}tx$, $tx^{-1} = x^{-1}t$, $x^{-1} \in C_G(T)$. По теореме 1.11 централизатор $C_G(T)$ является подгруппой.

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 $gt^x = t^x g$ для всех $t \in T$. Так как $gt^x = gx^{-1}tx = t^x g = x^{-1}txg$, то $xgx^{-1}t = txgx^{-1}$, $xgx^{-1} \in C_G(T)$. 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 из G, перестановочных с каждым элементом группы. Центр 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) $Z(G)$ является абелевой подгруппой;

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

5) если H — подгруппа, то $C_G(H) \cap H = Z(H)$;

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

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

2. Поскольку $Z(G) = C_G(G)$, 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 1.18.

3. По лемме 1.18 множество $Z(G) = C_G(G)$ является подгруппой. Если $x, y \in Z(G)$, 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 п.1 леммы следует, что G абелева.

5. 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 $x \in G$ 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 1.16 подгруппа H абелева.

Приведем примеры подгрупп. 1. Так как $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ — аддитивные группы, то $\mathbb{Z} \le \mathbb{Q} \le \mathbb{R} \le \mathbb{C}$.

2. Поскольку $\mathbb{Q}^\#, \mathbb{R}^\#, \mathbb{C}^\#, \{-1, 1\}$ — мультипликативные группы, то $\{-1, 1\} \le \mathbb{Q}^\# \le \mathbb{R}^\# \le \mathbb{C}^\#$.

3. Относительно умножения $GL(n, P)$ и $SL(n, P)$ — группы, где P — некоторое поле. Значит, $SL(n, P) \le GL(n, P)$.

4. Совокупность S_n всех перестановок степени n и совокупность A_n всех четных перестановок с операцией умножения перестановок являются группами. Поэтому $A_n \le S_n$. Несложно показать, что при любом $n \ge 4$ центры этих групп являются единичными подгруппами.

1.3. Циклические группы

Зафиксируем в группе G элемент a. Пересечение всех подгрупп группы G, содержащих элемент a, назовем *циклической подгруппой, порожденной элементом* a, и обозначим через $\langle a\rangle$. Таким образом, $\langle a\rangle = \bigcap_{a \in H \le G} H$. Из теоремы 1.16, с. 19, в случае $T = \{a\}$ следует

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

Следствие. *Циклическая подгруппа абелева.*

□ Пусть G — группа, $\langle a\rangle$ — циклическая подгруппа, порожденная элементом $a \in G$, и x, y — произвольные элементы подгруппы $\langle a\rangle$. Тогда по теореме 1.20 $x = a^n$, $y = a^m$ 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. Пусть a — элемент группы G. Если все степени элемента a различны, т.е. $a^m \neq a^n$ для всех целых $m \neq n$, то говорят, что элемент a имеет *бесконечный порядок.*

Предположим, что 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: $\mid a \mid = k$.

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

Следующая теорема показывает, что циклическая подгруппа, порожденная 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 k делит m.*

□ По теореме 1.20 $\langle a\rangle = \{a^m \mid m \in \mathbb{Z}\}$. Любое целое число m можно представить в виде $m = kq + r$, $0 \leq r \leq k - 1$. 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. когда k делит m. ⊠

Если группа G совпадает с одной из своих циклических подгрупп, то G называют *циклической группой.* В этом случае в группе G имеется элемент a такой, что

$G = \langle a \rangle$ и по теореме 1.20

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

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 $G = \langle a \rangle = \{e, a, \ldots, a^{k-1}\}$ по теореме 1.21, 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. Вначале рассмотрим бесконечные циклические группы.

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.*

$\square$ 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 $n = mq + r$, $\ 0 \leq r < m$, 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, $H \subseteq \langle a^m \rangle$. Поскольку 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.*

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 частно-*

сти, 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 $(n_1, m_1) = 1$. 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/m для каждого натурального m, 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 t на m с остатком: $t = mq + r$, $\ 0 \le r < m$. Теперь $a^r = a^{t-mq} = a^t a^{-mq} = a^t (a^{mq})^{-1} \in H$, поскольку a^t, $a^m \in H$. 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 $n = mq + r$, $\ 0 \le r < m$. 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 1.23 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 1.24 в группе G существует подгруппа $D = \langle a^{n/d} \rangle$ порядка d. Если M — другая подгруппа порядка d, то по теореме 1.24 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 теорему 1.11, с. 17, в случае, когда группа конечная.

Теорема 1.25. *Пусть H — непустое подмножество группы G и каждый элемент из H имеет конечный по-*

рядок. Если $h_1h_2 \in H$ для всех $h_1, h_2 \in H$, то H — подгруппа.

□ Так как каждый элемент $h \in H$ имеет конечный порядок, то $\langle h\rangle = \{e, h, \ldots, h^{k-1}\}$, $\quad k =| h |$. Очевидно, что $hh^{k-1} = h^{k-1}h = h^k = e$, $\quad h^{k-1} = h^{-1} \in H$. Теперь H — подгруппа по теореме 1.11, с. 17.

Следствие. *Если H — непустое подмножество конечной группы G и $h_1h_2 \in H$ для всех $h_1, h_2 \in H$, то H — подгруппа.*

Рассмотрим аддитивную группу $\mathbb{Z}$. В аддитивной записи теорема 1.20 принимает вид: $\langle a\rangle = \{ma \mid m \in \mathbb{Z}\}$. Так как $\langle 1\rangle = \{m1 \mid m \in \mathbb{Z}\}$, то $\mathbb{Z} = \langle 1\rangle$ — бесконечная циклическая группа. Ясно, что $\langle -1\rangle = \mathbb{Z}$ и $\langle a\rangle \neq \mathbb{Z}$ для любого целого $a \notin \{-1, 1\}$.

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:

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

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.

Теорема 1.26. *Порядок перестановки есть наименьшее общее кратное длин ее независимых циклов.*

□ Если (a_1a_2) — цикл длиной 2, то $(a_1a_2)(a_1a_2) = \varepsilon$, т.е. транспозиция есть перестановка порядка 2. Аналогично цикл $(a_1a_2 \ldots a_k)$ длиной k есть перестановка порядка k. Пусть теперь перестановка

$$\tau = (a_1a_2 \ldots a_{l_1}) \ldots (b_1b_2 \ldots b_{l_t})$$

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

$$\tau^k = (a_1a_2 \ldots a_{l_1})^k \ldots (b_1b_2 \ldots b_{l_t})^k.$$

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

Перечислим порядки элементов в S_3. Так как $S_3 = \{\varepsilon, (12), (13), (23), (123), (132)\}$, то на основании теоремы 1.26 имеем:

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

Перечислим порядки элементов в S_4. Запись (...)(.) обозначает любую перестановку в S_4, распадающуюся на циклы длины 3 и 1. В S_4 возможны следующие разложения: (.)(.)(.)(.), (.)(.)(..), (.)(...), (..)(..), (....). На основании теоремы 1.26 в группе S_4 элементы имеют порядки 1,2,3,4.

В группе S_6 нет элементов порядка 7,8,9,10.

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, с. 12. Пусть a, x — элементы группы G и $|\,a\,| = k$. Тогда $(a^x)^k = (a^k)^x = e$ и $|a^x|$ делит k по теореме 1.21. 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 $f : G \to G_1$ такая, что $f(ab) = f(a)f(b)$ для всех $a, b \in G$. Для обозначения изоморфизма используется запись $G \simeq G_1$. Отметим простейшие свойства изоморфизма.

Лемма 1.29. *Пусть $f : G \to G_1$ — изоморфизм группы G на группу G_1. Тогда:*

1) $f(e)$ — единичный элемент группы G_1, где e — единичный элемент группы G;

2) $f(a^{-1})$ — обратный элемент к элементу $f(a)$ в группе G_1 для любого $a \in G$.

Лемма 1.30. *1. $G \simeq G$.*

2. Если $G \simeq G_1$, то $G_1 \simeq G$.

3. Если $G \simeq G_1$ и $G_1 \simeq G_2$, то $G \simeq G_2$.

4. Отношение "быть изоморфными группами" является отношением эквивалентности.

□ 1. Отображение $\varepsilon_G : G \to G$, переводящее каждый элемент в себя, является изоморфизмом G на G.

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

3. Пусть $f : G \to G_1$ — изоморфизм групп G и G_1, а $\varphi : G_1 \to G_2$ — изоморфизм G_1 и G_2. Тогда φf — биективное отображение G на G_2 причем $\varphi f(ab) = \varphi(f(ab)) = \varphi(f(a)f(b)) = \varphi(f(a))\varphi(f(b)) = \varphi f(a)\varphi f(b)$ для любых a и $b \in G$. Значит, φf — изоморфизм G и G_2.

4. Данное утверждение следует из свойств 1–3.

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 $< g >$ — 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 $< g >$. 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 $G_1 = \{e_1, g_1, g_1^2, \ldots, g_1^{k-1}\}$; $G_2 = \{e_2, g_2, g_2^2, \ldots, g_2^{k-1}\}$ — циклические группы порядка k. Определим отображение $f : g_1^t \mapsto g_2^t,\ t = 0, 1, 2, \ldots, k-1$. Для $n, m \in \{0, 1, \ldots, k-1\}$ имеем $n + m = kq + r,\ 0 \leq r \leq k-1$. Тогда $f(g_1^n g_1^m) = f(g_1^r) = g_2^r = g_2^n g_2^m = f(g_1^n)f(g_1^m)$

и f — изоморфизм G_1 на G_2.

Матрица перестановки. *Матрицей перестановки* $\pi \in S_n$ называется $n\times n$-матрица $\mathcal{M}(\pi)=(a_{ij})$, определенная следующим образом:

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

В матрице перестановки n единиц, остальные элементы равны нулю. Единица встречается один раз в каждой строке и в каждом столбце. В j-м столбце единица стоит на $\pi(j)$-м месте, т.е. в матрице $\mathcal{M}(\pi)$ только элементы $a_{\pi(k)k} = 1$, где $k = 1, 2, \ldots, n$, а остальные — нули. Очевидно, что $\mathcal{M}(\varepsilon) = E$ — единичная матрица, здесь ε — единичный элемент в S_n. Через $\operatorname{sgn}(\pi)$ 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. $\det \mathcal{M}(\pi) = sgn(\pi)$ 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 $Im\mathcal{M} = \{\mathcal{M}(\tau) \mid \tau \in S_n\}$ из группы $GL(n, \mathbb{R})$.

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

$$\mathcal{M}(\pi)_i\mathcal{M}(\tau)^j = (0\ldots1\ldots0)[0\ldots1\ldots0] =$$

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

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. Определитель матрицы вычисляется по формуле

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

В матрице $\mathcal{M}(\pi) = (a_{ij})$ только элементы $a_{\pi(k)k}$ равны единице, остальные — нули. Поэтому $\det \mathcal{M}(\pi) = \mathrm{sgn}(\pi)$.

3. Так как $\det \mathcal{M}(\tau) = \mathrm{sgn}(\tau) \in \{-1, 1\}$, то $\mathcal{M}$ — отображение S_n в $GL(n, \mathbb{R})$. Из построения $\mathcal{M}(\tau)$ следует, что $\mathcal{M}$ — инъекция. Покажем, что $\mathrm{Im}\mathcal{M}$ — подгруппа группы $GL(n, \mathbb{R})$. Так как $\mathcal{M}(\tau)\mathcal{M}(\pi) = \mathcal{M}(\tau\pi)$ (см. утверждение 1 теоремы), то $\mathcal{M}(\tau)\mathcal{M}(\pi) \in \mathrm{Im}\mathcal{M}$. 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 согласно теореме 1.25, с. 25, $\mathrm{Im}\mathcal{M}$ — подгруппа $GL(n, \mathbb{R})$. Поэтому $\mathcal{M} : S_n \to \mathrm{Im}\mathcal{M}$ — биекция, а по утверждению 1 отображение $\mathcal{M}$ — изоморфизм.

Теорема 1.33. *Любая конечная группа порядка n изоморфна подгруппе симметрической группы S_n степени n.*

□ Пусть G — группа порядка n и $G = \{g_1, g_2, \dots, g_n\}$ — все ее элементы. Можно считать, что S_n — совокупность всех биективных отображений множества $\{g_1, g_2, \dots, g_n\}$ 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 $\varphi : G \to S_n$, полагая $\varphi : x \mapsto l_x$, $x \in G$. Тогда $\mathrm{Im}\varphi = \{lg_1, lg_2, \dots, lg_n\}$. Покажем, что $\mathrm{Im}\varphi$ — подгруппа группы S_n. Если l_x и l_y — произвольные элементы из $\mathrm{Im}\varphi$, то

$$l_x l_y(g_i) = l_x(l_y(g_i)) = l_x(yg_i) = xyg_i = l_{xy}(g_i)$$

и $l_x l_y = l_{xy} \in \mathrm{Im}\varphi$. По теореме 1.25, с. 25, множество $\mathrm{Im}\varphi$ есть подгруппа группы S_n. Так как $l_x l_y = l_{xy}$, то $\varphi(xy) = \varphi(x)\varphi(y)$ и φ — изоморфизм между G и $\mathrm{Im}\varphi$.

Следствие. *Любая конечная группа порядка n изоморфна подгруппе полной линейной группы $GL(n, \mathbb{R})$*

степени n над $\mathbb{R}$. В частности, число неизоморфных групп данного порядка конечно.

$\square$ Первое утверждение вытекает из теорем 1.32, 1.33. Для получения второго — зафиксируем натуральное число n. По теореме 1.33 каждая группа порядка n изоморфна подгруппе симметрической группы S_n. Поскольку S_n — конечная группа, то число ее неизоморфных подгрупп конечно.

Автоморфизмы групп. Изоморфное отображение группы G на себя называют *автоморфизмом группы* G. Совокупность всех автоморфизмов группы G обозначим через $\mathrm{Aut}G$. Если φ и ψ — автоморфизмы группы G, то согласно определению умножения отображений произведение автоморфизмов определяется так:

$$\varphi\psi(ab) = \varphi(\psi(ab)) = \varphi(\psi(a)\psi(b)) =$$
$$= \varphi(\psi(a))\varphi(\psi(b)) = \varphi\psi(a)\varphi\psi(b)$$

для любых $a, b \in G$. Поэтому $\varphi\psi$ — автоморфизм G, и умножение автоморфизмов определено на $\mathrm{Aut}G$. Ассоциативность умножения автоморфизмов следует из ассоциативности умножения отображений. Отображение $\varepsilon_G : G \to G$, переводящее каждый элемент в себя, является автоморфизмом группы G. По лемме 1.30 каждый автоморфизм имеет обратный. Итак, доказана следующая

Теорема 1.34. *Совокупность $AutG$ всех автоморфизмов группы G является группой.*

Мультипликативная группа $\mathbb{R}_+$ положительных действительных чисел изоморфна аддитивной группе $\mathbb{R}$ всех действительных чисел. Логарифмическая функция $y = \ln x$ задает биективное отображение $\mathbb{R}_+$ на $\mathbb{R}$. Если $x, y \in \mathbb{R}_+$, то $\ln(xy) = \ln x + \ln y$ и $\ln$ — изоморфизм групп $\mathbb{R}_+$ и $\mathbb{R}$.

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

$$f(h_1h_2) = (h_1h_2)^x = (h_1)^x(h_2)^x = f(h_1)f(h_2),$$

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

Перечислим матрицы, соответствующие перестановкам степени

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

$$\mathcal{M}(\varepsilon) = E, \qquad \mathcal{M}(12) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$\mathcal{M}(13) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \quad \mathcal{M}(23) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\mathcal{M}(123) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \mathcal{M}(132) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Пример 1.2. Проверить, 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

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

Остальные произведения элементов из G также принадлежат G, поэтому G — группа. Очевидно, что отображение

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

будет изоморфизмом.

1.5. Смежные классы

Пусть G — группа, H — ее подгруппа 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 $\mid Hg \mid = \mid H \mid$ для всех $g \in G$.

□ 1–3. Данные утверждения очевидны.

Докажем свойство 4. Если $Ha = Hb$, то $ea = hb$, $h \in H$ и $ab^{-1} = h \in H$. Обратно, если $ab^{-1} \in H$, то $a \in Hb$ и $Ha = Hb$ по утверждению 3.

Докажем свойство 5. Пусть $Ha \cap Hb \neq \emptyset$ и $c \in Ha \cap Hb$. Тогда $c = h_1 a = h_2 b$ и $ab^{-1} = h_1^{-1} h_2 \in H$. Теперь $Ha = Hb$ по утверждению 4.

Докажем свойство 6. Отображение $\phi : h \mapsto hg$ есть биекция множеств H и Hg. Поэтому $\mid H \mid = \mid Hg \mid$.

Трансверсаль. Пусть H — подгруппа группы G. Из свойств 2 и 5 леммы 1.35 следует, что каждый элемент группы G содержится точно в одном правом смежном классе по подгруппе H. Это свойство позволяет ввести следующее определение. Подмножество T элементов группы G называется *правой трансверсалью* H в 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 H в G, то $G = \bigcup_{t_\alpha \in T} Ht_\alpha$, $Ht_\alpha \cap Ht_\beta = \emptyset$ при $\alpha \neq \beta$. Таким образом справедлива

Теорема 1.36. *Если H — подгруппа группы G, то G совпадает с объединением непересекающихся правых смежных классов по H.*

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

Теорема 1.37 (Лагранжа). *Если H — подгруппа конечной группы G, то $\mid G \mid = \mid H \mid \mid G : H \mid$. В частно-*

сти, порядок конечной группы делится на порядок каждой своей подгруппы.

☐ Пусть индекс H в G равен n. По теореме 1.36 имеем разложение $G = Hg_1 \cup Hg_2 \cup \ldots \cup Hg_n,\ Hg_i \cap Hg_j = \emptyset$ при $i \neq j$. Так как $\mid Hg_i \mid = \mid H \mid$ для всех i, то $\mid G \mid = \mid H \mid\mid G : H \mid$.

Следствие 1. *Порядок каждого элемента конечной группы делит порядок всей группы.*

☐ По теореме 1.21, с. 23, $\mid a \mid = \mid \langle a \rangle \mid$ для каждого $a \in G$, поэтому $\mid a \mid$ делит $\mid G \mid$. ⊠

Аналогично определяется *левая трансверсаль* подгруппы H в группе G. Если $L = \{l_\alpha \mid \alpha \in J\}$ — левая трансверсаль H в G, то $G = \bigcup_{\alpha \in J} l_\alpha H,\ l_\alpha H \cap l_\beta H = \emptyset$ при $\alpha \neq \beta$. Ясно, что индекс подгруппы H в конечной группе G совпадает с числом элементов в левой трансверсали L подгруппы H, т.е. $\mid G : H \mid = \mid L \mid$. Для левой трансверсали справедлив аналог теоремы 1.36. Поэтому из теоремы Лагранжа имеем

Следствие 2. *Если H — подгруппа конечной группы G, то число левых и число правых смежных классов G по H совпадают.*

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

☐ Пусть G — группа простого порядка p. Если H — подгруппа, то по теореме Лагранжа $\mid H \mid$ делит $\mid G \mid$. Поэтому либо $\mid H \mid = 1$ и $H = E$, либо $\mid H \mid = p$ и $H = G$. Выберем неединичный элемент a и рассмотрим циклическую подгруппу $\langle a \rangle$, порожденную этим элементом. Так как $a \neq e$, то $\langle a \rangle \neq E$, поэтому $\langle a \rangle = G$ — циклическая группа.

Теорема 1.39. *Пусть $H \leq K \leq G$ и G — конечная группа. Если T — правая трансверсалъ H в K, а S — правая трансверсаль K в G, то TS — правая трансверсалъ H в G. В частности, $\mid G : H \mid = \mid G : K \mid\mid K : H \mid$.*

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

$$K = Ht_1 \cup \ldots \cup Ht_k,\ Ht_i \cap Ht_j = \emptyset,\ i \neq j,$$

$$G = Ks_1 \cup \ldots \cup Ks_n,\ Ks_i \cap Ks_j = \emptyset,\ i \neq j,$$

$$G = (Ht_1 \cup \ldots \cup Ht_k)s_1 \cup \ldots \cup (Ht_1 \cup \ldots \cup Ht_k)s_n. \quad (1.3)$$

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

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

следовательно, $s_b s_d^{-1} \in t_a^{-1} K t_c = K,\ Ks_b = Ks_d$. Но s_b и s_d — элементы из правой трансверсали K в G, значит, $s_b = s_d$ и $b = d$. Теперь

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

Таким образом, формула (1.3) является разложением G по H и TS — правая трансверсаль H в G. Так как индекс подгруппы совпадает с числом элементов в ее правой трансверсали, то $\mid G : H \mid = \mid TS \mid = \mid T \mid\mid S \mid = \mid K : H \mid\mid G : K \mid$. $\boxtimes$

Отметим, что теорема Лагранжа вытекает из теоремы 1.39 при $H = E$.

Двойные смежные классы. Пусть H и K — подгруппы группы G и $g \in G$. Множество $HgK = \{hgk \mid h \in H,\ k \in K\}$ 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 и левых смежных классов по K;

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

□ Докажем свойство 1. Так как каждая подгруппа содержит единичный элемент, то $g = ege \in HgK$. Допустим, что $g \in HxK$. Тогда $g = hxk$ для некоторых $h \in H,\ k \in K$ и $HgK = H(hxk)K = HxK$.

2–3. Утверждения следуют из утверждения 1.

Утверждение 4 следует из равенства $HgK = \bigcup_{k\in K} Hgk = \bigcup_{h\in H} hgK$.

Для доказательства свойства 5 подсчитаем число правых смежных классов в разложении $HgK = \bigcup_{k\in K} Hgk$ по подгруппе H. Допустим, что $Hgk_1 = Hgk_2$. Тогда

$$Hgk_1k_2^{-1} = Hg,\ k_1k_2^{-1} \in g^{-1}Hg \cap K = H^g \cap K.$$

Справедливо и обратное, т.е. если $k_1k_2^{-1} \in H^g \cap K$, то

$$k_1k_2^{-1} \in g^{-1}Hg,\ gk_1k_2^{-1} \in Hg,\ gk_1 \in Hgk_2,\ Hgk_1 = Hgk_2.$$

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

Аналогично $HgK = \bigcup_{h\in H} hgK$ и $h_1gK = h_2gK$ тогда и только тогда, когда $h_1^{-1}h_2 \in H \cap K^{g^{-1}}$. Поэтому в произведении HgK левых смежных классов по K будет точно столько, каков индекс $\mid H : H \cap K^{g^{-1}} \mid$.

Произведение подгрупп. При $g = e$ двойной смежный класс $HgK = HK = \{hk \mid h \in H,\ k \in K\}$ превращается в произведение подгрупп H и K. В общем случае HK 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 $h_1k_1 = k_2h_2$.

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

□ Пусть H, K — подгруппы группы G. Предположим, что HK — подгруппа и $h \in H,\ k \in K$. 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_1k_1 такой, что $(h_1k_1)^{-1} = hk$, то $hk = k_1^{-1}h_1^{-1} \in$

KH и $HK \subseteq KH$. 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 $k_1h_2 = h_3k_3$, где $h_3 \in H$, $k_3 \in K$. Поэтому

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1h_3k_3k_2 \in HK,$$
$$(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH = HK.$$

Значит, произведение HK является подгруппой.

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

☐ Согласно лемме 1.40 произведение $HeK = HK$ есть объединение правых смежных классов по H и таких классов $| K : K \cap H |$. Поскольку $| Hk |=| H |$ 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 *факторизуема подгруппами* H, 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 $G = H^xK$ при любом $x \in G$.*

☐ Если $G = HK$, то $G = KH$ по теореме 1.41. Если x — произвольный элемент из G, то $x = hk$, где $h \in H, k \in K$ и $H^xK = H^{hk}K = H^kK = k^{-1}HkK = k^{-1}HK = k^{-1}KH = KH = G$.

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

☐ Допустив, что $H^xH = G$ для некоторого $x \in G$, согласно лемме 1.43 имеем $G = (H^x)^{x^{-1}}H = H$, т.е. получили противоречие.

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 положим $A = \langle a \rangle$. Если $A = G$, то G — циклическая группа. Пусть $A \neq G$.

По теореме Лагранжа $\mid A \mid = p$. Выберем $b \in G \setminus A$ и положим $B = \langle b \rangle$. Если $B = G$, то $G = \langle b \rangle$ — циклическая группа. Пусть $B \neq G$. По теореме Лагранжа $\mid B \mid = p$. Так как $A \cap B$ — собственная подгруппа в A, и в B, то по теореме Лагранжа $A \cap B = E$ и $\mid AB \mid = \mid A \mid\mid B \mid = p^2$, т.е. $AB = BA = G$. По лемме 1.44 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

$$\mid AA^g \mid = \mid A \mid\mid A^g \mid = \mid G \mid,$$

т.е. $G = AA^g$, что противоречит лемме 1.44. Поэтому $A = A^g$ при любом $g \in G$. Аналогично $B = B^g$ при любом $g \in G$. Теперь для любых $a \in A,\ b \in B$ имеем:

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

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

Лемма 1.46. *Пусть H — подгруппа группы G. Тогда:*

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

2) $Z(G)Z(H)$ — абелева подгруппа.

☐ 1. Из определения центра следует, что для $Z(G)$ и H выполняются условия теоремы 1.41, поэтому $Z(G)H = HZ(G)$ — подгруппа. Если $x, y \in Z(G)H$, 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 H — произвольная подгруппа. Тогда $Z(H)$ является абелевой подгруппой и $Z(G)Z(H)$ — абелева подгруппа по свойству 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 $G,\ x, y \in G$. Тогда:*

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

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

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

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

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

то $y^{-1}(x^{-1}tx)y \in (T^x)^y$, 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

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

Таким образом, $(T^x)^y = T^{(xy)}$.

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

Утверждения 3 и 4 очевидны.

Нормализатор. Если T — непустое подмножество группы G и $g \in G$, то $gT = \{gt \mid t \in T\}$ 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 $gT = Tg$ 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) $N_G(T) \le G$;

2) $C_G(T) \le N_G(T)$;

3) $N_G(T^g) = N_G(T)^g$;

4) $N_G(T) \le N_G(C_G(T))$;

5) если H — подгруппа группы G, то $H \le N_G(H)$.

□ 1. Утверждение вытекает из леммы 1.47.

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 $C_G(T) = C_G(T^x) = C_G(T)^x$, 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 $T = \{t_1, \ldots, t_n\}$ — правая трансверсаль нормализатора $N_G(S)$ в группе G, то $\Sigma = \{S^{t_1}, \ldots, S^{t_n}\}$ — 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 G, совпадает с индексом нормализатора $N_G(S)$.*

□ Пусть $K = N_G(S)$. По условию $G = Kt_1 \cup \ldots \cup Kt_n$, $Kt_i \neq Kt_j$ при $i \neq j$. Если x — произвольный элемент из G, то $x = kt_i$ для некоторого $k \in K$ и натурального числа i. Поэтому $S^x = S^{kt_i} = S^{t_i} \in \Sigma$. Если предположить, что $S^{t_i} = S^{t_j}$, то $S = S^{t_jt_i^{-1}}$ и $t_jt_i^{-1} \in K$, т.е. $Kt_j = Kt_i$. Так как элементы t_i и t_j принадлежат правой трансверсали K в 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 1. *Число подмножеств, сопряженных данному непустому подмножеству S в конечной группе G, делит порядок группы G.*

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

Следствие 2. *Если s — элемент конечной группы G и $T = \{t_1, \ldots, t_n\}$ — правая трансверсаль централиза-*

тора $C_G(S)$, *то* $s^G = \{s^{t_1}, \ldots, s^{t_n}\}$. *В частности, число элементов, сопряженных элементу* s *в* G, *совпадает с индексом централизатора* $C_G(S)$ *в* G *и делит порядок группы* G.

В дальнейшем мы неоднократно будем использовать приводимое ниже 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 $x = ab \in A(C \cap B)$, $a \in A$, $b \in C \cap B$. Поскольку $A \leq C$, то $a \in C$ и $x = ab \in C$. Таким образом, $x = ab \in C \cap AB$.

Пример 1.3. Найти разложение симметрической группы S_3 в левые смежные классы по подгруппе $\langle(12)\rangle$.

□ Вначале перечислим 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 1.4. Найти 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. 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 1.1), то H_3, H_4, H_5 сопряжены и 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 фактор-группы

Подгруппа H называется *нормальной подгруппой* группы G, если $xH = Hx$ для всех $x \in G$. Запись $H \lhd G$ читается: "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. *Для подгруппы H группы G следующие утверждения эквивалентны:*

1) H — нормальная подгруппа;

2) подгруппа H вместе с каждым своим элементом содержит все ему сопряженные 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 $H \lhd G$, 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 $x^{-1}hx = h_1 \in H$.

$2 \Rightarrow 3$. Ясно, что $H^x = \{h^x \mid h \in H\} \subseteq H$ 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 — нормальная подгруппа группы G.

Следствие. *Если $H \lhd G$ и $h \in H$, то $h^G \subseteq H$. Обратно, если $h^G \subseteq H$ для всех $h \in H$, то $H \lhd G$.*

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

Лемма 1.52. *Пусть H — подгруппа группы G. Тогда:*

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

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

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

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

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

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

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

3. Из утверждения 1 следует, что $H \lhd N_G(H)$, а из утверждения 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.

4. Утверждение следует из утверждения 3.

5. Если $x \in N_G(T)$, то $T = T^x$. Поэтому $C_G(T)^x = C_G(T)$ согласно лемме 1.18, с. 20, и $C_G(T) \lhd N_G(T)$.

Лемма 1.53. *Пусть H — нормальная подгруппа группы G. Тогда:*

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

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

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

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

$\square$ 1. Если $L \leq G$, то $HL = LH$ и $HL \leq G$ по теореме 1.41, с. 36. Так как $(H \cap L)^l = H^l \cap L^l = H \cap L$ для всех $l \in L$, то $H \cap L \lhd L$.

2. Если $L \lhd G$, то очевидно, что $HL \lhd G$ и $H \cap L \lhd G$.

3. Так как $C_G(H) \lhd N_G(H)$ и $N_G(H) = G$ на основании леммы 1.52, то $C_G(H) \lhd G$.

4. Поскольку $Z(H) = H \cap C_G(H)$ согласно лемме 1.19, с. 21, то $Z(H) \lhd G$ по свойству 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, каж-*

дая 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 1.22, с. 24, 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 $\langle a^p \rangle$, порожденная 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 1.38, с. 34, 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 $n > 4$.

Фактор-группа. 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

$$(xH)(yH) = xyH. \tag{1.4}$$

Проверим, задает ли это равенство 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 $(x_1H)(y_1H) = x_1y_1H = (xh)(yg)H = xy(y^{-1}hy)gH = xyH$, так как $y^{-1}hy \in H$ по теореме 1.51. Таким образом, равенство (1.4) не зависит от выбора представителей смежных классов и каждой паре xH, yH ставится в соответствие единственный элемент xyH.

Ясно, что предложенная операция (1.4) 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 $(aH)^{-1} = a^{-1}H$.*

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

Если группа G конечна, то фактор-группа группы G по любой нормальной подгруппе H также будет конечной группой порядка, равного индексу подгруппы H в группе G, т.е. $\mid G/H \mid = \mid G : H \mid = \mid G \mid / \mid H \mid$.

Лемма 1.56. *Если фактор-группа $G/Z(G)$ — циклическая, то группа G абелева.*

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

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

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

Теорема 1.57. *Все фактор-группы 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 числа m.*

$\square$ Так как каждая циклическая группа абелева, то в ней любая подгруппа нормальна. По теореме 1.22, с. 24, все подгруппы бесконечной циклической группы $A = \langle a \rangle$ исчерпываются единичной подгруппой E и бесконечными циклическими подгруппами $M = \langle a^m \rangle$, $m \in \mathbb{N}$. Фактор-группа A/E будет бесконечной циклической группой, изоморфной A. Так как $A = \{a^k \mid k \in \mathbb{Z}\}$, то A/M состоит из смежных классов $a^k M$, $k \in \mathbb{Z}$. Если $a^s M = a^t M$, то $a^{s-t} \in M$ и $s - t$ кратно m. Отсюда следует, что смежные классы $M, aM, a^2 M, \ldots, a^{m-1} M$ попарно различны. Кроме того, для любого $a^t M \in A/M$ имеем:

$t = mq + r, \quad 0 \le r < m$ и $a^t M = a^{mq} a^r M = a^r M$. Таким образом, $A/M = \{M, aM, a^2 M, \ldots, a^{m-1} M\} = \langle aM \rangle$, т.е. A/M будет конечной циклической группой порядка m.

Теорема 1.58. *Все фактор-группы 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 1.24, с. 25, все подгруппы группы $A = \langle a \rangle$ исчерпываются подгруппами $M = \langle a^m \rangle$ порядка n/m для каждого m, делящего n. Легко доказать, что

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

т.е. $A/M = \langle a \langle a^m \rangle \rangle$ — циклическая группа порядка m.

Теорема о соответствии. Через $\mathbf{S}(G, H)$ условимся 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 (о соответствии). *Пусть H — нормальная подгруппа группы G. Тогда:*

1) если U — подгруппа группы G и $H \le U$, то $\overline{U} = U/H$ — подгруппа фактор-группы $\overline{G} = G/H$;

2) каждая подгруппа фактор-группы $\overline{G} = G/H$ имеет вид $\overline{V} = V/H$, где V — подгруппа группы G и $H \le V$;

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

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

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

$$(u_1 H)(u_2 H) = u_1 u_2 H \in \overline{U}, \ (u_1 H)^{-1} = u_1^{-1} H \in \overline{U}$$

и согласно теореме 1.11, с. 17, $\overline{U}$ — подгруппа группы $\overline{G}$.

2. Пусть $\overline{V}$ — произвольная подгруппа из $\overline{G}$. Тогда $\overline{V}$ состоит из некоторых смежных классов G по H. Обозна-

чим через V множество всех тех элементов группы G, из которых состоят смежные классы, принадлежащие $\overline{V}$, т.е. $V = \{x \in G \mid xH \in \overline{V}\}$. Если $v_1, v_2 \in V$, то $v_1H, v_2H \in \overline{V}$, а так как $\overline{V}$ — подгруппа, то

$$(v_1H)(v_2H) = v_1v_2H \in \overline{V},\ (v_1H)^{-1} = v_1^{-1}H \in \overline{V}.$$

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

3. Отображение $\varphi : U \mapsto \overline{U}$ будет сюръекцией по свойству 2. Докажем, что φ — инъекция. Пусть U и V — подгруппы, содержащие H. Предположим, что подгруппы $\overline{U} = \{uH \mid u \in U\}$ и $\overline{V} = \{vH \mid v \in V\}$ совпадают. Тогда для любого $u \in U$ существует $v \in V$ 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 $N \lhd G$, $N \in \mathbf{S}(G, H)$, то $(gH)^{-1}(nH)(gH) = g^{-1}ngH \in N/H$ для всех $g \in G$, $n \in N$. Поэтому $\overline{N} = N/H \lhd \overline{G}$. Обратно, если $\overline{N} \lhd \overline{G}$, то

$$g^{-1}ngH = (gH)^{-1}(nH)(gH) \in \overline{N},\ g^{-1}ng \in N.$$

Значит $N \lhd G$. ⊠

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 1.17, с. 20, доказано, что множество $\mathbf{S}(G)$ с бинарным отношением $\leq$ является решеткой. Ясно, что $\mathbf{Sn}(G) \subseteq \mathbf{S}(G)$. По лемме 1.53

$$H \cap L \lhd G,\ \langle H \cup L \rangle = HL \lhd G$$

для всех $H, L \lhd G$, поэтому $\mathbf{Sn}(G)$ — подрешетка решетки $\mathbf{S}(G)$. ⊠

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

Теорема 1.61. *1. Если H — максимальная нормальная подгруппа нееденичной группы G, то фактор-группа G/H является простой группой.*

2. Если H — нормальная подгруппа группы G и фактор-группа G/H простая, то H — максимальная нормальная подгруппа группы G.

□ 1. Предположим, что G/H непростая. Тогда существует нетривиальная нормальная подгруппа K/H группы G/H. По теореме 1.59 подгруппа K нормальна в G и $K \neq G,\ K \neq H,\ H \leq K$. Получили противоречие.

2. Пусть H — нормальная подгруппа группы G и 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 в G/H, т.е. G/H непростая.

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 $\mid G \mid$ и H — подгруппа индекса p. Предположим, что подгруппа H не является нормальной. По теореме 1.51 существует элемент $x \in G$ такой, что $H \neq H^x$. Поскольку $\mid H \mid / \mid H \cap H^x \mid \neq 1$ и делит $\mid G \mid$, то $\mid H \mid / \mid H \cap H^x \mid \geq p$ и $\mid G \mid \geq \mid HH^x \mid = \mid H \mid\mid H^x \mid / \mid H \cap H^x \mid \geq \mid H \mid p = \mid H \mid\mid G : H \mid = \mid G \mid$ по теореме 1.42, с. 37. Поэтому $G = HH^x$, что противоречит лемме 1.44, с. 37.

Подгруппа индекса 2 нормальна в группе. В частности, $A_n \lhd S_n$.

В аддитивной группе $\mathbb{Z}$ целых чисел подгруппа $5\mathbb{Z} = \{5k \mid k \in \mathbb{Z}\}$ чисел, кратных 5, нормальна. Смежные классы $\mathbb{Z}$ по $5\mathbb{Z}$ имеют вид $i + 5\mathbb{Z}$, где $i = 0, 1, 2, 3, 4$. Фактор-группа

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

состоит из пяти элементов. Нулевым элементом будет $5\mathbb{Z}$. Сложение в G/H определяется равенством $(a + H) + (b + H) = (a + b) + H$. Например, $(2+5\mathbb{Z})+(4+5\mathbb{Z}) = 6+5\mathbb{Z} = 1+5\mathbb{Z}$. Вычислив остальные суммы, можно составить таблицу сложения для фактор-группы. Ясно, что $\mathbb{Z}/5\mathbb{Z} = \langle 1 + 5\mathbb{Z}\rangle$ — циклическая группа порядка 5.

Пример 1.5. Найти все фактор-группы группы S_3.

$\square$ Среди подгрупп группы S_3 со своими сопряженными совпадают следующие подгруппы: $E,\ S_3,\ H = \langle(123)\rangle$, см. пример 1.4, с. 41. По теореме 1.51 эти три подгруппы нормальны в S_3. Ясно, что S_3/S_3 — единичная группа, а S_3/E изоморфна S_3. Порядок подгруппы $H = \langle(123)\rangle$ равен 3, а порядок S_3/H равен 2. Поэтому S_3/H — циклическая группа порядка 2. Смежные классы S_3 по H исчерпываются классами H и $(12)H$. Таким образом, группа S_3 имеет три фактор-группы: $S_3/E \simeq S_3,\ S_3/S_3 \simeq E,\ S_3/H = \{H, (12)H\} = \langle(12)H\rangle$.

1.7. Силовские подгруппы конечных групп

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

Пример 1.6. Доказать, что знакопеременная группа A_4 порядка 12 не содержит подгрупп порядка 6.

$\square$ Допустим противное. Пусть H — подгруппа порядка 6. Тогда $\mid A_4 : H \mid = 2$ и $H \lhd A_4$ согласно теореме 1.62. Группа A_4 содержит подгруппы $K_1 = \langle(234)\rangle$, $K_2 = \langle(134)\rangle$. Если $K_i \not\leq H$, то $H \cap K_i = E$ и $\mid HK_i \mid = \mid H \mid\mid K_i \mid = 18$, т.е. получили противоречие. Следовательно, $K_1K_2 \subseteq H$, а так как $K_1 \cap K_2 = E$, то $\mid K_1K_2 \mid = 9$. Снова получили противоречие. Значит допущение неверно и A_4 не содержит подгрупп порядка 6.

Вполне естественно возникает вопрос: *для каких делителей d порядка группы имеется подгруппа порядка d?* В случае, когда d — степень простого числа, ответ 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 G существует подгруппа порядка p.*

$\square$ Применим индукцию по порядку группы. Пусть H — максимальная подгруппа. Ясно, что H абелева и $|H| < |G|$. Если $|H|$ делится на p, то по индукции в H имеется подгруппа порядка p. Пусть $|H|$ не делится на p. Так как $|G| = |H||G : H|$, то p делит $|G : H|$. По теореме 1.61, с. 48, G/H является простой группой, а на основании теоремы 1.54, с. 43, фактор-группа $G/H = \langle gH \rangle$ является циклической группой простого порядка p. Но теперь $G = H\langle g \rangle$ и согласно теореме 1.42, с. 37, число $p = |G : H| = |\langle g \rangle : H \cap \langle g \rangle|$ делит $|\langle g \rangle|$. Пусть $|\langle g \rangle| = pm$. Тогда $\langle g^m \rangle$ — подгруппа порядка p. ⊠

Пусть p — простое число. Конечная группа, порядок которой есть степень простого числа p, называется *p-группой.* Если группа является p-группой для некоторого простого числа p, то она называется *примарной.*

Теорема 1.64 (Силова). *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 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;

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

□ 1. Доказательство проведем индукцией по $\mid G \mid$. По индукции считаем, что для всех групп, порядок которых меньше порядка G, утверждение 1 теоремы выполняется. Предположим вначале, что 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 фактор-группа G/N имеет порядок $p^{m-1}s <\mid G \mid$ и по индукции в $G/N = \overline{G}$ найдется подгруппа $\overline{P_i}$ порядка p^i для каждого $i = 1, 2, \dots, m-1$. По теореме о соответствии в G имеется подгруппа P_i такая, что $P_i \geq N$ и $P_i/N = \overline{P_i}$. Теперь $\mid P_i \mid = p^{i+1}$, где $i = 1, 2, \dots, m-1$. Итак, в группе G существуют подгруппы $P_1, P_2, \dots, P_{m-1}$ порядков $p^2, p^3, \dots, p^m$ соответственно, и подгруппа N порядка p.

Теперь перейдем к случаю, когда порядок $Z(G)$ не делится на p. Рассмотрим разложение группы G на различные классы сопряженных элементов

$$G = K_1 \cup K_2 \cup \ldots \cup K_d, \tag{1.5}$$

где $K_i = x_i^G = \{x_i^g \mid g \in G\}$ — класс сопряженных с x_i элементов. По лемме 1.9, с. 12, пересечение различных классов — пустое множество, а по следствию 2 теоремы 1.49, с. 40, число элементов в классе x_i^G равно индексу централизатора $C_G(x_i)$. Пусть $k_i =\mid K_i \mid=\mid G : C_G(x_i) \mid$. 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 разложения (1.5) получаем

$$\mid G \mid= \underbrace{1 + 1 + \ldots + 1}_{\mid Z(G)\mid} + k_c + k_{c+1} + \ldots + k_d, \tag{1.6}$$

где $k_j > 1$ для каждого $j \geq c$. Если все числа $k_c, \ldots, k_d$ делятся на p, то из суммы (1.6) следует, что $\mid Z(G) \mid$ делится на p, что противоречит рассматриваемому случаю. Итак, существует k_f, где $f \geq c$ такое, что p не делит k_f. Поскольку $k_f =\mid G : C_G(x_f) \mid$, то $\mid C_G(x_f) \mid= p^m s_1 <\mid G \mid$, 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 $C_G(x_f)$ существует подгруппа порядка p^i для каждого $i = 1, 2, \ldots, m$, которая является искомой для группы G.

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

$$G = Px_1H \cup Px_2H \cup \ldots \cup Px_tH. \tag{1.7}$$

Зададим отображение $\varphi_i : gx_ih \mapsto x_i^{-1}gx_ih,\ g \in P, h \in H$, переводящее элементы двойного смежного класса Px_iH в элементы произведения подгрупп $x_i^{-1}Px_i = P^{x_i}$ и H. Легко показать, что отображение φ_i взаимно однозначно, поэтому, используя теорему 1.42, с. 37, получаем:

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

где $p^b =\mid H \mid$. Так как $P^{x_i} \cap H$ есть подгруппа в H, то по теореме Лагранжа $\mid P^{x_i} \cap H \mid$ делит p^b и $p^b/ \mid P^{x_i} \cap H \mid$ —

целое число. Из разложения (1.7) теперь имеем:

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

Сокращая обе части равенства на p^m получаем:

$$s = \sum_{i=1}^{t} \frac{p^b}{\mid P^{x_i} \cap H \mid}. \qquad (1.8)$$

Так как s взаимно просто с p, а $p^b / \mid p^{x_i} \cap H \mid$ — целое число, являющееся степенью p, то в правой части равенства (1.8) существует слагаемое, равное единице. Пусть, например, $p^b = \mid P^{x_j} \cap H \mid$, где $1 \leq j \leq t$. Тогда $H \leq P^{x_j}$.

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

$$G = Px_1N \cup Px_2N \cup \ldots \cup Px_tN. \qquad (1.9)$$

Отображение $\varphi_i : gx_ih \mapsto x_i^{-1}gx_ih$, $g \in P$, $h \in N$, будет взаимно однозначным отображением Px_iN на $P^{x_i}N$. Теперь из разложения (1.9) имеем:

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

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

$$\rho = 1 + \sum_{i=2}^{t} \mid P^{x_i} \mid / \mid P^{x_i} \cap N \mid. \qquad (1.10)$$

Покажем, что под знаком суммы в формуле (1.10) нет слагаемых, равных 1. Допустим противное, т.е. что для некоторого $j \geq 2$ имеем равенство $\mid P^{x_j} \mid = \mid P^{x_j} \cap N \mid$. Это означает, что $P^{x_j} \leq N$ и подгруппа N содержит две подгруппы P и P^{x_j} порядка p^m. По утверждению 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 $x_j \in N$. Это возможно только при $j = 1$, противоречие. Значит, допущение неверно и в формуле (1.10) под знаком суммы все слагаемые отличны от единицы. Поскольку каждое слагаемое есть степень простого p, то из формулы (1.10) получаем сравнение $\rho \equiv 1 \pmod{p}$. По утверждению 3 все подгруппы порядка p^m в G сопряжены между собой, а по следствию 2 теоремы 1.49, с. 40, 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 ее 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.

Теорема 1.65. *Для конечной группы G и ее силовской p-подгруппы P справедливы следующие утверждения:*

1) если K — нормальная подгруппа группы 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 и K_2 — нормальные подгруппы группы 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 $p_1, p_2, \ldots, p_n$ — все простые делители порядка группы G, $p_i \neq p_j$ при $i \neq j$, и $P_1, P_2, \ldots, P_n$ — соответствующие им силовские подгруппы. Тогда $G = \langle P_1 \cup P_2 \cup \ldots \cup P_n \rangle$, а если $n = 2$, то $G = P_1P_2$.

$\square$ 1. Так как $\mid P \mid = p^m$ и p не делит $\mid G : P \mid$, то $P \cap K$ — p-группа, а из того, что $\mid PK \mid = \mid P \mid \mid K \mid / \mid P \cap K \mid$, следует $\mid PK : P \mid = \mid K : K \cap P \mid$. Из теоремы 1.39, с. 34, получаем, что $\mid G : P \mid = \mid G : PK \mid \mid PK : P \mid$ и $\mid K : K \cap P \mid$ не делится на p. Значит, $K \cap P$ — силовская p-подгруппа в K. Поскольку $\mid PK/K \mid = \mid P/P \cap K \mid$, то PK/K — p-группа, а так как число p не делит

$$\mid G : P \mid / \mid PK : P \mid = \mid G : PK \mid = \mid G/K : PK/K \mid,$$

то PK/K — силовская p-подгруппа в группе G/K.

2. Для элемента $x \in N_G(P)$ получаем:

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

т.е. $N_G(P)K/K \leq N_{G/K}(PK/K)$. Обратно, если $yK \in N_{G/K}(PK/K)$, то $P^y K = PK$. Теперь P и P^y — силовские подгруппы в PK, которые согласно следствию теоремы 1.64 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 $ab \in (K_1 \cap P)(K_2 \cap P)$, $a \in K_1 \cap P$, $b \in K_2 \cap P$, 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 $\mid M \mid_p$ означает наивысшую степень p, делящую порядок M. Согласно следствию теоремы 1.64 $\mid M \mid_p$ — порядок силовской p-подгруппы из M. Из утверждения 1 получаем

$$\mid K_i \cap P \mid = \mid K_i \mid_p, \ i = 1, 2; \quad \mid K_1K_2 \cap P \mid = \mid K_1K_2 \mid_p .$$

Поэтому $\mid (K_1 \cap P)(K_2 \cap P) \mid = \mid K_1 \mid_p \mid K_2 \mid_p / \mid K_1 \cap K_2 \mid_p = \mid K_1K_2 \mid_p = \mid K_1K_2 \cap P \mid$ и $(K_1 \cap P)(K_2 \cap P) = K_1K_2 \cap P$.

Если $ab \in (K_1 \cap K_2)P$, $a \in K_1 \cap K_2$, $b \in P$, то $ab \in K_1P \cap K_2P$ и $(K_1 \cap K_2)P \leq K_1P \cap K_2P$.

Обратно, пусть $a_1b_1 = a_2b_2 \in K_1P \cap K_2P$, где $a_1 \in K_1, a_2 \in K_2$, $b_1, b_2 \in P$. 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 $a_1c_1^{-1} = a_2c_2 \in K_1 \cap K_2$ и $a_1b_1 = a_1c_1^{-1}c_1b_1 \in (K_1 \cap K_2)P$.

Следовательно, $K_1P \cap K_2P = (K_1 \cap K_2)P$.

4. Пусть $H = \langle P_1 \cup P_2 \cup \ldots \cup P_n \rangle$. Тогда $\mid P_i \mid$ делит $\mid H \mid$ для каждого $i = 1, 2, \ldots, n$ и поэтому $\mid G \mid = \mid P_1 \mid\mid P_2 \mid \ldots \mid P_n \mid$ делит $\mid H \mid$, т.е. $H = G$. Для $n = 2$ по теореме 1.42, с. 37, имеем $\mid G \mid = \mid P_1P_2 \mid$, 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 $P \le K \triangleleft G$, то $P^g \le K^g = K$ и по теореме Силова подгруппы P и P^g сопряжены в K. Поэтому существует элемент $k \in K$ такой, что $P = P^{gk}$, откуда $gk \in N_G(P)$ и $g \in N_G(P)k^{-1} \subseteq N_G(P)K$. 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, 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 $\mid N \mid$. Тогда $N_{G/N}(PN/N) = N_G(P)N/N$.*

□ Ясно, что $N_G(P)N/N \le N_{G/N}(PN/N)$. Пусть $N_{G/N}(PN/N) = A/N$. Тогда $PN \triangleleft A$ и $A = N_G(P)N$ по лемме Фраттини.

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, а силовские 3- и 5-подгруппы — 3^2 и 5 соответственно.

Пример 1.7. Доказать, что группа порядка 15 — циклическая.

□ Пусть G — группа порядка 15. Силовская 3-подгруппа P имеет порядок 3, а силовская 5-подгруппа Q имеет порядок 5. По теореме Силова число силовских 3-подгрупп равно $1 + 3k$ для некоторого неотрицательного целого k и делит 5. Поэтому в G имеется только одна подгруппа порядка 3. Так как любые две силовские 3-подгруппы сопряжены, то $P \triangleleft G$. Аналогично число силовских 5-подгрупп равно $1 + 5t$ и делит 3, поэтому $Q \triangleleft G$.

Если x — элемент порядка 3, то $\langle x \rangle$ — подгруппа порядка 3, поэтому $\langle x \rangle = P$. Значит, в G только два элемента порядка 3: x и

x^2. Аналогично если y — элемент порядка 5, то $\langle y \rangle$ — подгруппа порядка 5, поэтому $\langle y \rangle = Q$ и в G только четыре элемента порядка 5: y, y^2, y^3 и y^4. Так как в группе четырнадцать неединичных элементов, то должны существовать элементы других порядков. По теореме Лагранжа порядок каждого элемента делит число 15, поэтому в G существует элемент порядка 15 и G — циклическая группа.

2. ГОМОМОРФИЗМЫ И ПРОИЗВЕДЕНИЯ

2.1. Гомоморфизмы групп

Пусть G и $\varGamma$ — мультипликативные группы. Отображение $\varphi : G \to \varGamma$ называется *гомоморфизмом*, если

$$\varphi(xy) = \varphi(x)\varphi(y) \tag{2.1}$$

для любых $x, y \in G$. 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 $\mathrm{Im}\varphi$. *Ядром гомоморфизма* φ называется множество $\mathrm{Ker}\varphi = \{x \in G \mid \varphi(x) = \varepsilon\}$, где ε — единичный элемент группы $\varGamma$. Другими словами, в ядре собраны все элементы группы G, переходящие при отображении φ в единичный элемент группы $\varGamma$, т.е. $\mathrm{Ker}\varphi = \varphi^{-1}(\{\varepsilon\})$.

Лемма 2.1. *Пусть $\varphi : G \to \varGamma$ — гомоморфизм. Тогда:*

1) единичный элемент e группы G переходит в единичный элемент ε группы $\varGamma$, 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 $\varGamma$, т.е. $Im\varphi \le \varGamma$;

4) ядро гомоморфизма является нормальной подгруппой группы G, т.е. $Ker\varphi \lhd G$;

5) $\varphi(g) = \varphi(h)$ для элементов $g, h \in G$ тогда и только тогда, когда $gh^{-1} \in Ker\varphi$.

□ 1. Предположим, что $\varphi(e) = \varepsilon_1 \in \varGamma$. Так как ε — единица группы $\varGamma$, то $\varepsilon_1\varepsilon = \varepsilon_1$. Применяя формулу (2.1) 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 $\varGamma$.

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 $\alpha, \beta \in \mathrm{Im}\varphi$, то существуют $a, b \in G$ такие, что $\varphi(a) = \alpha$, $\varphi(b) = \beta$. Так как G — группа, то $ab \in G$ и $a^{-1} \in G$. Отсюда $\alpha\beta = \varphi(a)\varphi(b) = \varphi(ab) \in \mathrm{Im}\varphi$ и $\alpha^{-1} = \varphi(a)^{-1} = \varphi(a^{-1}) \in \mathrm{Im}\varphi$, т.е. $\mathrm{Im}\varphi \le \varGamma$.

4. Если $a, b \in \mathrm{Ker}\varphi$, то $\varphi(a) = \varepsilon = \varphi(b)$. Поэтому $\varphi(ab) = \varphi(a)\varphi(b) = \varepsilon$, т.е. $ab \in \mathrm{Ker}\varphi$. Далее, $\varphi(a^{-1}) = \varphi(a)^{-1} = \varepsilon$, т.е. $a^{-1} \in \mathrm{Ker}\varphi$. Значит, $\mathrm{Ker}\varphi \leq G$.

Для произвольных элементов $g \in G,\ a \in \mathrm{Ker}\varphi$ имеем:

$$\varphi(g^{-1}ag) = \varphi(g)^{-1}\varphi(a)\varphi(g) = \varphi(g)^{-1}\varepsilon\varphi(g) = \varepsilon.$$

Поэтому $g^{-1}ag \in \mathrm{Ker}\varphi$ и $\mathrm{Ker}\varphi \lhd G$ по теореме 1.51, с. 42.

5. Пусть $g, h \in G$ и $\varphi(g) = \varphi(h)$. Тогда

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = \varepsilon,\ gh^{-1} \in \mathrm{Ker}\varphi.$$

Обратно, если $gh^{-1} \in \mathrm{Ker}\varphi$, то $\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = \varepsilon$ и $\varphi(g) = \varphi(h)$. ⊠

Гомоморфизм $\varphi : G \to \Gamma$ называется *мономорфизмом*, если $\mathrm{Ker}\varphi = \{\varepsilon\}$. Из леммы 2.1 следует, что гомоморфизм φ является мономорфизмом тогда и только тогда, когда φ — инъекция. Если $\mathrm{Im}\varphi = \Gamma$, то гомоморфизм $\varphi : G \to \Gamma$ называется *эпиморфизмом.* Ясно, что в этом случае φ — сюръекция. Гомоморфизм, который одновременно является мономорфизмом и эпиморфизмом, будет *изоморфизмом.*

Лемма 2.2. *Пусть $\varphi : G \to \Gamma$ — гомоморфизм. Тогда:*

1) если $H \leq G$, то $\varphi(H) \leq \Gamma$;

2) если $H \lhd G$, то $\varphi(H) \lhd Im\varphi$;

3) если подмножества T и S сопряжены в G, то $\varphi(T)$ и $\varphi(S)$ сопряжены в $Im\varphi$.

□ Доказательство всех утверждений леммы выполняется элементарной проверкой.

Теорема 2.3 (основная о гомоморфизме). *Если $\varphi : G \to \Gamma$ — гомоморфизм, то $G/Ker\varphi \simeq Im\varphi$, т.е. при гомоморфизме групп фактор-группа по ядру изоморфна образу.*

□ Поставим в соответствие элементу $aK \in G/K$ элемент $\varphi(a) \in \mathrm{Im}\varphi$, 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 $\mathrm{Im}\varphi$. 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 $\mathrm{Im}\varphi$, 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 $a^{-1}b \in \mathrm{Ker}\varphi = K$, т.е. $aK = bK$. Следовательно, f — инъекция и f — изоморфизм групп G/K и $\mathrm{Im}\varphi$.

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 $\varphi : aH \mapsto a(A\cap H)$ — изоморфизмом групп AH/H и $A/A\cap H$.*

$\square$ Произведение AH — подгруппа группы G согласно лемме 1.53, с. 43. 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 фактор-группу AH/H. По лемме 1.53, с. 43 пересечение $A \cap H$ является нормальной подгруппой в A. Поэтому можно рассматривать фактор-группу $A/A \cap H$.

Отображение $\varphi : aH \mapsto a(A \cap H)$ будет биекцией множества AH/H на $A/A\cap H$, причем $\varphi((a_1H)(a_2H)) = \varphi(a_1a_2H) = a_1a_2(A \cap H) = a_1(A \cap H)a_2(A \cap H) = \varphi(a_1H)\varphi(a_2H)$. Следовательно, φ — изоморфизм. $\boxtimes$

Теорему 1.59, с. 46, о соответствии дополняет следующая

Теорема 2.5. *Если N и H — нормальные подгруппы группы G, причем $H \leq N$, то G/N изоморфна $G/H\big/N/H$.*

$\square$ По теореме о соответствии подгруппа N/H нормальна в G/H и фактор-группа $G/H\big/N/H$ состоит из смежных классов $gH(N/H)$, где gH — элемент из группы G/H. Рассмотрим отображение $\varphi : G/H \to G/N$, определяемое равенством $\varphi(gH) = gN$. Это отображение будет эпиморфизмом. Если $gH \in \mathrm{Ker}\varphi$, то $\varphi(gH) = gN = N$ и $g \in N$, поэтому $\mathrm{Ker}\varphi = N/H$. По теореме о гомоморфизме группы $G/H\big/N/H$ и G/N изоморфны.

Приведем примеры гомоморфизмов групп. 1. Пусть G — произвольная группа, а K — её произвольная нормальная подгруппа. Отображение $\varphi : g \mapsto gK$ группы G в фактор-группу G/K будет эпиморфизмом с ядром K.

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 $\mathbb{Z}$ в G. Так как $\varphi(k+l) = a^{k+l} = a^k a^l = \varphi(k)\varphi(l)$, то φ — гомоморфизм. Образ $\mathrm{Im}\varphi = \{\varphi(k) \mid k \in \mathbb{Z}\} = \{a^k \mid k \in \mathbb{Z}\} = \langle a \rangle$ совпадает с циклической подгруппой, порожденной элементом a. Ядро $\mathrm{Ker}\varphi = \{k \mid \varphi(a) = e\} = \{a^k = e\}$ состоит из тех целых чисел k, для которых $a^k = e$. По теореме 1.21, с. 23, все эти числа кратны порядку элемента a, т.е. $\mathrm{Ker}\varphi = \mid a \mid \mathbb{Z}$. Согласно основной теореме о гомоморфизме $\mathbb{Z}/\mid a \mid \mathbb{Z} \simeq \langle a \rangle$.

3. Пусть S_n — симметрическая группа степени n, а $\mathit{\Gamma} = \{-1, 1\}$ — мультипликативная группа. Рассмотрим отображение $\mathrm{sgn} : \tau \mapsto \mathrm{sgn}\tau$. Поскольку знак произведения перестановок равен произведению знаков, то равенство (2.1) выполняется и sgn — гомоморфизм. Ядро этого гомоморфизма состоит из четных перестановок, поэтому $\mathrm{Kersgn} = A_n$ — знакопеременная группа. Так как sgn — сюръекция, то $\mathrm{Imsgn} = \mathit{\Gamma}$ и $S_n/A_n \simeq \mathit{\Gamma}$.

4. Зададим отображение $\det : A \mapsto \det A$, которое каждой невырожденной матрице $A \in GL(n, P)$, где P — поле, ставит в соответствии ее определитель. Так как определитель произведения двух матриц равен произведению определителей, то равенство (2.1) выполняется и отображение det — гомоморфизм группы $GL(n, P)$ в мультипликативную группу $P^{\#}$. Каждый элемент $a \in P^{\#}$ будет определителем матрицы

$$\begin{pmatrix} a & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$

поэтому $\mathrm{Im}\det = P^{\#}$, т.е. det — эпиморфизм. Ядро $\mathrm{Ker}\det = \{A \in GL(n, P) \mid \det A = 1\}$ состоит из матриц с единичным определителем, поэтому $\mathrm{Ker}\det = SL(n, P)$ — специальная линейная группа, а по лемме 2.1 $SL(n, P)$ нормальна в $GL(n, P)$. Согласно теореме о гомоморфизме $GL(n, P)/SL(n, P)$ изоморфна мультипликативной группе $P^{\#}$.

2.2. Автоморфизмы

Напомним, что изоморфное отображение группы на себя называется *автоморфизмом.* Два автоморфизма φ и ψ группы G считаются равными, если они одинаково действуют на элементах, т.е. если $\varphi(x) = \psi(x)$ для всех $x \in G$. Если автоморфизмы φ и ψ различны, то существует $y \in G$ такой, что $\varphi(y) \neq \psi(y)$. Совокупность $\mathrm{Aut}G$ всех автоморфизмов группы G с операцией $(\varphi\psi)(x) = \varphi(\psi(x))$ для всех $x \in G$ является группой, см. теорему 1.34, с. 31.

Приведем примеры автоморфизмов групп. 1. Пусть G — абелева группа и $\alpha : x \mapsto x^{-1}$. Тогда α — автоморфизм группы G.

2. Пусть $\mathbb{C}^{\#}$ — мультипликативная группа ненулевых комплексных чисел. Тогда отображение $a + bi \mapsto \overline{a + bi} = a - bi$ является автоморфизмом $\mathbb{C}^{\#}$.

3. 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.

Действительно, так как G абелева, то $(ab)^m = a^m b^m$ для всех $a, b \in G$. Поэтому отображение $\beta : g \mapsto g^m$ — гомоморфизм. Если $a^m = e$ для некоторого $a \in G$, то порядок a делит m по теореме 1.21, с. 23. Но $\mid a \mid$ делит n по теореме Лагранжа, а числа m и n взаимно просты. Из равенства $a^m = e$ следует, что $a = e$ и β — инъекция. Поэтому β — автоморфизм.

При автоморфизмах сохраняются многие свойства групп. Отметим простейшие из них в следующей лемме.

Лемма 2.6. *Пусть G — группа, H и K — подгруппы G, $H \leq K$, $x \in G$ и $\varphi \in AutG$. Тогда:*

1) $\mid x \mid = \mid \varphi(x) \mid$;

2) $C_G(\varphi(x)) = \varphi(C_G(x))$;

3) $\varphi(H) = \{\varphi(h) \mid h \in H\} \simeq H$;

4) $\varphi(H) \leq \varphi(K)$ и $\mid K : H \mid = \mid \varphi(K) : \varphi(H) \mid$;

5) если $H \lhd K$, то $\varphi(H) \lhd \varphi(K)$ и $K/H \simeq \varphi(K)/\varphi(H)$;

6) $N_G(\varphi(H)) = \varphi(N_G(H))$; $C_G(\varphi(H)) = \varphi(C_G(H))$.

Внутренние автоморфизмы. Пусть G — группа и $g \in G$. Зададим отображение $i_g : x \mapsto gxg^{-1}$ 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.

Автоморфизм $i_g : x \mapsto gxg^{-1}$ называется *внутренним автоморфизмом* группы G, порожденным элементом g. Совокупность всех внутренних автоморфизмов группы G обозначается через $\mathrm{Inn}G$. Таким образом,

$$\mathrm{Inn}G = \{i_g : x \mapsto gxg^{-1} \ \mid \ g, x \in G\}.$$

Теорема 2.7. *Пусть G — группа. Тогда:*

1) $\mathrm{Inn}G \lhd \mathrm{Aut}G$;

2) $\mathrm{Inn}G \simeq G/Z(G)$.

□ 1. Пусть $i_g, i_h \in \mathrm{Inn}G$, $g, h \in G$. Тогда $i_g i_h(x) = i_g(i_h(x)) = i_g(hxh^{-1}) = g(hxh^{-1})g^{-1} = (gh)x(gh)^{-1} = i_{gh}(x)$. Таким образом, $i_g i_h = i_{gh}$ и умножение определено на $\mathrm{Inn}G$. Для единичного элемента $e \in G$ внутренний автоморфизм i_e будет тождественным отображением, т.е. единичным элементом в $\mathrm{Inn}G$. Поэтому из равенства $i_g i_h = i_{gh} = i_e$ следует, что $h = g^{-1}$ и $(i_g)^{-1} = i_{g^{-1}} \in \mathrm{Inn}G$. Оба условия теоремы 1.11, с. 17, выполняются, значит, $\mathrm{Inn}G$ — подгруппа. Пусть $\varphi \in \mathrm{Aut}G$, $i_g \in \mathrm{Inn}G$. Тогда для любого $x \in G$

$$\begin{aligned}(\varphi^{-1}i_g\varphi)(x) &= (\varphi^{-1}i_g)(\varphi(x)) = \varphi^{-1}(g\varphi(x)g^{-1}) = \\ &= \varphi^{-1}(g)\varphi^{-1}(\varphi(x))\varphi^{-1}(g^{-1}) = \varphi^{-1}(g)x(\varphi^{-1}(g))^{-1} = \\ &= i_{\varphi^{-1}(g)}(x), \quad \text{т.е.} \quad \varphi^{-1}i_g\varphi = i_{\varphi^{-1}(g)} \in \mathrm{Inn}G.\end{aligned}$$

Следовательно, $\mathrm{Inn}G$ — нормальная подгруппа группы $\mathrm{Aut}G$.

2. Определим отображение $f : G \to \mathrm{Inn}G$ 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 $\mathrm{Inn}G$. Ясно, что f — сюръекция, т.е. $\mathrm{Im}f = \mathrm{Inn}G$. Ядро $Kerf = \{g \in G \mid f(g) = i_e\} = \{g \in G \mid gxg^{-1} = x$ для всех $x \in G\} = Z(G)$. Применяя основную теорему о гомоморфизме, получаем, что $G/Z(G) \simeq \mathrm{Inn}G$.

Теорема 2.8. *Пусть G — группа и H — ее подгруппа. Тогда $C_G(H) \lhd N_G(H)$ и фактор-группа $N_G(H)/C_G(H)$ 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 H. Рассмотрим отображение $f : g \mapsto i_g^0$ для всех $g \in N_G(H)$. Оно является гомоморфизмом группы $N_G(H)$ в $\mathrm{Aut}H$, ядро которого $Ker f = \{g \in N_G(H) \mid ghg^{-1} = h$ для всех $h \in H\} = C_{N_G(H)}(H) = C_G(H)$. Теперь осталось только применить основную теорему о гомоморфизме.

Характеристические подгруппы. Пусть H — подгруппа группы G и α — автоморфизм группы G. Если $\alpha(H) = H$ для всех $\alpha \in \mathrm{Aut}G$, то H называют *характеристической подгруппой группы* G и пишут: $H\ char\ G$. В каждой группе G единичная подгруппа и вся группа являются характеристическими подгруппами. Если в группе G нет других характеристических подгрупп, то она называется *характеристически простой*. Ясно, что простые группы являются характеристически простыми.

Лемма 2.9. *Каждая подгруппа конечной циклической группы характеристическая.*

□ В циклических группах подгруппа фиксированного порядка единственна, см. следствие теоремы 1.21, с. 25. Поэтому если G — циклическая группа и $H \leq G$, то из условия $\mid H \mid = \mid \alpha(H) \mid$ следует, что $\alpha(H) = H$ и $H\ char\ G$.

Лемма 2.10. *Пусть $H \leq G$. Тогда:*

1) если $H\ char\ G$, то $H \lhd G$;

2) если $H\ char\ G$, то $C_G(H)\ char\ G$;

3) если H и $K\ char\ G$, то $HK\ char\ G$ и $H \cap K\ char\ G$;

4) если $H \leq K \leq G$, $H\ char\ G$ и $K/H\ char\ G/H$, то $K\ char\ G$.

□ 1. Пусть $H\ char\ G$. 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 $H \lhd G$.

2. Пусть $H\ char\ G$ и $\alpha \in \mathrm{Aut}G$. 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 так как $\alpha(H) = H$, то $\alpha(g) \in C_G(H)$ и $C_G(H)\ char\ G$.

3–4. Достаточно выполнить простую проверку.

Лемма 2.11. *Пусть $H \le K \le G$. Тогда:*

1) если H char K char G, то H char G;

2) если H char $K \lhd G$, то $H \lhd G$.

□ 1. Для любого $\alpha \in \mathrm{Aut}G$ из условия K *char* G следует, что $\alpha(K) = K$. Ограничение $\alpha\mid_K$ автоморфизма α на K будет автоморфизмом K, а поскольку H *char* K, то $\alpha\mid_K(H) = \alpha(H) = H$ и H *char* G.

2. Так как $K \lhd G$, то $i_g(K) = K$. Ограничение i_g^0 автоморфизма i_g группы G на K будет автоморфизмом K, а т.к. H *char* K, то $i_g^0(H) = i_g(H) = H$ и $H \lhd G$. ⊠

Холловой подгруппой конечной группы называют подгруппу, порядок и индекс которой взаимно просты. Силовская 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 $M \le N$.*

□ Докажем вначале второе утверждение. Пусть $M \le G$ и порядок M делит порядок N. Так как MN — подгруппа, то ее порядок делит порядок G. Но $\mid MN \mid = \mid M \mid\mid N \mid / \mid M \cap N \mid$, поэтому $\mid MN \mid / \mid N \mid = \mid M \mid / \mid M \cap N \mid$ делит $\mid G/N \mid$. Так как $\mid M/M \cap N \mid$ делит $\mid N \mid$, а числа $\mid N \mid$ и $\mid G/N \mid$ взаимно просты, то $\mid M \mid = \mid M \cap N \mid$ и $M \le N$. Второе утверждение доказано. Если $\alpha \in \mathrm{Aut}G$, то $\alpha(N)$ — подгруппа, порядок которой равен порядку N. По доказанному имеем $\alpha(N) = N$ и N *charG*.

Следствие. *Нормальная силовская подгруппа конечной группы является характеристической.*

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 группы G является центральным тогда и только тогда, когда $g^{-1}\alpha(g) \in Z(G)$ для всех $g \in G$.*

□ Пусть α — центральный автоморфизм. Тогда $\alpha i_g = i_g\alpha$ для всех $g \in G$. Если x — произвольный элемент, 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 и $g^{-1}\alpha(g) \in Z(G)$ 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 1. *Группа с единичным центром не имеет нетождественных центральных автоморфизмов.*

Следствие 2. *Если G — группа с единичным центром, то $C_{AutG}InnG = E$.*

$\square$ Достаточно вспомнить, что множество центральных автоморфизмов группы G совпадает с $C_{\mathrm{Aut}G}\mathrm{Inn}G$, а затем применить следствие 1.

2.3. Эндоморфизмы и операторы

Гомоморфное отображение группы в себя называется *эндоморфизмом*. 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 $\mathrm{End}G$.

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 $EndG$ всех эндоморфизмов группы G с операцией $\varphi\psi(x) = \varphi(\psi(x))$ для всех $x \in G$ является полугруппой с единицей $\varepsilon : x \mapsto x$.*

$\square$ Пусть $\varphi, \psi \in \mathrm{End}G$. Так как $\varphi\psi(xy) = \varphi(\psi(xy)) = \varphi(\psi(x)\psi(y)) = \varphi(\psi(x))\varphi(\psi(y)) = (\varphi\psi)(x)(\varphi\psi)(y)$, то $\varphi\psi$ — эндоморфизм G. Поскольку умножение отображений ассоциативно, то $\mathrm{End}G$ — полугруппа. Далее, $\varphi\varepsilon(x) = \varphi(x)$ и $\varepsilon\varphi(x) = \varphi(x)$, поэтому $\varphi\varepsilon = \varepsilon\varphi = \varphi$ для всех $\varphi \in \mathrm{End}G$ и ε — единичный элемент в $\mathrm{End}G$.

Понятие гомоморфизма, введенное для групп, распространяется и на полугруппы. Отображение $\varphi : P_1 \to P_2$ мультипликативных полугрупп P_1 и P_2 называется *гомоморфизмом,* если $\varphi(xy) = \varphi(x)\varphi(y)$ для всех $x, y \in P_1$. Если гомоморфизм $\varphi : P_1 \to P_2$ 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 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 $End\langle g \rangle \simeq (\mathbb{Z}, \cdot)$.*

2. Если $\langle g \rangle$ — конечная циклическая группа порядка n, то $End\langle g \rangle \simeq (\mathbb{Z}_n, \cdot)$.

☐ По теореме 1.20, с. 22, $\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$. 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 $\varphi(g^i) = (\varphi(g))^i = g^{mi}$ и $\varphi = \varphi_m$. Таким образом, каждый эндоморфизм группы $\langle g \rangle$ имеет вид $\varphi_k : g^i \mapsto g^{ik}$, где $k \in \mathbb{Z}$, поэтому $\mathrm{End}\langle g \rangle = \{\varphi_k \mid k \in \mathbb{Z}\}$. Поскольку

$$(\varphi_s \varphi_t) g^i = \varphi_s(\varphi_t(g^i)) = \varphi_s(g^{ti}) = g^{sti} = \varphi_{st}(g^i),$$

то $\varphi_s \varphi_t = \varphi_{st}$ и отображение $\alpha : k \mapsto \varphi_k$ будет эпиморфизмом полугруппы $(\mathbb{Z}, \cdot)$ на полугруппу $\mathrm{End}\langle g \rangle$.

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 $\mathrm{End}\langle g \rangle$.

2. Пусть $\langle g \rangle$ — конечная группа порядка n. Тогда $\langle g \rangle = \{g^0 = e, g, g^2, \ldots, g^{n-1}\}$ по теореме 1.21, с. 23. Если $\varphi_s = \varphi_t$, то $\varphi_s(g) = g^s = \varphi_t(g) = g^t$, $g^{s-t} = e$ и $s - t$ делится на n (см. теорему 1.21). Поэтому отображение $\beta : \overline{k} \mapsto \varphi_k$, $\overline{k} = k + n\mathbb{Z} \in \mathbb{Z}_n$, будет изоморфизмом полугрупп $(\mathbb{Z}_n, \cdot)$ и $\mathrm{End}\langle g \rangle$.

Теорема 2.16. *1. Если $\langle g \rangle$ — бесконечная циклическая группа, то $Aut\langle g \rangle$ — группа порядка 2.*

2. Если $\langle g\rangle$ — конечная циклическая группа порядка n, то $Aut\langle g\rangle$ 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 $\varphi_1 : g \mapsto g$; $\varphi_{-1} : g \mapsto g^{-1}$ будут автоморфизмами.

2. Пусть X — множество всех обратимых элементов полугруппы $(\mathbb{Z}_n, \cdot)$. Если $\varphi \in \mathrm{Aut}\langle g\rangle$, то φ — обратимый элемент, поэтому $\varphi \in X$. Если $\psi \in X$, то ψ — биекция, поэтому $\psi \in \mathrm{Aut}\langle g\rangle$ и $\mathrm{Aut}\langle g\rangle = X$.

3. Так как $(\mathbb{Z}, \cdot)$ и $(\mathbb{Z}_n, \cdot)$ — абелевы полугруппы, то в обоих случаях группа $\mathrm{Aut}\langle g\rangle$ 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 $p-1$. Теперь из утверждения 2 получаем, что $\mathrm{Aut}\langle g\rangle \simeq (\mathbb{Z}_p^{\#}, \cdot)$.

Операторы. Пусть даны группа G, множество Ω и отображение $f : \Omega \to \mathrm{End}G$, переводящее элемент $\alpha \in \Omega$ в элемент $f(\alpha) \in \mathrm{End}G$. 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 действием на группе G, поскольку им может соответствовать один и тот же эндоморфизм.

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 также 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. $f(\alpha)|_H \in \mathrm{End}H$. Это позволяет считать Ω областью операторов любой Ω-подгруппы группы G.

Рассмотрим наиболее употребительные операторы. 1. Пусть Ω — непустое множество и отображение $f : \Omega \to \mathrm{End}G$ 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 $\mathrm{Aut}G \leq \mathrm{End}G$ и $\alpha(g) = f(\alpha)(g) = \varepsilon(g) = g$. Поэтому каждая подгруппа группы G будет Ω-допустимой.

2. 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, $f(A) \subseteq \mathrm{Inn}G \leq \mathrm{End}G$. 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.

3. Положим $A = G$. Тогда $f(G) = \mathrm{Inn}G$ — подгруппа группы $\mathrm{End}G$. Поэтому G-допустимыми подгруппами будут нормальные подгруппы и только они.

4. Если $\Omega = \mathrm{Aut}G$, то $\mathrm{Aut}G$-допустимыми будут характеристические подгруппы и только они.

Если H — Ω-подгруппа группы G и $H \lhd G$, то фактор-группа G/H становится Ω-группой, если положить $\alpha(gH) = \alpha(g)H$ для $g \in G$ и $\alpha \in \Omega$. Для теоремы 1.59, с. 46, Ω-аналогом 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 фактор-группы G/H;

2) каждая Ω-подгруппа фактор-группы 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.* Для теоремы 1.61, с. 48, Ω-аналогом является следующая

Теорема 2.18. *1. Если H — максимальная нормальная Ω-подгруппа неединичной Ω-группы G, то фактор-группа G/H является Ω-простой группой.*

2. Если H — нормальная Ω-подгруппа Ω-группы G и фактор-группа G/H Ω-простая, то H — максимальная нормальная Ω-подгруппа Ω-группы G.

Пусть G и $\varGamma$ — группы с одной областью операторов Ω. Гомоморфизм $\varphi : G \to \varGamma$ называется *Ω-гомоморфизмом*, если $\alpha(\varphi(g)) = \varphi(\alpha(g))$ для всех $g \in G$, $\alpha \in \Omega$. В следующей лемме перечислены его очевидные свойства.

Лемма 2.19. *Пусть G и $\varGamma$ — группы с одной областью операторов Ω и $\varphi : G \to \varGamma$ Ω-гомоморфизм. Тогда:*

1) ядро $Ker\varphi = \{x \in G \mid \varphi(x) = \varepsilon\}$, где ε — единица группы $\varGamma$, является нормальной Ω-подгруппой группы G;

2) образ $\varphi(H)$ любой Ω-подгруппы H из G является Ω-подгруппой группы $\varGamma$;

3) образ $Im\varphi = \varphi(G) = \{\varphi(g) \mid g \in G\}$ Ω-гомоморфизма φ является Ω-подгруппой группы $\varGamma$.

Ω-гомоморфизм $\varphi : G \to \varGamma$ называется *Ω-эпиморфизмом*, если $\mathrm{Im}\varphi = \varGamma$. При $\mathrm{Ker}\varphi = E$, говорят об Ω-*мономорфизме.* Если φ является одновременно Ω-эпиморфизмом и Ω-мономорфизмом, то его называют *Ω-изоморфизмом.* В этом случае говорят, что группы G и $\varGamma$ Ω-изоморфны и пишут $G \simeq_\Omega \varGamma$. Обратим внимание на то, что если $\varphi : G \to \varGamma$ есть Ω-мономорфизм, то $\varphi : G \to \mathrm{Im}\varphi$ Ω-изоморфизм.

Теорема 2.20. *При любом Ω-гомоморфизме $\varphi : G \to \varGamma$ группы $G/Ker\varphi$ и $Im\varphi$ Ω-изоморфны.*

$\square$ По теореме 2.3, с. 58, отображение $f : g\mathrm{Ker}\varphi \mapsto \varphi(g)$ является изоморфизмом группы $G/\mathrm{Ker}\varphi$ и группы $\mathrm{Im}\varphi$. Если $\alpha \in \Omega$, то $f(\alpha(g\mathrm{Ker}\varphi)) = f(\alpha(g)\mathrm{Ker}\varphi) = \varphi(\alpha(g)) = \alpha(\varphi(g)) = \alpha(f(g\mathrm{Ker}\varphi))$ и f — Ω-изоморфизм.

Теорема 2.21. *Если N и H — нормальные Ω-подгруппы Ω-группы G, причем $H \leq N$, то N/H — нормальная Ω-подгруппа фактор-группы G/H и имеет место Ω-изоморфизм $(G/H)/(N/H) \simeq_\Omega G/N$.*

$\square$ Из теоремы 2.17 следует, что N/H — нормальная Ω-подгруппа Ω-фактор-группы G/H. По теореме 2.5, с. 59, отображение $\varphi : G/H \to G/N$, 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 $gH \in \mathrm{Ker}\varphi$, то $\varphi(gH) = gN = N$ и $g \in N$, поэтому $\mathrm{Ker}\varphi = N/H$. По теореме 2.20 группы $G/H\big/N/H$ 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 $A/A \cap H$.*

$\square$ Ясно, что $A \cap H$ является нормальной Ω-подгруппой в A, а по теореме 2.4, с. 59, φ — изоморфизм AH/H и $A/A \cap H$. Если $\alpha \in \Omega$, то $\alpha(\varphi(aH)) = \alpha(a(A \cap H)) = (\alpha(a))(A \cap H) = \varphi(\alpha(a)H) = \varphi(\alpha(aH))$ и φ — Ω-изоморфизм.

2.4. Композиционные ряды

Цепочка подгрупп $E = A_0 < A_1 < \ldots < A_{a-1} < A_a = G$ называется *рядом* длины a неединичной группы G и обозначается через $(A_i)_{i=0,\ldots,a}$. Ряд называется *нормальным*, если $A_i \lhd G$ для всех i, и *субнормальным*, если $A_{i-1} \lhd A_i$ для всех i. Ясно, что каждый нормальный ряд будет субнормальным.

Пусть $(A_i)_{i=0,\ldots,a}$ — субнормальный ряд конечной группы G. Фактор-группы A_i/A_{i-1}, $i = 1, \ldots, a$, называются *факторами ряда*, числа $|A_i/A_{i-1}|$ — *индексами ряда*. Нормальный ряд $(A_i)_{i=0,\ldots,a}$ конечной группы G называется *главным*, если A_{i-1} является максимальной нормальной подгруппой группы G, содержащейся в A_i, $i = 1, \ldots, a$. Ясно, что в этом случае *главный фактор* A_i/A_{i-1} является минимальной нормальной подгруппой группы G/A_{i-1} для каждого $i = 1, \ldots, a$.

Субнормальный ряд $(A_i)_{i=0,\ldots,a}$ конечной группы G

называется *композиционным*, если A_{i-1} является максимальной нормальной подгруппой в A_i, $i = 1, \ldots, a$. *Композиционные факторы* A_i/A_{i-1} по теореме 1.61, с. 48, являются простыми группами.

Ряд $E = E$ считается композиционным и главным рядом единичной группы E, а число 0 — длиной этого ряда.

Пусть G — конечная группа с областью операторов Ω. Ряд $(A_i)_{i=0,\ldots,a}$, состоящий из Ω-подгрупп, называется Ω-*рядом*. Субнормальный Ω-ряд $(A_i)_{i=0,\ldots,a}$ называется Ω-*композиционным*, если A_{i-1} является максимальной нормальной Ω-допустимой подгруппой в A_i, $i = 1, \ldots, a$. Ясно, что Ω-композиционные факторы A_i/A_{i-1} по теореме 2.18, с. 69, являются Ω-простыми группами.

Приведем примеры рядов. 1. Пусть $(A_i)_{i=0,\ldots,a}$ — композиционный ряд группы G порядка $p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$. Предположим, что все композиционные факторы этого ряда абелевы. Тогда по теореме 1.38, с. 34, все композиционные факторы имеют простые порядки. Поэтому число композиционных факторов порядка p_i равно a_i, $a = a_1 + a_2 + \ldots + a_k$ и $|G| = \prod_{i=1}^{a} |A_i/A_{i-1}|$.

2. Пусть $\Omega = \langle\varepsilon\rangle$ — единичная подгруппа в $\mathrm{Aut}G$. Тогда Ω-композиционный ряд является композиционным рядом конечной группы G.

3. Если $\Omega = G$, то G-допустимые подгруппы группы G — это в точности её нормальные подгруппы. Поэтому G-композиционный ряд будет главным рядом.

4. Если $\Omega = \mathrm{Aut}G$, то $\mathrm{Aut}G$-допустимые подгруппы группы G — это в точности ее характеристические подгруппы. Поэтому $\mathrm{Aut}G$-композиционный ряд состоит из характеристических подгрупп и $\mathrm{Aut}G$-композиционные факторы являются $\mathrm{Aut}G$-простыми группами.

Пусть G — конечная Ω-группа. Будем говорить, что *два Ω-композиционных ряда* $(A_i)_{i=0,1,\ldots,a}$, $(B_i)_{i=0,1,\ldots,b}$ *группы G изоморфны*, если $a = b$ и существует биекция

$$\tau : \{A_i/A_{i-1} \mid i = 1, \ldots, a\} \to \{B_i/B_{i-1} \mid i = 1, \ldots, b\}$$

такая, что $\tau(A_i/A_{i-1}) \simeq_\Omega A_i/A_{i-1}$.

Теорема 2.23 (Жордана-Гельдера). *Любые два Ω-композиционных ряда конечной Ω-группы G изоморфны.*

□ Будем следовать схеме доказательства этой теоремы в [27]. Применим индукцию к порядку группы. Ясно, что можно считать группу G неединичной. Пусть $(A_i)_{i=0,1,\ldots,a}$ и $(B_i)_{i=0,1,\ldots,b}$ — два Ω-композиционных ряда Ω-группы G. Подгруппа $N = B_{b-1}$ является максимальной нормальной Ω-подгруппой Ω-группы G, поэтому $A_i \leq N$ или $A_iN = G$ для всех $i = 0, \ldots, a$. Положим $A_i^* = A_i \cap N$ и зафиксируем наибольшее j для которого $A_j \leq N$. Тогда $A_j^* = A_j \lhd A_{j+1}^* < A_{j+1}$. Поскольку A_{j+1}/A_j — Ω-простая группа, то $A_j^* = A_j = A_{j+1}^*$ и

$$G/N = A_{j+1}N/N \simeq_\Omega A_{j+1}/A_{j+1} \cap N = A_{j+1}/A_j. \quad (2.2)$$

Для $k \geq j+2$ имеем $A_k^* \cap A_{k-1} = A_k \cap N \cap A_{k-1} = A_{k-1}^*$ и $A_k^*/A_{k-1}^* \simeq_\Omega A_k^*A_{k-1}/A_{k-1} \lhd A_k/A_{k-1}$. Поскольку A_k/A_{k-1} — Ω-простая группа, то $A_k^*/A_{k-1}^* \simeq_\Omega A_k/A_{k-1}$ или $A_k^*/A_{k-1}^* = E$. Если $A_k^*/A_{k-1}^* = E$, то из равенств $NA_k = NA_{k-1} = G$ получаем:

$$G/N = NA_k/N \simeq_\Omega A_k/A_k \cap N = A_k/A_k^*,$$
$$G/N = NA_{k-1}/N \simeq_\Omega A_{k-1}/A_{k-1} \cap N = A_{k-1}/A_{k-1}^*,$$

что приводит к равенству $A_k = A_{k-1}$. Получили противоречие. Поэтому

$$A_k^*/A_{k-1}^* \simeq_\Omega A_k/A_{k-1} \text{ при } k \geq j+2. \quad (2.3)$$

Теперь $E = A_0^* < \ldots < A_j^* < A_{j+2}^* < \ldots < A_k^* = N$,

$$E = B_0 < \ldots < B_{b-1} = N$$

— два Ω-композиционных ряда Ω-группы N. По индукции $a-1 = b-1$ и существует биекция

$$\tau^* : \{A_i^*/A_{i-1}^* \mid i = 1, \ldots, j, j+2, \ldots, a\} \to$$
$$\to \{B_i/B_{i-1} \mid i = 1, \ldots, b-1\}$$

такая, что $\tau^*(A_i^*/A_{i-1}^*) \simeq_\Omega A_i^*/A_{i-1}^*$. Согласно формуле (2.3) $\tau^*(A_i^*/A_{i-1}^*) \simeq_\Omega A_i/A_{i-1}$, $i \neq j+1$, а из формулы (2.2) 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 $\mathrm{Aut}G$ получаем

Следствие 1. *Любые два композиционных ряда конечной группы G изоморфны.*

В случае, когда $\Omega = G$ получаем

Следствие 2. *Любые два главных ряда конечной группы G изоморфны.*

Лемма 2.24. *Пусть $H, K \lhd G$ и $K \leq H$. Тогда централизатор*

$$C_G(H/K) = \langle g \in G \mid g^{-1}h^{-1}gh \in K,\ h \in H \rangle$$

является нормальной в G подгруппой и фактор-группа $G/C_G(H/K)$ изоморфна подгруппе группы $Aut(H/K)$.

□ Для каждого $g \in G$ зададим отображение $\gamma_g : Kh \mapsto Kghg^{-1}$. Если $Kghg^{-1} = Kgfg^{-1}$ для некоторых h и $f \in H$, то $gh(gf)^{-1} \in K$, а так как $K \lhd G$, 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 $\gamma_g \in \mathrm{Aut}(H/K)$. Рассмотрим отображение $\delta : G \to \mathrm{Aut}(H/K)$, 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 $\mathrm{Aut}(H/K)$ с ядром

$$\mathrm{Ker}\delta = \{g \in G \mid \gamma_g : Kh \mapsto Kghg^{-1} = Kh\} =$$

$$= \{g \in G \mid ghg^{-1}h^{-1} \in K\} = C_G(H/K).$$

По основной теореме о гомоморфизме фактор-группа $G/C_G(H/K)$ изоморфна подгруппе из $\mathrm{Aut}(H/K)$. ⊠

Введем обозначение $\mathrm{Aut}_G(H/K) = \{\gamma_g \mid g \in G\}$, где $\gamma_g : Kh \mapsto Kghg^{-1}$. Тогда $\mathrm{Aut}_G(H/K) = \mathrm{Im}\delta$ и лемма 2.24 утверждает, что $G/C_G(H/K) \simeq \mathrm{Aut}_G(H/K)$.

Если $K \lhd G$, $H \lhd G$, $K \leq H$ 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 $|H/K|$ — 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 $C_G(H/K) \lhd G$ и $G/C_G(H/K) \simeq Aut_G(H/K)$.*

2. Если H/K — главный фактор порядка p конечной группы G, то фактор-группа $G/C_G(H/K)$ — циклическая порядка, делящего $p-1$.

□ 1. Доказательство следует из леммы 2.24.

2. По теореме 2.16, с. 66, группа автоморфизмов группы простого порядка p является циклической порядка $p-1$. Поэтому, если H/K — p-главный фактор группы G порядка p, то фактор-группа $G/C_G(H/K)$ — циклическая порядка, делящего $p-1$.

2.5. Прямые произведения

Пусть G — группа, A, 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 $A \cap B = E$. Запись $G = A \times B$ означает, что группа G является прямым произведением своих подгрупп A, B.

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 свойства 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 $a = a_1$, $b = b_1$.

2. Рассмотрим произведение $g = a^{-1}b^{-1}ab$. Поскольку $A \lhd G$, то $b^{-1}ab \in A$ и $g \in A$. Так как $B \lhd G$, 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 $ab = ba$.

Пусть выполняются свойства 1 и 2. Из свойства 1 следует, что $G = AB$. Элемент $d \in A \cap B$ можно записать в виде $d = ed = de$, где $e, d \in A \cap B$. Из однозначности представления элементов следует, что $d = e$, т.е. $A \cap B = E$. Из свойства 2 получаем, что A и B — нормальные подгруппы. Итак, все условия определения прямого произведения выполняются, поэтому $G = A \times B$. ⊠

Теорема 2.25 позволяет дать иное определение прямого произведения, эквивалентное сформулированному выше. Группа G является *прямым произведением подгрупп* A и B, если каждый элемент $g \in G$ единственным образом представим в виде $g = ab$, где $a \in A; b \in B$, и каждый элемент подгруппы A перестановочен с каждым элементом подгруппы B.

Определение прямого произведения дано для двух подгрупп. Для большего числа сомножителей определение формулируется так. Группа G является *прямым произведением подгрупп* $A_1, A_2, \ldots, A_n$, если выполняются следующие требования: $G = A_1 A_2 \ldots A_n$, $A_i \cap A_1 \ldots A_{i-1} A_{i+1} \ldots A_n = E, A_i \lhd G$, $i = 1, \ldots, n$. В этом случае пишут: $G = A_1 \times A_2 \times \ldots \times A_n = \times_{i=1}^{n} A_i$.

Данное определение можно заменить следующим, эквивалентным ему. Группа G является *прямым произведением подгрупп* $A_1, A_2, \ldots, A_n$, если каждый элемент $g \in G$ единственным образом представим в виде $g = a_1 a_2 \ldots a_n$, где $a_i \in A_i$, $i = 1, 2, \ldots, n$, и элементы из любых двух подгрупп A_i и A_j, $i \neq j$, перестановочны между собой.

Перечислим свойства прямых произведений. Утверждения приводимой ниже леммы непосредственно следует из определений прямых произведений.

Лемма 2.26. *1. Если* $G = A \times B$, $A = A_1 \times \ldots \times A_k$, $B = A_{k+1} \times \ldots \times A_n$, *то* $G = A \times \ldots \times A_k \times A_{k+1} \times \ldots \times A_n$.

2. Если $G = A_1 \times \ldots \times A_n$, *то* $G = A \times B$, *где* $A = A_1 \times \ldots \times A_l, B = A_{l+1} \times \ldots \times A_n$ *для* $l = 1, 2, \ldots, n-1$.

Лемма 2.27. *1. Если* $G = A \times B$, $A_1 \leq A$, $B_1 \leq B$, *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 $C_G(X) = C_A(X) \times B$, $N_G(X) = N_A(X) \times B$.

4. Если $G = A \times B$ и $A_1 \lhd A$, то $A_1 \lhd G$.

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_1B_1 — подгруппа группы G согласно теореме 1.41, с. 36. Ясно, что $A_1 \cap B_1 \leq A \cap B = E$. Кроме того, подгруппы A_1 и B_1 нормальны в A_1B_1, следовательно, $A_1B_1 = A_1 \times B_1$.

2. На основании тождества Дедекинда имеем, что $H = A(H \cap B)$. Остается применить свойство 1.

3. Согласно теореме 2.25 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 свойству 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 $A_1 \lhd A$, то $N_G(A_1) \geq A$ и $A_1 \lhd G$ по свойству 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 из G однозначно представим в виде $ab, a \in A, b \in B$. Следовательно, $\varphi : ab \mapsto b$ будет отображением группы G в группу B. Так как

$$\varphi(a_1b_1a_2b_2) = \varphi(a_1a_2b_1b_2) = b_1b_2 = \varphi(a_1b_1)\varphi(a_2b_2),$$

то φ — гомоморфизм. Ясно, что φ — сюръекция, поэтому $\mathrm{Im}\varphi = B$. Если $ab \in \mathrm{Ker}\varphi$, то $e = \varphi(ab) = b$ и $\mathrm{Ker}\varphi = A$. Согласно основной теореме о гомоморфизме $G/A \simeq B$.

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. 59,) отображение $\alpha_i : b_i \mapsto b_iA, \quad b_i \in B_i, \ i = 1,2$, является изоморфизмом B_i на 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 подгруппы B_1 и B_2 централизуют 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 согласно теореме 2.13, с. 64. Но действие f на B_1 совпадает с изоморфизмом $\alpha : B_1 \to B_2$, поэтому $f(B_1) = B_2$. ⊠

С учетом следствия теоремы 2.13, с. 64 получаем

Следствие 1. *Если $G = A\times B_1 = A\times B_2$ и $Z(G) = E$, то $B_1 = B_2$.*

Следствие 2. *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 $A\cap C = B\cap C = E$. Теперь $CA/A \simeq C$ и CA/A изоморфна нормальной подгруппе простой группы $G/A \simeq B$. Поэтому, $C \simeq B$ и $G = A \times C$. Применяя следствие 1 теоремы 2.29, получаем, что $C = B$.

Теорема 2.30. *Пусть $G = \times_{i=1}^{n} G_i$, G_i — неабелева простая группа для всех i и $E \neq N \lhd G$. Тогда существует подмножество $J \subseteq \{1,\dots,n\}$ такое, что $N = \times_{j\in J} G_j$.*

□ Применим индукцию по n. Предположим, что $N \cap G_i = E$ для всех i. Тогда $NG_i = N\times G_i$ и $N \leq Z(G)$ на основании теоремы 2.25. По лемме 2.27 $Z(G) = \times_{i=1}^{n} Z(G_i)$, а поскольку подгруппы G_i простые неабелевы, то $Z(G) = E$ и $N = E$, т.е. получили противоречие. Следовательно, без ущерба для доказательства можно считать, что $N \cap G_1 \neq E$. Так как $N \cap G_1 \lhd G_1$, то $G_1 \leq N$ и по лемме 2.27 $N = G_1 \times (N \cap \times_{i=2}^{n} G_i)$. Применим индукцию к группе $\times_{i=2}^{n} G_i$ и ее нормальной подгруппе $K = N \cap \times_{i=2}^{n} G_i$. По индукции существует подмножество $J_1 \subseteq \{2, \ldots, n\}$ такое, что $K = \times_{j \in J_1} G_j$. Теперь $N = G_1 \times K = \times_{j \in J} G_j$, где $J = J_1 \cup \{1\}$.

Внешнее прямое произведение. Пусть G_1 и G_2 — 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 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.*

В группе $G = G_1 \times G_2$ имеются две подгруппы

$$G_1' = \{(g_1, e_2) \mid g_1 \in G_1\},\ G_2' = \{(e_1, g_2) \mid g_2 \in G_2\},$$

причем G_1' изоморфна G_1, а G_2' изоморфна G_2. Кроме того, $G_1' \lhd G$, $G_2' \lhd G$, $G_1' \cap G_2' = E$ 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 $Aut(G_1 \times G_2) = AutG_1 \times AutG_2$.*

□ Пусть $f \in Aut(G_1 \times G_2)$. Так как по лемме 2.12, с. 64, G_1 и G_2 — характеристические подгруппы группы $G_1 \times G_2$, 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 $Aut(G_1 \times G_2)$ во внешнее прямое произведение $AutG_1 \times AutG_2$ будет мономорфизмом.

Обратно, каждый элемент $(\varphi_1, \varphi_2) \in AutG_1 \times AutG_2$ является образом при отображении α следующего автоморфизма группы $G : (g_1, g_2) \mapsto (\varphi_1(g_1), \varphi_2(g_2))$. Поэтому, $Aut(G_1 \times G_2) = AutG_1 \times AutG_2$.

Теорема 2.32. *Пусть группа $G = A \times B$ является прямым произведением своих подгрупп A и B, и пусть $A_1 \lhd A$, $B_1 \lhd B$. Тогда $A_1 B_1 = A_1 \times B_1 \lhd G$ 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 $ab \in \mathrm{Ker}\varphi$, то $e = \varphi(ab) = (aA_1, bB_1)$ и $a \in A_1$, $b \in B_1$. Таким образом, $\mathrm{Ker}\varphi = A_1B_1 = A_1 \times B_1$. Теперь остается применить основную теорему о гомоморфизме.

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 $g = a_1a_2,\ a_1 \in A_1,\ a_2 \in A_2$. Поэтому отображение $\varphi_i : g \mapsto a_i$ с учетом теоремы 2.25 будет эпиморфизмом G на A_i. Эпиморфизм $\varphi_i : G \to A_i$ 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 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 (Ремака). *Если N_1 и N_2 — нормальные подгруппы группы G, то фактор-группа $G/(N_1 \cap N_2)$ 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, так как $\varphi(gh) = (ghN_1, ghN_2) = (gN_1, gN_2)(hN_1, hN_2) =$

$\varphi(g)\varphi(h)$, $g,h\in G$. Ясно, что $Im\varphi=\{(gN_1,gN_2)\mid g\in G\}$ и $Im\varphi$ есть подгруппа группы $(G/N_1)\times(G/N_2)$, которая является подпрямым произведением. Найдем ядро отображения φ. По определению ядра $\mathrm{Ker}\varphi=\{g\in G\mid\varphi(g)=e\}$, 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, $\mathrm{Ker}\varphi=N_1\cap N_2$. По основной теореме о гомоморфизме $G/(N_1\cap N_2)\simeq Im\varphi\le(G/N_1)\times(G/N_2)$.

Разложение циклической группы. Группа, которая не может быть представлена в виде прямого произведения двух различных собственных подгрупп, называется *неразложимой*. Очевидно, что неразложимыми будут все простые группы.

Симметрическая группа S_3 степени 3 содержит единственную нетривиальную нормальную подгруппу $\langle(123)\rangle$, поэтому S_3 неразложима.

Теорема 2.34. *Множество всех подгрупп циклической примарной группы с бинарным отношением $\le$ является линейно упорядоченным множеством. В частности, циклическая примарная группа неразложима.*

□ Пусть $\langle g\rangle$ — циклическая группа порядка p^n, где p — простое число. По теореме 1.24, с. 25, все ее 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 $m=0,1,\ldots,n$, и $\langle g^{p^0}\rangle=\langle g\rangle$, $\langle g^p\rangle$, $\langle g^{p^2}\rangle$, $\ldots$, $\langle g^{p^{n-1}}\rangle$, $\langle g^{p^n}\rangle=E$ — 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 $k\le l$. Тогда $l-k\ge 0$ и $(g^{p^k})^{p^{l-k}}=g^{p^l}$, т.е. элемент g^{p^l} является степенью элемента g^{p^k} и $\langle g^{p^l}\rangle\le\langle g^{p^k}\rangle$. 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 $\le$ является линейно упорядоченным множеством. В частности, в циклической примарной группе нет двух неединичных подгрупп, имеющих единичное пересечение.

Теорема 2.35. *Если $\langle g \rangle$ — 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 $g^k \in \langle g^m \rangle \cap \langle g^n \rangle$, т.е. $g^k = g^{mk_1} = g^{nk_2}$. Тогда $g^{mk_1 - nk_2} = e$ и mn делит $mk_1 - nk_2$ по теореме 1.21, с. 23. 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 $\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle$, где $\langle g_i \rangle = \langle g^{n/p_i^{\alpha_i}} \rangle$ — циклическая подгруппа порядка $p_i^{\alpha_i}$, $i = 1, 2, \dots, k$.*

□ Воспользуемся индукцией по k. На основании теоремы 2.35 имеем $\langle g \rangle = \langle g^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \rangle \times \langle g^{p_1^{\alpha_1}} \rangle$. Подгруппа $\langle g^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} \rangle$ 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 $\langle g^{p_1^{\alpha_1}} \rangle = \langle g_2 \rangle \times \dots \times \langle g_k \rangle$, где $g_i = g^{p_1^{\alpha_1}(n_1/p_i^{\alpha_i})} = g^{n/p_i^{\alpha_i}}$ — элемент порядка $p_i^{\alpha_i}$, $i = 2, 3, \dots, k$. Теперь согласно лемме 2.26 получаем, что $\langle g \rangle = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_k \rangle$, где $g_1 = g^{p_2^{\alpha_2} \cdots p_k^{\alpha_k}} = g^{n/p_1^{\alpha_1}}$.

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. На основании теоремы 2.34 подгруппы $\langle g^{25} \rangle$ и $\langle g^4 \rangle$ неразложимы.

2.6. Минимальные нормальные подгруппы

Минимальной нормальной подгруппой группы G называют такую нормальную подгруппу N, 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. 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 $\mathrm{Soc}G$. Таким образом, $\mathrm{Soc}G = \prod_{N \cdot\triangleleft G} N$.

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 $N \not\subseteq K$, то $NK/K \cdot\triangleleft\, G/K$.

□ 1. Пусть $N \not\subseteq K$. Тогда $N \cap K \triangleleft G$ по лемме 1.53, с. 43, 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 $N \not\subseteq K$, 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 свойства 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 $N_1, N_2, \ldots, N_k \in \mathcal{M}$ такие, что $KM = K \times N_1 \times N_2 \times \ldots \times N_k$;

2) существуют подгруппы $N_1, N_2, \ldots, N_m \in \mathcal{M}$ такие, что $M = N_1 \times N_2 \times \ldots \times N_m$;

3) если $\mathcal{M}$ — множество всех минимальных нормальных подгрупп, то существуют подгруппы $N_1, N_2, \ldots, N_s \in \mathcal{M}$ такие, что $SocG = N_1 \times N_2 \times \ldots \times N_s$.

□ 1. Если $N \in \mathcal{M}$ и $N \not\subseteq K$, то $NK = N \times K$ по лемме 2.36. Пусть $\{N_1, \ldots, N_k\}$ — подмножество из $\mathcal{M}$ с наибольшим k, для которого

$$K(\prod_{i=1}^{k} N_i) = K \times N_1 \times \ldots \times N_k.$$

Обозначим через $X = K \times N_1 \times \ldots \times N_k$. Ясно, что $K \leq X \leq KM$. Если $X \neq KM$, то существует подгруппа $N \in \mathcal{M}$ такая, что $N \not\subseteq X$. Но тогда по лемме 2.36 $XN = X \times N$ и $XN = K \times N_1 \times \ldots \times N_k \times N$, что противоречит максимальности k. Поэтому допущение неверно и $X = KM$.

2. Утверждение следует из утверждения 1 при $K = E$.

3. Если $\mathcal{M}$ — множество всех минимальных нормальных подгрупп, то подгруппа $M = \prod_{N \in \mathcal{M}} N$ совпадает с цоколем группы G и остается только применить утверждение 2.

Теорема 2.38. *1. В каждой группе минимальная нормальная подгруппа характеристически проста.*

2. Характеристически простая группа является прямым произведением изоморфных простых групп.

□ 1. Пусть $N \cdot\!\lhd G$ и $KcharN$. По лемме 2.11, с. 64, подгруппа $K \lhd G$. Из минимальности N следует, что $K = E$ или $K = N$. Поэтому N характеристически проста.

2. Пусть G — характеристически простая группа и $N \cdot\!\lhd G$. Ясно, что $\alpha(N)$ — минимальная нормальная подгруппа группы G для любого $\alpha \in \mathrm{Aut}G$. Пусть $\mathcal{M} = \{\alpha(N) \mid \alpha \in \mathrm{Aut}G\}$ и $M = \prod_{K \in \mathcal{M}} K$. Так как

$$\beta(M) = \beta(\prod_{K \in \mathcal{M}} K) = \prod_{K \in \mathcal{M}} \beta(K) = M$$

для любого $\beta \in \mathrm{Aut}G$, то M — характеристическая подгруппа, поэтому $M = G$. По лемме 2.37 получаем, что $G = N_1 \times N_2 \times \ldots \times N_m$ для $\{N_1, N_2 \ldots, N_m\} \subseteq \mathcal{M}$. Итак, группа G является прямым произведением изоморфных подгрупп $N_1, \ldots, N_m$. По свойствам прямых произведений каждая нормальная в N_1 подгруппа будет нормальной подгруппой группы G, поэтому N_1 — простая подгруппа.

Элементарной абелевой p-группой называют группу, являющуюся прямым произведением своих подгрупп порядка p.

Теорема 2.39. *Пусть $N \cdot \lhd G$ и $K \cdot \lhd N$. Тогда K — простая подгруппа и существуют элементы $g_1, \ldots, g_m \in G$ такие, что $N = K^{g_1} \times \ldots \times K^{g_m}$. Кроме того:*

1) если N абелева, то $\mid K \mid= p$ для некоторого простого p и N — элементарная абелева p-группа;

2) если N неабелева, то каждая минимальная нормальная в N подгруппа принадлежит множеству $\{K^{g_1}, \ldots, K^{g_m}\}$.

$\square$ 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 $g_1, \ldots, g_m \in G$ такие, что $N = K^{g_1} \times \ldots \times K^{g_m}$. Из леммы 2.27 следует, что подгруппа K простая.

1. Пусть N абелева. По теореме 1.54, с. 43, K имеет простой порядок. Пусть $\mid K \mid= p$. Тогда N — элементарная абелева p-группа порядка p^m.

2. Пусть N неабелева. По теореме 2.30, с. 77, каждая минимальная нормальная в N подгруппа принадлежит множеству $\{K^{g_1}, \ldots, K^{g_m}\}$.

Следствие. *Минимальная нормальная подгруппа группы либо элементарная абелева p-группа для некоторого простого p, либо является прямым произведением изоморфных простых неабелевых групп.*

Лемма 2.40. *Пусть $N \cdot \lhd G$, $N \leq H \lhd G$. Если $K \cdot \lhd H$, $K \leq N$, то существуют элементы $g_1, \ldots, g_n \in G$ такие, что $N = K^{g_1} \times \ldots \times K^{g_n}$.*

$\square$ 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 2.37

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 $U = U_0 \lhd U_1 \lhd \dots \lhd U_{s-1} \lhd U_s = G$. Запись $U \lhd\lhd G$ означает, что U — субнормальная подгруппа группы G. Очевидно, что каждая субнормальная подгруппа является членом некоторого субнормального ряда группы G.

Лемма 2.41. *Пусть $U \lhd \lhd G$. Тогда:*

1) если $T \lhd \lhd U$, то $T \lhd \lhd G$;

2) если $V \leq G$, то $V \cap U \lhd \lhd V$;

3) если $V \lhd \lhd G$, то $U \cap V \lhd \lhd G$;

4) если $N \lhd G$, то $UN/N \lhd \lhd G/N$.

□ 1. Это свойство очевидно.

2. Пусть $U = U_0 \lhd U_1 \lhd \dots \lhd U_{s-1} \lhd U_s = G$. Так как $U_i \lhd U_{i+1}$, то $(V \cap U_{i+1}) \cap U_i = V \cap U_i \lhd V \cap U_{i+1}$. Поэтому $U \cap V = U_0 \cap V \lhd U_1 \cap V \lhd \dots \lhd U_{s-1} \cap V \lhd U_s \cap V = V$ и $U \cap V \lhd \lhd V$.

3. По свойству 2 $U \cap V \lhd \lhd V$, а поскольку $V \lhd \lhd G$, то $U \cap V \lhd \lhd G$.

4. Так как $UN/N = U_0N/N \lhd U_1N/N \lhd \dots \lhd U_{s-1}N/N \lhd U_sN/N = G/N$, то $UN/N \lhd \lhd G/N$.

Лемма 2.42. *Если $U \lhd \lhd G$, то $SocG \leq N_G(U)$.*

□ Пусть $U = U_0 \lhd U_1 \lhd \dots \lhd U_{n-1} \lhd U_n = G$. Воспользуемся индукцией по n. Если $n = 1$, то $U \lhd G$ и $\mathrm{Soc}G \leq N_G(U) = G$. По индукции $\mathrm{Soc}U_{n-1} \leq N_{U_{n-1}}(U) \leq N_G(U)$. Пусть N — произвольная минимальная нормальная подгруппа группы G. Если $N \leq U_{n-1}$, то $N \leq \mathrm{Soc}U_{n-1}$ по лемме 2.40 и $N \leq N_G(U)$. Если $N \nleq U_{n-1}$, то $NU_{n-1} = N \times U_{n-1}$ по лемме 2.36 и $N \leq C_G(U) \leq N_G(U)$. Таким образом, в любом случае $N \leq N_G(U)$ и $\mathrm{Soc}G \leq N_G(U)$ по определению цоколя.

Теорема 2.43. *Если $\{U_i \mid i \in I\}$ — некоторое множество субнормальных подгрупп группы G, то $U = \langle U_i \mid i \in I \rangle \lhd \lhd G$.*

□ Воспользуемся индукцией по порядку G. Пусть $N \cdot\lhd G$. Тогда $U_iN/N \lhd \lhd G/N$ на основании леммы 2.41

и по индукции $UN/N \lhd \lhd G/N$. Согласно лемме 2.42 $N \subseteq \bigcap_{i\in I} N_G(U_i)$, поэтому $U \lhd UN \lhd \lhd G$ и $U \lhd \lhd G$.

Из леммы 2.41 и теоремы 2.43 получаем

Следствие. *Совокупность всех субнормальных подгрупп группы G образует решетку.*

Лемма 2.44. *Пусть $G = \times_{i=1}^{m} G_i$, G_i — неабелева простая группа для всех i и $E \neq N \lhd \lhd G$. Тогда существует подмножество $J \subseteq \{1, \ldots, m\}$ такое, что $N = \times_{j\in J} G_j$.*

$\square$ Пусть $N = N_0 \lhd N_1 \lhd \ldots \lhd N_{n-1} \lhd N_n = G$. Воспользуемся индукцией по n. Согласно теореме 2.30, с. 77, существует подмножество $J_1 \subseteq \{1, \ldots, m\}$ такое, что $N_{n-1} = \times_{j\in J_1} G_j$. По индукции найдется подмножество $J \subseteq J_1$ такое, что $N = \times_{j\in J} G_j$.

Теорема 2.45. *Пусть $H \lhd\lhd G$, $K \lhd\lhd G$ и $H \cap K = E$. Если H — неабелева простая подгруппа, то $\langle H \cup K\rangle = H \times K$.*

$\square$ Пусть $U = \langle H \cup K\rangle$ и

$$H = H_0 \lhd H_1 \lhd \ldots \lhd H_{n-1} \lhd H_n = U,$$
$$K = K_0 \lhd K_1 \lhd \ldots \lhd K_{m-1} \lhd K_m = U.$$

Воспользуемся индукцией по n. Если $n = 1$, то $H \lhd U$ и $U = [H]K$. Если $K \lhd U$, 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 $K_1 \lhd \lhd U$, то $E \neq K_1 \cap H \lhd \lhd H$. 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 $H_{n-1} \lhd U$, 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 $V = H \times H^{k_1} \times \ldots \times H^{k_t}$, $k_1, ..., k_t \in K$, с наибольшим номером t. Ясно, что $V \lhd \lhd H_{n-1}$. 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. Получили противоречие с выбором числа 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 2.44 $V \cap K = \times_{i\in I} H^{k_i}$ 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 $K \lhd U$, 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 2.44 существует множество J такое, что $V \cap K_1 = \times_{j \in J} H^{k_j}$. Так как $V \cap K_1 \lhd K_1$, 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 $H \lhd\lhd G$. Тогда $H^G \cdot\lhd G$ и существуют элементы $g_1, \ldots, g_n \in G$ такие, что $H^G = \times_{i=1}^{n} H^{g_i}$.*

□ Если $H \lhd G$, то утверждение теоремы очевидно. Пусть H не является нормальной подгруппой группы G. Тогда существует элемент $g \in G$ такой, что $H \neq H^g$. По теореме 2.45 получаем, что $\langle H \cup H^g \rangle = H \times H^g$. Пусть $V = H^{g_1} \times H^{g_2} \times \ldots \times H^{g_t}$ — прямое произведение с наибольшим номером t. Если $H^x \not\subseteq V$ для некоторого $x \in G$, то $V \cap H^x \lhd\lhd H^x$, 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 2.45. Получили противоречие с выбором t. Поэтому $H^x \subseteq V$ для всех $x \in G$ и $V = H^G \lhd G$. Предположим, что $V_1 \cdot\lhd G$, $V_1 \leq V$. Тогда по лемме 2.44 $V_1 = \times_{i \in I} H^{g_i}$ и $V = H^G \subseteq V_1$. Поэтому $V = V_1 \cdot\lhd G$.

Следствие. *Если H — неабелева простая подгруппа группы G и $H \lhd\lhd G$, то $H \leq SocG$.*

2.7. Полупрямые произведения

Теорема 2.47. *Пусть K и H — группы и ψ — гомоморфизм группы K в $AutH$. Тогда существует группа G, обладающая следующими свойствами:*

1) G содержит подгруппы $H^* \simeq H$ и $K^* \simeq K$;

2) $G = H^*K^*$;

3) $H^* \cap K^* = E$;

4) $H^* \lhd G$.

□ Условимся обозначать образ элемента $h \in H$ при автоморфизме $\psi(k) \in \mathrm{Aut}H$, $k \in K$, через $[\psi(k)h]$. Проверим, что множество $G = \{(k,h) \mid k \in K,\ h \in H\}$ с операцией

$$(k_1,h_1)(k_2,h_2) = (k_1k_2, [\psi(k_2^{-1})h_1]h_2) \tag{2.4}$$

является искомой группой.

Так как $[\psi(k_2^{-1})h_1] \in H$, то операция (2.4) определена на G. Проверим ее ассоциативность:

$$\big((k_1,h_1)(k_2,h_2)\big)(k_3,h_3) = \big(k_1k_2, [\psi(k_2^{-1})h_1]h_2\big)(k_3,h_3) =$$
$$= \big(k_1k_2k_3, \big[\psi(k_3^{-1})([\psi(k_2^{-1})h_1]h_2)\big]h_3\big) =$$
$$= \big(k_1k_2k_3, \big[\big(\psi(k_2k_3)^{-1}\big)h_1\big]\big[\psi(k_3^{-1})h_2\big]h_3\big),$$
$$(k_1,h_1)\big((k_2,h_2)(k_3,h_3)\big) = (k_1,h_1)\big(k_2k_3, [\psi(k_3^{-1})h_2]h_3\big) =$$
$$= \big(k_1k_2k_3, \big[\psi((k_2k_3)^{-1})h_1\big]\big[\psi(k_3^{-1})h_2\big]h_3\big).$$

Следовательно, операция (2.4) ассоциативна. Пусть e_K — единичный элемент группы K, а e_H — единичный элемент группы H. Так как

$$(k_1,h_1)(e_K,e_H) = \big(k_1e_K, \big[\psi(e_K^{-1})h_1\big]e_H\big) = (k_1,h_1),$$
$$(e_K,e_H)(k_1,h_1) = \big(e_Kk_1, \big[\psi(k_1^{-1})e_H\big]h_1\big) = (k_1,h_1),$$

то (e_K,e_H) — единичный элемент G.

Покажем, что $(k,h)^{-1} = \big(k^{-1}, [\psi(k)h^{-1}]\big)$:

$$(k,h)\big(k^{-1}, [\psi(k)h^{-1}]\big) = \big(kk^{-1}, [\psi(k)h][\psi(k)h^{-1}]\big) =$$
$$= \big(e_K, [\psi(k)(hh^{-1})]\big) = (e_K,e_H),$$
$$\big(k^{-1}, [\psi(k)h^{-1}]\big)(k,h) = (k^{-1}k, \big[\psi(k^{-1})[\psi(k)h^{-1}]\big]h\big) =$$
$$= \big(e_K, [\psi(k^{-1})\psi(k)(h^{-1})]h\big) = (e_K,e_H).$$

Итак, G — группа. Рассмотрим два множества: $K^* = \{(k,e_H) \mid k \in K\}$, $H^* = \{(e_K,h) \mid h \in H\}$. Так как

$$(k_1,e_H)(k_2,e_H) = \big(k_1k_2, [\psi(k_2^{-1})e_H]e_H\big) = (k_1k_2,e_H) \in K^*,$$
$$(e_K,h_1)(e_K,h_2) = \big(e_Ke_K, [\psi(e_K^{-1})h_1]h_2\big) = (e_K,h_1h_2) \in H^*,$$

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 $(k, e_H)^{-1}(e_K, h)(k, e_H) =$

$$= (k^{-1}, e_H)(e_K, h)(k, e_H) = \big(k^{-1}, [\psi(e_K^{-1})e_H]h\big)(k, e_H) =$$

$$= \big(k^{-1}, h\big)\big(k, eH\big)\big(k^{-1}k, [\psi(k^{-1})h]e_H\big) = \big(e_K, [\psi(k^{-1})h]\big) \in$$

$\in H^*$, то $H^* \triangleleft G$. ⊠

Построенная в теореме 2.47 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 $\psi : K \to AutH$ 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 (2.4) принимает вид: $(k_1, h_1)(k_2, h_2) = (k_1k_2, h_1h_2)$, $\quad [\psi(k_2^{-1})h_1]h_2 = h_1h_2$, 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 формулы (2.4) следует, что $(k_1, h_1)(k_2, h_2) = (k_1k_2, h_1h_2)$ и произведение $G = K_\psi[H]$ будет прямым.

Пример 2.1. Построить полупрямое произведение двух циклических групп.

□ Пусть $K = \langle k \rangle, \mid K \mid= m$, $H = \langle h \rangle$, $\mid H \mid= n$. Выберем натуральное r, для которого $r^m \equiv 1 \ (mod\ n)$ и $r^l \not\equiv 1 \ (mod\ n)$ при $0 < l < m$. Для каждого $i = 1, 2, \ldots, m$ зададим отображение $\varphi_i : h^t \mapsto h^{tr^i}$, $t = 1, \ldots, n$. Так как

$$\varphi(h^{t_1}h^{t_2}) = \varphi_i(h^{t_1+t_2}) = h^{t_1r^i}h^{t_2r^i} = \varphi_i(h^{t_1})\varphi_i(h^{t_2}),$$

то φ_i — эндоморфизм H. Поскольку $\mathrm{Ker}\varphi_i = \{h^t \mid h^{tr^i} = e\} = \{h^t \mid n$ делит $tr^i\} = \{h^t \mid n$ делит $t\} = \{e\}$, то φ_i — автоморфизм H. Заметим, что $(\varphi_i\varphi_j)(h^t) = \varphi_i(\varphi_j(h^t)) =$

$$= \varphi_i(h^{tr^j}) = h^{tr^jr^i} = h^{tr^{i+j}} = \varphi_{i+j}(h^t),\ \varphi_i\varphi_j = \varphi_{i+j}.$$

Здесь сложение $i+j$ происходит по модулю n. Отображение $\psi : k^i \mapsto \varphi_i$ будет гомоморфизмом группы K в группу $\mathrm{Aut}H$. По теореме 2.47 существует группа G, являющаяся полупрямым произведением групп K и H относительно ψ, т.е. $G = K_\psi[H]$. ⊠

Положим в предыдущем примере $m = 2$. Тогда $r = n-1, \varphi_1 : h^t \mapsto h^{(n-1)t} = h^{-t}, \varphi_2 : h^t \mapsto h^{t(n-1)^2} = h^t, \varphi_2$ — тождественный автоморфизм и $G = \langle k\rangle_\psi[\langle h\rangle] = \langle k, h \mid k^2 = h^n = e,\ h^k = h^{-1}\rangle$.

Говорят, что группа G является *полупрямым произведением подгрупп* A и B, если выполняются следующие требования: $G = AB,\ A\cap B = E,\ B \lhd G$. Полупрямое произведение обозначают так: $G = A[B]$ или $G = [B]A$. Построенная в теореме 2.47 группа G является полупрямым произведением своих подгрупп K^* и H^*.

Лемма 2.48. *Пусть $G = A[B]$. Тогда:*

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 $(a_1b_1)(a_2b_2) = (a_1a_2)(b_1^{a_2}b_2)$.

☐ 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 $g = a_1b_1$, $a_1 \in A$, $b_1 \in B$, 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. $(a_1b_1)(a_2b_2) = a_1a_2a_2^{-1}b_1a_2b_2 = (a_1a_2)(b_1^{a_2}b_2)$. ⊠

Элемент порядка 2 называется *инволюцией*. *Диэдральной группой* называется группа, порожденная двумя различными инволюциями.

Теорема 2.49. *Пусть G – группа. Тогда следующие утверждения эквивалентны:*

1) G — диэдральная группа;

2) $G = [A]B$, где $A = \langle a\rangle, B = \langle b\rangle, |B| = 2, a^b = a^{-1}$.

☐ Пусть G — диэдральная группа. 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

$$a^i = (ij)^i = iiji = ji = (ij)^{-1} = a^{-1} \in A,$$
$$a^j = (ij)^j = jijj = ji = (ij)^{-1} = a^{-1} \in A,$$

поэтому $A \lhd G$ и $AB \le G$. Так как $j \in B \le AB$ и $aj = ijj = i \in AB$, то $G = \langle i, j\rangle = AB$. Если $E \ne A \cap B$, то $B \le A$ и $i = j$ по следствию теоремы 1.24, с. 25. Получили противоречие. Поэтому $A \cap B = E$ и $G = [A]B$.

Обратно, пусть группа $G = [A]B$, где $A = \langle a\rangle$, $B = \langle b\rangle$, $\mid B \mid = 2$, $a^b = a^{-1}$. Тогда $abab = aa^{-1} = e$ и ab — инволюция. Так как $B = \langle b\rangle \le \langle ab, b\rangle$ и $a = abb \le \langle ab, b\rangle$, то $G \le \langle ab, b\rangle$, т.е. $G = \langle ab, b\rangle$ — диэдральная группа. ⊠

Обычно диэдральную группу порядка $2n$ записывают так: $D_{2n} = \langle a, b \mid a^n = b^2 = e,\ a^b = a^{-1}\rangle$. Отметим, что группа из примера 2.1 при $m = 2$ является диэдральной группой порядка $2n$.

Говорят, что группа G является *центральным произведением* своих подгрупп A и B, если выполняются следующие условия: $G = AB,\ A \lhd G,\ B \lhd G,\ A \cap B \subseteq Z(G)$. Очевидно, что прямое произведение двух подгрупп является центральным. Кроме того, если $G = AB$ — центральное произведение, то

$$G/(A \cap B) = A/(A \cap B) \times B/(A \cap B)$$

будет прямым произведением.

Над полем $\mathbb{Z}_5$ определители матриц

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix},\quad B = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}$$

равны 1, поэтому $A, B \in SL(2, \mathbb{Z}_5)$. Далее, $A^2 = B^2 = 4E, A^4 = B^4 = E$,

$$A^3 = \begin{pmatrix} 3 & 0 \\ 0 & 2 \end{pmatrix},\quad B^3 = \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}.$$

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 произведением двух нормальных подгрупп $\langle A\rangle$ и $\langle B\rangle$. Поскольку $B^{-1}AB = B^3AB = A^3 = A^{-1}$, 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

$Q = \langle A, B \mid A^4 = B^4 = E, A^2 = B^2, B^{-1}AB = A^{-1} \rangle$

называют *группой кватернионов.*

В группе $GL(2, \mathbb{C})$ подгруппа, порожденная матрицами

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

изоморфна группе Q.

2.8. Линейные группы

Нам потребуется следующая информация из теории полей, которую можно найти в учебнике [2]. Характеристика конечного поля — всегда простое число и если P — конечное поле характеристики p, то число элементов в поле P равно p^m, $m \in \mathbb{N}$, т.е. $\mid P \mid= p^m$. Любые два конечных поля равных порядков изоморфны между собой. Пусть P — конечное поле и $|P| = p^m = q$. Если Q — другое поле порядка q, то поле Q изоморфно полю P.

Матрица над полем P, у которой ниже диагонали все элементы — нули, а на диагонали все элементы единицы, называют *верхней унитреугольной.* Множество всех верхних унитреугольных матриц обозначают через $U(n, P)$. Очевидно, что $U(n, P)$ является подгруппой специальной линейной группы $SL(n, P)$ и полной линейной группы $GL(n, P)$, см. параграф 1.1. Кроме того, $SL(n, P) \lhd GL(n, P)$ и фактор-группа $GL(n, P)/SL(n, P)$ изоморфна мультипликативной группе поля P, см. параграф 1.6.

Поскольку любые два конечных поля P, Q равных порядков изоморфны между собой, то группы $GL(n, P), GL(n, Q)$ изоморфны. Этот факт позволяет вместо $GL(n, P)$ писать $GL(n, q)$, где $q = |P| = |Q| = p^m$. Аналогично, вместо $SL(n, P)$ будем писать $SL(n, q)$.

Заметим, что если $E_{p^n} =< a_1 > + \ldots + < a_n >$ — 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, $Aut(E_{p^n}) = AutV(n,p) = GL(n,p)$. Таким образом, доказана

ТЕОРЕМА 2.50. *Элементарная абелева p-группа E_{p^n} порядка p^n изоморфна аддитивной группе векторного пространства размерности n над полем $\mathbb{Z}_p$ из p элементов, а группа автоморфизмов $AutE_{p^n}$ изоморфна полной линейной группе $GL(n,p)$.*

ТЕОРЕМА 2.51. *1.* $\mid GL(n,q) \mid= \prod_{i=0}^{n-1}(q^n - q^i)$.

2. $\mid SL(n,q) \mid= q^{n-1}\prod_{i=0}^{n-2}(q^n - q^i)$.

3. $\mid U(n,q) \mid = q^{n(n-1)/2}$ *и группа* $U(n,p^m), p^m = q$, *является силовской p-подгруппой в группах* $GL(n,p^m)$ *и* $SL(n,p^m)$.

☐ 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 совпадает с порядком группы $GL(n, q)$.

2. Так как $GL(n, P)/SL(n, P) \simeq P^{\#}, \mid P^{\#} \mid = q - 1$, то

$$\mid SL(n, P) \mid = \mid GL(n, P) \mid /(q-1) = \prod_{i=0}^{n-2}(q^n - q^i)q^{n-1}.$$

3. $\mid U(n, q) \mid = q^{(n^2-n)/2}$ поскольку в верхней унитреугольной матрице выше главной диагонали $(n^2 - n)/2$ мест. Далее,

$$\mid GL(n, q) \mid = \prod_{i=0}^{n-1}(q^n - q^i) = q^{1+\dots+(n-1)}\prod_{i=0}^{n-1}(q^{n-i} - 1) =$$

$$= q^{n(n-1)/2}\prod_{i=0}^{n-1}(q^{n-i} - 1) = \mid U(n, q) \mid \prod_{i=0}^{n-1}(q^{n-i} - 1),$$

причем $\prod_{i=0}^{n-1}(q^{n-i} - 1)$ не делится на p, поэтому $U(n, q)$ — силовская p-подгруппа группы $GL(n, q)$. Поскольку $U(n, q) \leq SL(n, q)$, то $U(n, q)$ — силовская p-подгруппа группы $SL(n, q)$.

Теорема 2.52. *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 $detE_{ij} = 1$, то $E_{ij} \in SL(n, P)$. Пусть $B = (b_{ij})$ — произвольная матрица, перестановочная с каждой матрицей E_{ij}. Тогда

$$BE_{ij} = \begin{pmatrix} b_{11} & \dots & b_{1j-1} & b_{1j}+b_{1i} & b_{1j+1} & \dots & b_{1n} \\ b_{21} & \dots & b_{2j-1} & b_{2j}+b_{2i} & b_{2j+1} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ b_{n1} & \dots & b_{nj-1} & b_{nj}+b_{ni} & b_{nj+1} & \dots & b_{nn} \end{pmatrix},$$

$$E_{ij}B = \begin{pmatrix} b_{11} & \dots & b_{1n} \\ \dots & \dots & \dots \\ b_{i-1\,1} & \dots & b_{i-1\,n} \\ b_{i1}+b_{j1} & \dots & b_{in}+b_{jn} \\ b_{i+1\,1} & \dots & b_{i+1\,n} \\ \dots & \dots & \dots \\ b_{n1} & \dots & b_{nn} \end{pmatrix}, \quad \begin{cases} b_{1j}+b_{1i} = b_{1j} \\ b_{2j}+b_{2i} = b_{2j} \\ \dots \\ b_{i-1\,j}+b_{i-1\,i} = b_{i-1\,j} \\ b_{ij}+b_{ii} = b_{ij}+b_{jj} \\ b_{i+1\,j}+b_{i+1\,i} = b_{i+1\,j} \\ \dots \\ b_{nj}+b_{ni} = b_{nj}. \end{cases}$$

Последняя система получилась из равенства $BE_{ij} = E_{ij}B$. Из нее следует, что

$$b_{1i} = b_{2i} = ... = b_{(i-1)i} = b_{(i+1)i} = ... = b_{ni} = 0, b_{ii} = b_{jj}.$$

Таким образом, при $i, j = 1, ..., n$ получаем, что B — скалярная матрица. Итак, 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}, $i, j = 1, ..., n$. Поэтому матрица B будет скалярной. Итак, $Z(GL(n, P)) = \{\alpha E \mid \alpha \in P^{\#}\}$.

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 $E_{ij}, i, j = 1, ..., n$. 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. *1.* $|\, Z(GL(n,q)) \,| = q-1$.

2. $|\, Z(SL(n,q)) \,| = (n, q-1)$.

$\square$ 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 $q-1$. $\boxtimes$

Фактор-группу $GL(n,q)/Z(GL(n,q))$ называют *проективной полной (общей) линейной группой* и обозначают через $PGL(n,q)$. Фактор-группу $SL(n,q)/Z(SL(n,q))$ называют *проективной специальной линейной группой* и обозначают через $PSL(n,q)$.

Следствие 1.

1. $|\, PGL(n,q) \,| = |\, SL(n,q) \,| = q^{n-1} \prod_{i=0}^{n-2}(q^n - q^i)$.

2. $|\, PSL(n,q) \,| = d^{-1} \,|\, SL(n,q) \,| =$

$= d^{-1} q^{n-1} \prod_{i=0}^{n-2}(q^n - q^i)$, *где* $d = (n, q-1)$.

$\square$ Оба утверждения вытекают из теоремы 2.51 и следствия 1.

Следствие 3. *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 2.53. *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 подгруппу индекса 2, изоморфную* $PSL(2,p^m)$.

$\square$ 1. Ясно, что обе подгруппы $Z(GL(2,2^m))$ и $SL(2,2^m)$ нормальны в $GL(2,2^m)$. По теореме 2.52 $Z(GL(2,2^m)) \cap SL(2,2^m) = Z(SL(2,2^m))$. 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 $\mid P^\# \mid = 2^m - 1$ — 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 $\mid Z(GL(2,2^m)) \cdot SL(2,2^m) \mid = \mid Z(GL(2,2^m) \mid\mid SL(2,2^m) \mid = \mid GL(2,2^m) \mid$, 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 $K \lhd GL(2,p^m)$. По следствию 1 теоремы 2.52

$$\mid Z(GL(2,p^m)) \cap SL(2,p^m) \mid = \mid Z(SL(2,p^m) \mid = 2,$$

$$\mid K \mid = \frac{\mid Z(GL(2,p^m)) \mid\mid SL(2,p^m) \mid}{\mid Z(GL(2,p^m)) \cap SL(2,p^m) \mid} =$$

$$= \frac{(p^m-1)p^m(p^{2m}-1)}{2} = \frac{\mid GL(2,p^m) \mid}{2},$$

т.е. $\mid GL(2,p^m) : K \mid = 2$. Кроме того, фактор-группа

$$PGL(2,p^m) = GL(2,p^m)/Z(GL(2,p^m))$$

содержит следующую подгруппу индекса 2:

$$K/Z(GL(2,p^m)) = Z(GL(2,p^m))SL(2,p^m)/Z(GL(2,p^m))$$
$$\simeq SL(2,p^m)/Z(GL(2,p^m)) \cap SL(2,p^m) =$$
$$= SL(2,p^m)/Z(SL(2,p^m)) = PSL(2,p^m).$$

Доказательство следующей теоремы можно найти в книге Хупперта [7], теорема II.8.27.

Теорема 2.54. *Группа $PSL(2,p^m)$ содержит только следующие подгруппы:*

1) элементарные абелевы p-группы порядков $p, p^2, ..., p^m$;

2) циклические группы порядка z в случае, когда z делит $(p^m \pm 1)/d$, где $d = (2, p^m - 1)$;

3) диэдральные группы порядка $2z$*, где* z *как в 2);*

4) A_4 *в случае, когда* $p > 2$ *или* $p = 2$ *и* m *четное;*

5) S_4 *в случае, когда* $p^{2m} \equiv 1 \pmod{16}$*;*

6) A_5 *в случае, когда* $p = 5$ *или* $p^{2m} \equiv 1 \pmod 5$*;*

7) полупрямое произведение элементарной абелевой группы порядка p^k *с циклической группой порядка* t *в случае, когда* t *делит* $(p^k - 1)/d$ *и* t *делит* $p^m - 1$*;*

8) группы $PSL(2, p^k)$ *в случае, когда* k *делит* m*;*

9) группы $PGL(2, p^k)$ *в случае, когда* p *нечетное и* $2k$ *делит* m*.*

3. АБЕЛЕВЫ И НИЛЬПОТЕНТНЫЕ ГРУППЫ

3.1. Строение конечных абелевых групп

В этом параграфе доказывается следующая

Теорема 3.1. *Конечная абелева группа является прямым произведением примарных циклических подгрупп. Любые два таких разложения имеют одинаковое число сомножителей каждого порядка.*

Вначале утверждение теоремы 3.1 докажем для примарных абелевых групп. Для этого потребуются следующие две леммы.

Лемма 3.2. *Если абелева p-группа P имеет единственную подгруппу порядка p, то P циклическая.*

$\square$ Применим индукцию по порядку P. Ясно, что отображение $\varphi: \ x \to x^p, \ x \in P$, является эндоморфизмом группы P, ядро $Ker\varphi = K$ которого состоит из единичного элемента и всех элементов порядка p. По условию в P только одна подгруппа порядка p, поэтому $|K| = p$. По основной теореме о гомоморфизме $P/K \simeq Im\varphi$, а так как по лемме 2.1, с. 57, $Im\varphi$ — подгруппа в P, то $Im\varphi$ — подгруппа индекса p в группе P. Если $Im\varphi = E$, то $P = K$ — циклическая по теореме 1.38, с. 34. Если $Im\varphi \neq E$, то по теореме Силова в $Im\varphi$ имеется подгруппа порядка p, а по индукции $Im\varphi$ циклическая. Это означает, что существует неединичный элемент $g \in P$ такой, что $\langle gK \rangle = P/K$. Теперь $P = \langle g \rangle K$, но в $\langle g \rangle$ имеется подгруппа порядка p, поэтому $K \subseteq \langle g \rangle$ и $P = \langle g \rangle$ циклическая.

Лемма 3.3. *Если H — циклическая подгруппа наибольшего порядка абелевой p-группы P, то существует подгруппа K такая, что $P = H \times K$.*

$\square$ Воспользуемся индукцией по $|P|$. Можно считать, что P нециклическая. По лемме 3.2 группа P имеет не менее двух подгрупп порядка p, а по следствию теоремы 1.24, с. 25, в H только одна подгруппа порядка p. Поэтому существует подгруппа K порядка p, не содержащаяся в H. Ясно, что $H \cap K = E$. В P/K нет циклических подгрупп строго большего порядка, чем порядок циклической подгруппы HK/K, поэтому HK/K является циклической подгруппой наибольшего порядка. По индукции $P/K = HK/K \times L/K$ для некоторой подгруппы L из P. Теперь $P = (HK)L = HL,\ H \cap L = E$ и $P = H \times L$.

Теорема 3.4. *Конечная абелева примарная группа является прямым произведением своих циклических подгрупп. Если имеется два таких разложения* $P = P_1 \times P_2 \times \ldots \times P_r = Q_1 \times Q_2 \times \ldots \times Q_s$, *то* $r = s$ *и при подходящей нумерации* $\mid P_i \mid = \mid Q_i \mid$ *для всех* i.

□ Воспользуемся индукцией по $\mid P \mid$. Пусть теорема верна для всех абелевых p-групп порядка меньше, чем $\mid P \mid$. Выберем в P циклическую подгруппу P_1 наибольшего порядка p^{a_1}. Тогда $P = P_1 \times K$ по лемме 3.3. По индукции $K = P_2 \times \ldots \times P_r$ и первое утверждение теоремы доказано.

Для получения второго утверждения удобно множители расположить так, чтобы их порядки не возрастали:

$$P = \langle g_1 \rangle \times \langle g_2 \rangle \times \ldots \times \langle g_r \rangle,\ P_i = \langle g_i \rangle,\ \mid g_i \mid = p^{a_i}, \quad (3.1)$$
$$a_1 \geq a_2 \geq \ldots \geq a_k \geq a_{k+1} = a_{k+2} = \ldots = a_r = 1,$$

$$P = \langle h_1 \rangle \times \langle h_2 \rangle \times \ldots \times \langle h_s \rangle,\ Q_i = \langle h_i \rangle,\ \mid h_i \mid = p^{b_i}, \quad (3.2)$$
$$b_1 \geq b_2 \geq \ldots \geq b_l \geq b_{l+1} = b_{l+2} = \ldots = b_s = 1,$$

Рассмотрим множество $P^p = \{x^p \mid x \in P\}$ всех p-х степеней элементов из P. Так как P — абелева группа, то $x^p y^p = (xy)^p \in P^p$, $(x^p)^{-1} = (x^{-1})^p \in P^p$ и P^p — подгруппа. Кроме того, $P_i^p = \langle g_i^p \rangle$ — подгруппа индекса p в группе P_i, т.е. $\mid P_i^p \mid = p^{a_i - 1}$.

В соответствии с разложениями (3.1) и (3.2) каждый элемент группы P представим в виде $x = g_1^{t_1} \ldots g_r^{t_r} = h_1^{m_1} \ldots h_s^{m_s}$, поэтому $x^p = g_1^{pt_1} \ldots g_k^{pt_k} = h_1^{pm_1} \ldots h_l^{pm_l}$ и

$$P^p = P_1^p \times P_2^p \times \ldots \times P_k^p = Q_1^p \times Q_2^p \times \ldots \times Q_l^p \quad (3.3)$$

— два разложения подгруппы P^p в прямые произведения циклических подгрупп. Так как $\mid P_i^p \mid = \mid P_i \mid /p$, то $\mid P^p \mid < \mid P \mid$ и к группе P^p применима индукция. Из (3.3) заключаем, что $k = l$ и $\mid P_i^p \mid = \mid Q_i^p \mid$ для всех i. Теперь,

$p^{a_i-1} = p^{b_i-1}$ и $a_i = b_i$ для всех $i = 1, 2, \ldots, k$. Таким образом, $\mid P_i \mid = \mid Q_i \mid$ для $i = 1, 2, \ldots, k$.

Пусть $p^d = \mid P_1 \times \ldots \times P_k \mid = \mid Q_1 \times \ldots \times Q_k \mid$. Тогда из (3.1) и (3.2) заключаем, что $\mid P \mid = p^d \mid P_{k+1} \times \ldots \times P_r \mid = p^d p^{r-k} = p^d \mid Q_{k+1} \times \ldots \times Q_s \mid = p^d p^{s-k}$. Поэтому $r = s$ и теорема полностью доказана.

Теорема 3.5. *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 $n = p_1^{a_1} p_2^{a_2} \ldots p_t^{a_t}$, где $p_1, p_2, \ldots, p_t$ — различные простые числа. По теореме Силова в G существуют силовские подгруппы $G_{p_1}, G_{p_2}, \ldots, G_{p_t}$, соответствующие простым числам $p_1, p_2, \ldots, p_t$. Силовские подгруппы нормальны в G, поскольку G абелева. Кроме того, порядки G_{p_1} и G_{p_2} взаимно просты, поэтому $G_{p_1} \cap G_{p_2} = E$ и $G_{p_1} G_{p_2} = G_{p_1} \times G_{p_2}$. Предположим, что для некоторого k уже доказано, что $G_{p_1} G_{p_2} \ldots G_{p_k} = G_{p_1} \times G_{p_2} \times \ldots \times G_{p_k}$. Тогда подгруппа $H = G_{p_1} \times \ldots \times G_{p_k}$ имеет порядок $p_1^{a_1} \ldots p_k^{a_k}$, а пересечение $H \cap G_{p_{k+1}}$ — подгруппа порядка делящего $\mid H \mid$ и $\mid G_{p_{k+1}} \mid$. Отсюда следует, что $H \cap G_{p_{k+1}} = E$. Так как H и $G_{p_{k+1}}$ — нормальные подгруппы, то $HG_{p_{k+1}} = H \times G_{p_{k+1}}$. Итак, $G_{p_1} \ldots G_{p_{k+1}} = G_{p_1} \times \ldots \times G_{p_{k+1}}$. Теперь согласно индукции, группа G разложима в прямое произведение своих силовских подгрупп. Так как силовские p-подгруппы сопряжены между собой, то для каждого простого p силовская p-подгруппа в абелевой группе единственна.

Доказательство теоремы 3.1. Утверждение теоремы 3.1 является следствием теоремы 3.4 и теоремы 3.5. Действительно, по теореме 3.5 каждая конечная абелева группа разлагается в прямое произведение своих силовских подгрупп. По теореме 3.4 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 3.4 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. ⊠

Вернемся к теореме 3.4. По теореме 1.31, с. 28, 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

$$P = P_1 \times P_2 \times \ldots \times P_r \tag{3.4}$$

циклических подгрупп $P_1, P_2, \ldots, P_r$ порядков $p^{a_1}, p^{a_2}, \ldots, p^{a_r}$. Ясно, что $a = a_1 + a_2 + \ldots + a_r$. Порядки $(p^{a_1}, p^{a_2}, \ldots, p^{a_r})$ циклических множителей прямого произведения (3.4) называют *инвариантами* абелевой p-группы P.

Если две абелевы группы P и Q имеют одинаковые инварианты $(p^{a_1}, p^{a_2}, \ldots, p^{a_r})$, то

$$P = P_1 \times P_2 \times \ldots \times P_r,\ Q = Q_1 \times Q_2 \times \ldots \times Q_r$$

и $|\ P_i\ |=|\ Q_i\ |= p^{a_i}$ для $i = 1, 2, \ldots, r$. Поэтому существуют изоморфизмы $\varphi_i : P_i \to Q_i$, 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 $g_1 g_2 \ldots g_r$, где $g_i \in P_i$. Поэтому отображение $\varphi(g_1 g_2 \ldots g_r) = \varphi_1(g_1)\varphi_2(g_2)\ldots\varphi_r(g_r)$ будет изоморфизмом групп P и Q. Тем самым доказана

Теорема 3.6. *Примарная абелева группа однозначно определяется своими инвариантами.*

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.

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.

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:

$C_8 \times C_{125},\ C_8 \times C_{25} \times C_5,\ C_8 \times C_5 \times C_5 \times C_5,$
$C_4 \times C_2 \times C_{125},\ C_4 \times C_2 \times C_{25} \times C_5,\ C_4 \times C_2 \times C_5 \times C_5 \times C_5,$
$C_2 \times C_2 \times C_2 \times C_{125},\ C_2 \times C_2 \times C_2 \times C_{25} \times C_5,$
$C_2 \times C_2 \times C_2 \times C_5 \times C_5 \times C_5.$

3.2. Примарные группы

Напомним, что *p-группой* называют группу, порядок которой есть степень простого числа p. Ясно, что подгруппы и фактор-группы любой p-группы также являются p-группами. *Примарной* называют группу, которая является p-группой для некоторого простого p.

Теорема 3.7. *Центр неединичной примарной группы отличен от единицы.*

□ Пусть P — p-группа порядка $p^n > 1$ и $K_1, K_2, \ldots, K_t$ — все различные классы сопряженных элементов группы P, $K_i = \{g_i^x \mid x \in P\}$. По следствию 2 теоремы 1.49, с. 40, число элементов в классе сопряженных с g_i элементов равно индексу централизатора элемента g_i, т.е. $\mid K_i \mid = \mid P : C_P(g_i) \mid = p^{a_i}$. Каждый элемент центра составляет отдельный класс и наоборот, если $\mid K_j \mid = 1$, то $g_j \in Z(P)$, где $Z(P)$ — центр. Итак, $P = K_1 \cup K_2 \cup \ldots \cup K_t$, где $K_i \cap K_j = \emptyset$ при $i \neq j$. Пусть

$K_1 = \{e\}$. Тогда $p^n = 1 + p^{a_2} + \ldots + p^{a_t}$. Отсюда следует, что существует $l > 1$ такое, что $a_l = 0$. Но тогда $1 = p^{a_l} =\mid P : C_P(g_l) \mid$ и $g_l \in Z(P)$.

Теорема 3.8. *В примарной группе каждая собственная подгруппа отлична от своего нормализатора.*

$\square$ Пусть P — p-группа и A — собственная подгруппа. Рассмотрим разложение группы P в двойные смежные классы по A.

$$P = Ax_1A \cup Ax_2A \cup \ldots \cup Ax_tA = A \cup (\cup_{i=2}^{t} Ax_iA). \quad (3.5)$$

Здесь $x_1 = e$. Используя теорему 1.42, с. 37, получаем

$$\mid Ax_iA \mid=\mid A^{x_i}A \mid=\mid A^{x_i} \mid\mid A \mid / \mid A^{x_i} \cap A \mid .$$

Теперь из (3.5) вытекает равенство:

$$\mid P \mid=\mid A \mid + \sum_{i=2}^{t} \mid A^{x_i} \mid\mid A \mid / \mid A^{x_i} \cap A \mid . \qquad (3.6)$$

Пусть $\mid P \mid= p^n$, $\mid A \mid= p^a$. Тогда из (3.6) следует, что

$$p^{n-a} = 1 + \sum_{i=2}^{t} \mid A \mid / \mid A^{x_i} \cap A \mid .$$

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 $\mid A \mid=\mid A^{x_j} \cap A \mid$. 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.*

$\square$ Пусть P — p-группа и $M < \cdot\, P$. По теореме 3.8 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 фактор-группе P/M нет нетривиальных подгрупп, поэтому по теореме Силова группа P/M имеет простой порядок.

Теорема 3.9. *В примарной группе пересечение неединичной нормальной подгруппы с центром группы отлично от единицы.*

$\Box$ Пусть P — p-группа и $A \triangleleft P$, $A \neq E$. Требуется доказать, что $A \cap Z(P) \neq E$. 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. $A = K_1 \cup K_2 \cup \ldots \cup K_t$, где $K_i = {a_i}^P$. Можно положить, что $K_1 = \{e\}$. Поскольку $\mid K_i \mid = \mid P : C_P(a_i) \mid$, то считая $\mid A \mid = p^n$, $\mid K_i \mid = p^{n_i}$ получаем

$$p^n = 1 + \sum_{i=2}^{t} p^{n_i}.$$

Теперь ясно, что существует $j \geq 2$ такое, что $p^{n_j} = \mid K_j \mid = 1$ и $a_j \in Z(P)$.

Следствие 1. *Нормальная подгруппа простого порядка примарной группы содержится в центре.*

Следствие 2. *Минимальная нормальная подгруппа примарной группы имеет простой порядок и содержится в центре группы.*

$\Box$ 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 $< a > \triangleleft P$ и из условия $N \cdot\!\triangleleft\, P$ следует, что $N =< a >$.

3.3. 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 группе S_3 силовская 2-подгруппа $\langle(12)\rangle$ ненормальна, поэтому S_3 ненильпотентна.

Лемма 3.10. *Нильпотентная группа является прямым произведением своих силовских подгрупп.*

$\Box$ Пусть группа G нильпотентна, $\mid G \mid = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, где все простые числа p_i различны, и пусть P_i — силовская p_i-подгруппа. Так как P_1 и

$P_2 \lhd G$, то $P_1P_2 \lhd G$, а поскольку $P_1 \cap P_2 = E$, то $P_1P_2 = P_1 \times P_2$. Далее, $(P_1P_2)P_3 \lhd G$, $P_1P_2 \cap P_3 = E$, поэтому $(P_1P_2)P_3 = P_1 \times P_2 \times P_3$, и т.д. Через n шагов с привлечением теоремы 1.65, с. 53, получаем, что $G = P_1P_2 \dots P_n = P_1 \times P_2 \times \dots \times P_n$.

Лемма 3.11. *1) Подгруппа и фактор-группа 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 из H. Так как в группе силовские p-подгруппы сопряжены, 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 $\mid H : P_1 \mid$ не делится на p получаем, что $P_1 = P \cap H$. Но $P \lhd G$, поэтому $P_1 \lhd H$ и H нильпотентна.

Пусть $N \lhd G$. По теореме 1.65, с. 53, PN/N — силовская в G/N. Так как $P \lhd G$ и $N \lhd G$, то $PN/N \lhd G/N$, т.е. 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 в G_i. Так как $P_i \lhd G_i$ и в прямом произведении элементы из различных множителей перестановочны, то $P_i \lhd G$ и $P = P_1 \times \dots \times P_n \lhd G$. Кроме того, $\mid P \mid = \prod_{i=1}^{n} \mid P_i \mid$ и P — p-группа. Ясно, что

$$\mid G : P \mid = \prod_{i=1}^{n} \mid G_i : P_i \mid,$$

поэтому $\mid G : P \mid$ не делится на p и P — силовская в G. ⊠

Напомним, что $\pi(X)$ — множество всех простых делителей порядка группы X.

Теорема 3.12. *1) Если G — неединичная нильпотентная группа, то центр $Z(G) \neq E$ 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* $\pi(N) = \pi(N \cap Z(G))$.

$\square$ 1. Пусть G — неединичная нильпотентная группа. По лемме 3.10 G является прямым произведением своих силовских подгрупп. Но центр каждой силовской подгруппы отличен от E по теореме 3.7, с. 103. По лемме 2.27, с. 75, центр прямого произведения равен прямому произведению центров сомножителей, поэтому $Z(G) \neq E$. Если $p \in \pi(G)$ и P — силовская p-подгруппа в G, то $E \neq Z(P) \leq Z(G)$ и $p \in \pi(Z(G))$. Значит, $\pi(Z(G)) = \pi(G)$.

2. Пусть теперь G — нильпотентная группа и $H < G$. По лемме 3.10 $G = P_1 \times P_2 \times \ldots \times P_n$, где P_i — силовская p_i-подгруппа, а по лемме 3.11

$$H = (H \cap P_1) \times (H \cap P_2) \times \ldots \times (H \cap P_n),$$

где $H \cap P_i$ — силовская p_i-подгруппа из H. Так как $H < G$, то существует номер j такой, что $H \cap P_j < P_j$. По теореме 3.8, с. 104, 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 $E \neq N \lhd G$. 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 $P_1 \lhd N$, а $P \lhd G$. По лемме Фраттини $G = NN_G(P_1) = N_G(P_1)$, т.е. $P_1 \lhd G$. Теперь $P_1 \lhd P$ и по теореме 3.9, с. 104, пересечение $P_1 \cap Z(P) \neq E$. Так как центр группы G совпадает с прямым произведением центров силовских подгрупп, то

$$E \neq P_1 \cap Z(P) \leq N \cap Z(G), \; p \in \pi(N \cap Z(G)).$$

Поэтому $\pi(N) \subseteq \pi(N \cap Z(G))$. Поскольку $N \cap Z(G) \leq Z(N)$, то $\pi(N \cap Z(G)) \subseteq \pi(Z(N)) = \pi(N)$. Итак, $\pi(N) = \pi(N \cap Z(G))$.

Следствие 1. *В нильпотентной группе каждая максимальная подгруппа нормальна и имеет простой индекс.*

$\square$ Пусть G — нильпотентная группа и $M < \cdot\, G$. По теореме 3.12 M — собственная подгруппа в своем нормализаторе $N_G(M)$. Поэтому $N_G(M) = G$ и $M \lhd G$. Теперь в G/M нет нетривиальных подгрупп и G/M имеет простой порядок по теореме Силова.

Следствие 2. *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 3.12. Поскольку $N \cap Z(G) \lhd G$ и $N \cdot\!\lhd G$, 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 $N_1 \lhd G$, то $N_1 = N$.

Теорема 3.13. *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 3.10 и теоремы 3.12. Из 2 следует 1 по определению прямого произведения. Из 3 следует 4. Пусть выполняется 4, т.е. в G все максимальные подгруппы нормальны. Предположим, что G ненильпотентна. Тогда в G существует ненормальная силовская подгруппа P. Пусть M — максимальная подгруппа группы G, содержащая $N_G(P)$. По условию $M \lhd G$, 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 3.14. *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. 43, подгруппа нильпотентной группы G/N. По теореме 3.12 $C/N \cap Z(G/N) \neq E$. 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. 45, подгруппа H абелева. Противоречие.

Лемма 3.15. *Пусть $Z \le Z(G)$. Тогда и только тогда группа G нильпотентна, когда фактор-группа G/Z нильпотентна.*

□ Если группа нильпотентна, то по лемме 3.11 G/Z нильпотентна. Обратно, пусть G/Z нильпотентна и P — силовская подгруппа в G. Тогда PZ/Z — силовская подгруппа в G/Z по лемме 1.65, с. 53, поэтому $PZ/Z \triangleleft G/Z$ и $PZ \triangleleft G$. По лемме Фраттини $G = N_G(P)Z$, а т.к. $Z \le Z(G)$, то $P \triangleleft G$. ⊠

Пусть G — неединичная группа. Введем следующие обозначения: $Z_0(G) = E$, $Z_1(G) = Z(G)$, $Z_2(G)/Z_1(G) = Z(G/Z_1(G)), \dots, Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)), \dots$. Ясно, что

$$E = Z_0(G) \le Z_1(G) \le \dots \le Z_{i-1}(G) \le Z_i(G) \le \dots.$$

Теорема 3.16. *Тогда и только тогда неединичная группа G нильпотентна, когда существует натуральное число c такое, что $Z_c(G) = G$.*

□ 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 3.11. Если $G/Z_1(G) = E$, то $c = 1$. Если $G/Z_1(G) \ne E$, то $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \ne E$ 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 $G \ne E$ и $Z_c(G) = G$ для некоторого натурального c. Воспользуемся индукцией по c. Если $c = 1$, то $Z(G) = Z_1(G) = G$ и G абелева. Пусть $Z(G) = Z_1(G) \ne G$. Для $G/Z_1(G)$ получаем, что $Z_{c-1}(G/Z_1(G)) = G/Z_1(G)$, поэтому $G/Z_1(G)$ нильпотентна по индукции. Теперь G нильпотентна по лемме 3.15. ⊠

Итак, каждая неединичная нильпотентная группа обладает *возрастающим центральным рядом* $E = Z_0(G) <$

$Z_1(G) < \ldots < Z_{i-1}(G) < Z_i(G) < \ldots < Z_c(G) = G$, где $Z_1(G) = Z(G), \ldots, Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G))$, $i = 1, \ldots, c$. Число c называется *ступенью нильпотентности* группы G и обозначается через $c(G)$. Для единичной группы полагают $c(E) = 0$. Очевидно, что $c(G) = 1$, когда $G \neq E$ и G абелева, а $c(G) = 2$, когда G неабелева, но $G/Z(G)$ абелева.

3.4. 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 используется запись $M < \cdot\ G$. Легко проверяется

Лемма 3.17. *Пусть $M < \cdot\ G$ и $K \lhd G$. Тогда:*

1) если $\alpha \in AutG$, то $\alpha(M) < \cdot\ G$;

2) если $x \in G$ то $M^x < \cdot\ G$;

3) если $K \leq M$, то $M/K < \cdot\ G/K$;

4) если K не содержится в M, то $MK = G$;

5) если $\overline{U}$ — максимальная подгруппа фактор-группы $\overline{G} = G/K$, то существует $U < \cdot\ G$ такая, что $K \leq U$ и $\overline{U} = U/K$;

6) если $M \lhd G$, то индекс подгруппы M в группе G является простым числом.

Подгруппой Фраттини неединичной группы называется пересечение всех её максимальных подгрупп. Подгруппа Фраттини неединичной группы G обозначается через $\Phi(G)$. Таким образом, $\Phi(G) = \cap_{M < \cdot\ G} M$. 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 $Core_G(H)$.

Лемма 3.18. *Пусть $H \leq G$. Тогда:*

1) $Core_G(H)$ — наибольшая нормальная подгруппа группы G, содержащаяся в H;

2) $\Phi(G) = \cap_{M <\cdot G} Core_G(M)$;

3) $\Phi(G)$ char G, в частности, $\Phi(G) \lhd G$.

☐ 1. По определению $Core_G(H) = \cap_{x \in G} H^x$. Поэтому $Core_G(H) \lhd G$. Если $K \lhd G$ и $K \leq H$, то $K^x = K \leq H^x$ для любого $x \in G$ и $K \leq Core_G(H)$. Поэтому, $Core_G(H)$ — наибольшая нормальная подгруппа группы G, содержащаяся в H.

2. Так как подгруппа, сопряжённая максимальной, будет также максимальной подгруппой, то $\Phi(G) = \cap_{M <\cdot G} M = \cap_{M <\cdot G}(\cap_{x \in G} M^x) = \cap_{M <\cdot G} Core_G(M)$.

3. Из леммы 3.17 следует, что $\Phi(G)$ *char* G, в частности, $\Phi(G) \lhd G$.

Теорема 3.19. *Подгруппа Фраттини является нормальной нильпотентной подгруппой.*

☐ Из леммы 3.18 следует, что $\Phi(G) \lhd G$. Пусть P — силовская подгруппа в $\Phi(G)$. Предположим, что P ненормальна. Тогда $N_G(P)$ — собственная подгруппа и можно выбрать максимальную подгруппу M в 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 $P \lhd G$. ⊠

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 3.20. *Подгруппа Фраттини группы G состоит из всех необразующих элементов. В частности, если $G/\Phi(G)$ циклическая, то 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, не содержащая x. Теперь $M \neq G$, а $\langle M, x\rangle = G$, противоречие с тем, что x необразующий. Поэтому, допущение неверно, и $X \subset \Phi(G)$.

Пусть $y \in \Phi(G)$ и пусть существует такое подмножество $T \subset G$, что $\langle T\rangle \neq G$, а $\langle T, y\rangle = G$. Пусть H — максимальная подгруппа, содержащая подгруппу $\langle T\rangle$. Так как $y \in \Phi(G) \le H$, то $G = \langle T, y\rangle \le H$, противоречие. Поэтому допущение неверно и y необразующий.

Пусть $G/\Phi(G)$ 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 G циклическая.

Следствие 1. *Если H — подгруппа группы G и $H\Phi(G) = G$, то $H = G$.*

Следствие 2. *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 3.20 $G = \langle K, H\rangle = \langle H\rangle = H$, 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 подгруппа обладает по крайней мере одним добавлением.

Лемма 3.21. *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 в H такая, что $H \cap K$ не содержится в H_1. Так как $H \cap K \triangleleft H$, то

$$H_1(H \cap K) = H;\ G = HK = H_1(H \cap K)K = H_1K,$$

противоречие с определением добавления. Поэтому допущение неверно и $H \cap K \le \Phi(H)$.

Обратно, пусть $HK = G$, $H \cap K \le \Phi(H)$. Предположим, что H не является добавлением к K. Тогда существует максимальная подгруппа H_1 в H такая, что $H_1K = G$. По тождеству Дедекинда $H = H_1(H \cap K) \le H_1\Phi(H) = H_1$, противоречие. Поэтому допущение неверно и H является добавлением к K.

Теорема 3.22. *Пусть $K \lhd G$. Тогда:*

1) $\Phi(K) \le \Phi(G)$;

2) $\Phi(G)K/K \le \Phi(G/K)$;

3) если $K \le \Phi(G)$, то $\Phi(G)/K = \Phi(G/K)$;

4) если $A \le G$ и $K \le \Phi(A)$, то $K \le \Phi(G)$.

□ 1. Так как $\Phi(K)$ *char* K, то $\Phi(K) \lhd G$. Предположим, что $\Phi(K) \nsubseteq \Phi(G)$. Тогда существует максимальная подгруппа M такая, что $\Phi(K)M = G$. По тождеству Дедекинда $K = \Phi(K)(K \cap M)$, а по следствию 1 теоремы 3.20 $K = K \cap M$, т.е. $K \le M$. Теперь $\Phi(K) \le M$, противоречие. Поэтому допущение неверно и $\Phi(K) \le \Phi(G)$.

2. Утверждение вытекает из леммы 3.17.

3. Так как $K \le \Phi(G)$, то K содержится в каждой максимальной подгруппе и $\Phi(G)/K = \Phi(G/K)$ по лемме 3.17.

4. Пусть $A \le G$ и $K \le \Phi(A)$. 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 $K \le \Phi(A)$, то по следствию 1 теоремы 3.20 $A = A \cap M$, т.е. $A \le M$. Теперь $K \le M$, что противоречит предположению. Поэтому предположение неверно и $K \le \Phi(G)$.

Теорема 3.23. $\Phi(G_1 \times G_2) = \Phi(G_1) \times \Phi(G_2)$.

□ Пусть $G = G_1 \times G_2$. Так как $G_1 \lhd G$ и $G_2 \lhd G$, то по теореме 3.22 $\Phi(G_1) \times \Phi(G_2) \subseteq \Phi(G)$. Пусть $G/(\Phi(G_1) \times \Phi(G_2)) = G^*$. По теореме 3.22

$$\Phi(G)/(\Phi(G_1) \times \Phi(G_2)) = \Phi(G^*).$$

Ясно, что $G^* = G_1^* \times G_2^*$, где $G_1^* = G_1/\Phi(G_1)$, $G_2^* = G_2/\Phi(G_2)$. Опять по теореме 3.22 $\Phi(G_1^*) = \Phi(G_2^*) = E$. Так как пересечение максимальных подгрупп группы G^*, содержащих подгруппу G_i^*, равно G_i^* и $G_1^* \cap G_2^* = E$, то $\Phi(G^*) = E$. Поэтому $\Phi(G) = \Phi(G_1) \times \Phi(G_2)$.

Теорема 3.24. *Пусть $D \lhd K \lhd G$, $D \le \Phi(G)$ и $D \lhd G$. Если K/D нильпотентна, то K нильпотентна.*

□ Пусть P — силовская p-подгруппа группы K. По теореме 1.65, с. 53, PD/D — силовская p-подгруппа в K/D, а т.к. K/D нильпотентна, то $PD/D \lhd K/D$. Поскольку PD/D *char* K/D, то $PD/D \triangleleft G/D$, $PD \triangleleft G$. По лемме Фраттини $G = N_G(P)D$, а из следствия 1 теоремы 3.20 вытекает, что $G = N_G(P)$, $P \triangleleft G$ и K нильпотентна.

При $D = \Phi(G)$ и $K = G$ получаем

Следствие. *Если* $G/\Phi(G)$ *нильпотентна, то* G *нильпотентна.*

Лемма 3.25. *Пусть* G *—* p*-группа. Тогда:*

1) $G/\Phi(G)$ *— 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*, фактор-группа по которой элементарная абелева* p*-группа;*

4) если $\mid G/\Phi(G) \mid = p^n$*, то существуют элементы* $x_1, \ldots, x_n \in G$ *такие, что* $G = \langle x_1, \ldots, x_n \rangle$.

☐ 1. В p-группах максимальные подгруппы нормальны и имеют индекс p, см. следствие теоремы 3.8, с. 104. Пусть $\{M_i \mid i = 1, \ldots, m\}$ — множество всех максимальных подгрупп группы G. Так как фактор-группа $G/\Phi(G) = G/\cap_{i=1}^{m} M_i$ по лемме 2.33, с. 79, 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 $\{H_i/K \mid i = 1, \ldots, k\}$ — множество всех максимальных подгрупп группы G/K. По условию G/K элементарная абелева, поэтому

$$\cap_{i=1}^{k}(H_i/K) = E,\ \Phi(G) = \cap_{X <\cdot G} X \subseteq \cap_{i=1}^{k} H_i = K.$$

3. Утверждение вытекает из 1 и 2.

4. Так как $G/\Phi(G)$ — элементарная абелева группа порядка p^n, то $G/\Phi(G) = \langle x_1\Phi(G)\rangle \times \ldots \times \langle x_n\Phi(G)\rangle$ для некоторых $x_1, \ldots, x_n \in G$. Теперь $G = \langle x_1, \ldots, x_n, \Phi(G)\rangle$ и $G = \langle x_1, \ldots, x_n\rangle$ по теореме 3.20.

4. РАЗРЕШИМЫЕ И СВЕРХРАЗРЕШИМЫЕ ГРУППЫ

4.1. Коммутант

В абелевой группе любые два элемента перестановочны. Если группа неабелева, то в ней существуют неперестановочные элементы, т.е. такие элементы a и b, что $ab \neq ba$. Поэтому естественно рассмотреть элемент x, для которого $ab = bax$. Отсюда $x = a^{-1}b^{-1}ab$.

Коммутатором элементов a и b называют элемент $a^{-1}b^{-1}ab$, который обозначают через $[a, b]$. Ясно, что $ab = ba[a, b]$. Подгруппа, порожденная коммутаторами всех элементов группы G, называется *коммутантом* группы G и обозначается через G'. Таким образом,

$$G' = \langle [a, b] \mid a, b \in G \rangle.$$

Лемма 4.1. *Пусть G — группа, $a, b, c \in G$. Тогда:*

1) $[a, b]^{-1} = [b, a]$;

2) $[ab, c] = [a, c]^b [b, c]$;

3) $[a, bc] = [a, c][a, b]^c$;

4) если $[a, b]$ перестановочен с элементами a и b, то $[a^i, b^j] = [a, b]^{ij}$ для любых $i, j \in \mathbb{N}$.

□ Доказательства утверждений 1–3 осуществляется простой проверкой. Докажем утверждение 4. Пусть $d = [a, b]$. По условию $da = ad$, $db = bd$. Поскольку $d = a^{-1}b^{-1}ab$, то $ad = b^{-1}ab$ и

$$b^{-1}a^i b = (b^{-1}ab)^i = (ad)^i = a^i d^i,$$

$$b^{-2}a^i b^2 = b^{-1}(b^{-1}a^i b)b = b^{-1}(a^i d^i)b = b^{-1}a^i b d^i = a^i d^{2i.}$$

Используя индукцию по j получаем: $b^{-j}a^i b^j = b^{-1}(b^{-(j-1)}a^i b^{j-1})b = b^{-1}(a^i d^{(j-1)i})b = b^{-1}a^i b d^{(j-1)i} = a^i d^{ji}$. Поэтому $[a^i, b^j] = d^{ij} = [a, b]^{ij}$.

Лемма 4.2. *1. Если $H \leq G$, то $H' \leq G'$.*

2. G' char G, в частности, $G' \lhd G$.

3. Если $H \lhd G$, то $H' \lhd G$.

4. Если $G = A \times B$, то $G' = A' \times B'$.

$\square$ 1. Утверждение очевидно.

2. Пусть a, b — произвольные элементы группы G и ψ — произвольный автоморфизм группы G. Тогда

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

Итак, образ коммутатора вновь является коммутатором. Поэтому G' $char$ G.

3. Если $H \lhd G$, то $H' char H \lhd G$ и $H' \lhd G$ по лемме 2.11, с. 64.

4. Из утверждения 1 следует, что $A' \times B' \leq G'$. Если $[a_1b_1, a_2b_2]$ — произвольный коммутатор, $a_1, a_2 \in A$, $b_1, b_2 \in B$, то $[a_1b_1, a_2b_2] = [a_1, a_2][b_1, b_2]$ и $G' \leq A' \times B'$.

Теорема 4.3. *1) Фактор-группа G/G' абелева;*

2) если $N \lhd G$ и G/N абелева, то $G' \leq N$;

3) если $H \leq G$, $G' \leq H$, то $H \lhd G$ и G/H абелева.

$\square$ 1. Для любых $aG', bG' \in G/G'$ имеем:

$$aG'bG' = abG' = ba[a,b]G' = baG' = bG'aG'.$$

Поэтому G/G' абелева.

2. Пусть $a, b \in G$. По условию G/N абелева, поэтому $aNbN = bNaN$, $abN = baN$. По свойствам смежных классов $(ba)^{-1}ab \in N$, поэтому $[a, b] \in N$ и $G' \leq N$.

3. Пусть $H \leq G$ и $G' \leq H$. По теореме о соответствии $H/G' \leq G/G'$. Но G/G' абелева, поэтому $H/G' \lhd G/G'$, $H \lhd G$. У абелевой группы все фактор-группы абелевы. Теперь, $G/H \simeq G/G' \big/ H/G'$ абелева.

Теорема 4.4. *Группа нильпотентна тогда и только тогда, когда её коммутант содержится в подгруппе Фраттини.*

$\square$ Пусть G — нильпотентная группа. По следствию 1 теоремы 3.12, с. 106, все максимальные подгруппы в G нормальны и имеют простые индексы. Поэтому, если $M < \cdot\ G$, то G/M абелева и $G' \leq M$ по теореме 4.3. Следовательно, $G' \leq \cap_{M <\cdot\ G} M = \Phi(G)$.

Обратно, пусть $G' \leq \Phi(G)$. Тогда $G/\Phi(G)$ абелева и по следствию теоремы 3.24, с. 113, группа G нильпотентна.

Теорема 4.5. *Если G — группа, то $G' \cap Z(G) \leq \Phi(G)$.*

$\square$ Положим $D = G' \cap Z(G)$. Допустим, что D не содержится в $\Phi(G)$. Тогда существует максимальная подгруппа M такая, что $DM = G$. Если $g = dm \in G$, $d \in D, m \in M$, то $M^g = M^m = M$. Поэтому $M \lhd G$ и $G' \subseteq M$. Теперь $G = M$, противоречие. ⊠

Подгруппа $G'' = (G')'$ называется *вторым коммутантом* группы G, а $G^{(i)} = (G^{(i-1)})'$ — *i–м коммутантом.*

Лемма 4.6. *Пусть $N \lhd G$. Тогда $(G/N)^{(i)} = G^{(i)}N/N$ для любого $i \in \mathbb{N}$.*

□ Обозначим $(G/N)' = K/N$. Воспользуемся теоремой 4.3. По утверждению 1 этой теоремы фактор-группа $G/N\big/K/N \simeq G/K$ абелева, а по по утверждению 2 — $G' \leq K$ и $G'N \subseteq K$.

Обратно, $(G/N)\big/(G'N/N) \simeq G/G'N$ абелева по утверждению 3 теоремы 4.3. По утверждению 2 этой теоремы $K/N \leq G'N/N$ и $K \subseteq G'N$. Следовательно, $K = G'N$ и $(G/N)' = G'N/N$. Для $i = 1$ лемма доказана.

Предположим, что лемма верна для t, т.е. $(G/N)^{(t)} = G^{(t)}N/N$, и докажем ее для $t + 1$. Ясно, что $(G/N)^{(t+1)} = ((G/N)^{(t)})' = (G^{(t)}N/N)' = (G^{(t)}N)'N/N \geq G^{(t+1)}N/N$. С другой стороны, $G^{(t)}N/N\big/G^{(t+1)}N/N \simeq G^{(t)}N\big/G^{(t+1)}N \simeq G^{(t)}\big/G^{(t)} \cap G^{(t+1)}N$ является абелевой группой поскольку $(G^{(t)})' = G^{(t+1)} \leq G^{(t)} \cap G^{(t+1)}$. Следовательно, $(G/N)^{(t+1)} = (G^{(t)}N/N)' \leq G^{(t+1)}N/N$. ⊠

Для подгрупп A и B группы G положим

$$\big[A, B\big] = \langle [a, b] \mid a \in A, b \in B\rangle.$$

Подгруппу $\big[A, B\big]$ называют *взаимным коммутантом подгрупп* A и B. Ясно, что $G' = \big[G, G\big]$.

Лемма 4.7. *Пусть G — группа, $A, B \leq G$. Тогда:*

1) $\big[A, B\big] = \big[B, A\big]$;

2) $\big[A, B\big] \lhd \langle A \cup B\rangle$;

3) если $A_1 \leq A$, $B_1 \leq B$, то $\big[A_1, B_1\big] \leq \big[A, B\big]$;

4) $\big[A, B\big] \leq A$ тогда и только тогда, когда $B \leq N_G(A)$;

5) если A и $B \lhd G$, то $\big[A, B\big] \leq A \cap B$.

□ 1. Так как $[b, a] = [a, b]^{-1} \in \big[A, B\big]$, то $\big[B, A\big] \leq$

$\big[A,B\big]$. Аналогично, $[a,b]=[b,a]^{-1}\in\big[B,A\big]$ и $\big[A,B\big]\le\big[B,A\big]$.

2. Пусть $a_1,a_2\in A,\ b_1,b_2\in B$. Тогда из утверждений 2 и 3 леммы 4.1 получаем:

$$[a_1,b_1]^{a_2}=[a_1a_2,b_1][a_2,b_1]^{-1}\in\big[A,B\big],$$
$$[a_1,b_1]^{b_2}=[a_1,b_2]^{-1}[a_1,b_1b_2]\in\big[A,B\big].$$

Поэтому, $\big[A,B\big]\lhd\langle A\cup B\rangle$.

3. Очевидно.

4. $[a,b]=a^{-1}b^{-1}ab\in A$ равносильно тому, что $b^{-1}ab\in A$, т.е. $B\le N_G(A)$.

5. Пусть $A,B\lhd G$. Тогда $[a,b]=a^{-1}(b^{-1}ab)\in A$, $[a,b]=(a^{-1}b^{-1}a)b\in B$ и $\big[A,B\big]\le A\cap B$.

Лемма 4.8. *Пусть группа $G=AB$. Тогда:*

1) $\big[A,B\big]\lhd G$ и $\big[A\big[A,B\big]/\big[A,B\big],B\big[A,B\big]/\big[A,B\big]\big]=E$;

2) если $A_1\lhd A$, то $A_1\big[A,B\big]\lhd G$;

3) $G'=A'B'\big[A,B\big]$.

□ 1. По лемме 4.7 $\big[A,B\big]\lhd\langle A\cup B\rangle=G$. Далее, $a\big[A,B\big]b\big[A,B\big]=ab\big[A,B\big]=ba[a,b]\big[A,B\big]=ba\big[A,B\big]=b\big[A,B\big]a\big[A,B\big]$, поэтому $\big[A\big[A,B\big]/\big[A,B\big],B\big[A,B\big]/\big[A,B\big]\big]=E$.

2. Пусть $A_1\lhd A$. Тогда $A_1\big[A,B\big]/\big[A,B\big]$ нормальна в $A\big[A,B\big]/\big[A,B\big]$, а из 1 следует, что $A_1\big[A,B\big]/\big[A,B\big]$ нормальна в $G/\big[A,B\big]$. Итак, $A_1\big[A,B\big]\lhd G$.

3. Ясно, что $A'B'\big[A,B\big]\le G'$. Так как $A'\big[A,B\big]\lhd G$, $B'\big[A,B\big]\lhd G$ и $G/A'B'\big[A,B\big]$ абелева, то $G'\le A'B'\big[A,B\big]$.

Теорема 4.9. *Если $G=AB$, подгруппы A и B абелевы, то коммутант группы G абелев.*

□ По лемме 4.8 $G'=\big[A,B\big]$. Пусть $a_1,a_2\in A,\ b_1,b_2\in B$, $a_1^{b_2}=a_3b_3,\ b_1^{a_2}=b_4a_4,\ a_3,a_4\in A,\ b_3,b_4\in B$. Учитывая абелевость подгрупп A и B получаем:

$$[a_1,b_1]^{a_2b_2}=[a_1,b_1^{a_2}]^{b_2}=[a_1,b_4a_4]^{b_2}=[a_1,b_4]^{b_2}=$$
$$=[a_1^{b_2},b_4]=[a_3b_3,b_4]=[a_3,b_4],\ \ [a_1,b_1]^{b_2a_2}=[a_1^{b_2},b_1]^{a_2}=$$

$$= [a_3b_3, b_1]^{a_2} = [a_3, b_1]^{a_2} = [a_3, b_1^{a_2}] = [a_3, b_4a_4] = [a_3, b_4].$$

$$[a_1, b_1]^{a_2b_2} = [a_1, b_1]^{b_2a_2},\ [b_2^{-1}, a_2^{-1}][a_1, b_1] = [a_1, b_1][b_2^{-1}, a_2^{-1}].$$

Отсюда следует, что коммутант группы G абелев. ⊠

Для группы G положим $K_0(G) = G$. Определим для каждого $i \in \mathbb{N}$ подгруппу $K_i(G) = \big[K_{i-1}(G), G\big]$. Ясно, что $K_1(G) = \big[K_0(G), G\big] = G'$.

Лемма 4.10. *1) $K_i(G)$ — характеристическая подгруппа группы G для любого $i \in \mathbb{N} \cup \{0\}$;*

2) $K_i(G) \le K_{i-1}(G)$ для всех $i \in \mathbb{N}$;

3) $K_i(G)/K_{i+1}(G) \le Z(G/K_{i+1}(G))$ для $i \in \mathbb{N} \cup \{0\}$.

□ 1. Применим индукцию по i. $K_1(G) = G'$ — характеристическая подгруппа группы G. Пусть уже доказано, что $K_i = K_i(G)$ *char* G и пусть $f \in \mathrm{Aut}G$, $a \in K_i$, $g \in G$. Тогда $f([a, g]) = [f(a), f(g)] \in \big[K_i, G\big] = K_{i+1}$ и K_{i+1} *char* G.

2. Утверждение следует из леммы 4.7.

3. Если $a \in K_i$, $g \in G$, то

$$aK_{i+1}gK_{i+1} = ga[a, g]K_{i+1} = gaK_{i+1} = gK_{i+1}aK_{i+1}$$

и $K_i/K_{i+1} \le Z(G/K_{i+1})$, $i \in \mathbb{N} \cup \{0\}$. ⊠

Итак, для группы G построена цепочка подгрупп: $G = K_0(G) \ge K_1(G) \ge \ldots \ge K_i(G) \ge \ldots$ с центральными факторами $K_{i-1}(G)/K_i(G) \le Z(G/K_i(G))$, $i \in \mathbb{N}$.

Теорема 4.11. *1. Если существует натуральное число m такое, что $K_m(G) = E$, то группа G нильпотентна.*

2. Ступень нильпотентности нильпотентной группы G есть наименьшее натуральное число n, для которого $K_n(G) = E$.

□ 1. Применим индукцию по m. Если $m = 1$, то $K_1(G) = G' = E$ и группа G абелева. Пусть $m > 1$ и $K_m(G) = E$, $K_{m-1}(G) \ne E$. Тогда подгруппа $K_{m-1}(G) \le Z(G)$, а фактор-группа $G/K_{m-1}(G)$ нильпотентна по индукции. По лемме 3.15, с. 109, группа G нильпотентна.

2. Пусть G — нильпотентная группа ступени нильпотентности n. Тогда n — наименьшее натуральное число,

для которого $Z_n(G) = G$. Положим $K_i = K_i(G)$, $Z_i = Z_i(G)$. Проверим индукцией по n, что

$$K_i \leq Z_{n-i} \text{ для всех } i \in \mathbb{N} \cup \{0\}. \qquad (4.1)$$

При $i = 0$ $K_0 = G \leq Z_n = G$. Пусть $K_{i-1} \leq Z_{n-i+1}$. Так как $Z_{n-i+1}/Z_{n-i} = Z(G/Z_{n-i})$, то

$$K_i = \langle [a, g] \mid a \in K_{i-1},\ g \in G \rangle \leq$$
$$\leq \langle [a, g] \mid a \in Z_{n-i+1},\ g \in G \rangle \leq Z_{n-i}$$

и (4.1) доказано. В частности, при $i = n$ из (4.1) получаем: $K_n \leq Z_0 = E$.

Пусть t — наименьшее натуральное число, для которого $K_t = E$. Ясно, что $t \leq n$. Проверим, используя индукцию по t, что

$$K_{t-i} \leq Z_i \text{ для всех } i \in \mathbb{N} \cup \{0\}. \qquad (4.2)$$

При $i = 0$ $K_t = E \leq Z_0 = E$. Пусть уже доказано, что $K_{t-i+1} \leq Z_{i-1}$. Поскольку

$$G/K_{t-i+1}/Z_{i-1}/K_{t-i+1} \simeq G/Z_{i-1},$$

то существует эпиморфизм G/K_{t-i+1} на G/Z_{i-1} с ядром $Kerf = Z_{i-1}/K_{t-i+1}$. Так как $K_{t-i}/K_{t-i+1} \leq Z(G/K_{t-i+1})$ по лемме 4.10, то

$$f(K_{t-1}/K_{t-i+1}) \leq Z(G/Z_{i-1}) = Z_i/Z_{i-1}$$

и (4.2) доказано. В частности, при $i = t$ из (4.2) получаем: $G = Z_t$ и $t \geq n$. Теперь, $t = n$.

В лемме 2.24, с. 73, для подгрупп H и $K \lhd G$, $K \leq H$ введена подгруппа

$$C_G(H/K) = \langle g \in G \mid g^{-1}h^{-1}gh \in K,\ h \in H \rangle,$$

которая нормальна в G и $G/C_G(H/K)$ изоморфна группе $\mathrm{Aut}_G(H/K)$. Ясно, что $C_G(H/K) = \{g \in G \mid [g, H] \subseteq K\}$.

4.2. Разрешимые группы

Для группы G можно построить цепочку коммутантов $G \geq G' \geq G'' \geq \ldots \geq G^{(i)} \geq G^{(i+1)} \geq \ldots$. Если существует номер n такой, что $G^{(n)} = E$, то группа G называется *разрешимой*. Наименьшее натуральное n, для которого $G^{(n)} = E$, называется *ступенью разрешимости* *группы* G или *производной длиной* и обозначается через $d(G)$. Группа, которая не является разрешимой, называется *неразрешимой.* Для единичной группы получаем $d(E) = 0$. Неединичная абелева группа G имеет цепочку коммутантов $G > G' = E$. Поэтому абелевы группы разрешимы ступени разрешимости ≤ 1.

Лемма 4.12. *Нильпотентные группы разрешимы.*

$\Box$ Пусть G — нильпотентная группа и $M_1 < \cdot\, G$. По следствию 1 теоремы 3.12, с. 106, подгруппа M_1 нормальна и $\mid G : M_1 \mid$ — простое число. По теореме 4.3 $G' \leq M_1$. Если $M_2 < \cdot\, M_1$, то опять $M_2 \lhd M_1$, $\mid M_1 : M_2 \mid$ — простое число и $G'' \leq M_1' \leq M_2$. Пусть $\mid G \mid = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_t^{\alpha_t}$ — каноническое разложение и $n = \alpha_1 + \alpha_2 + \ldots + \alpha_t$. Тогда $G^{(n)} = E$ и G — разрешимая группа ступени не выше n.

Лемма 4.13. *1. Подгруппы и фактор-группы разрешимой группы разрешимы.*

2. Если $N \lhd G$, N и G/N разрешимы, то G разрешима.

3. Прямое произведение разрешимых групп является разрешимой группой.

$\Box$ 1. Пусть G — разрешимая группа и $d(G) = n$. Если $H \leq G$, то $H' = \langle [h_1, h_2] \mid h_1, h_2 \in H \rangle \leq G'$. Аналогично, $H^{(i)} \leq G^{(i)}$ при любом $i = 1, 2, \ldots$ Поэтому $H^{(n)} \leq G^{(n)} = E$ и H разрешима, причем ступень разрешимости H не выше ступени разрешимости G.

Пусть $N \lhd G$. По лемме 4.6, $(G/N)^{(n)} = G^{(n)}N/N = E$ и G/N — разрешимая группа ступени не выше n.

2. Пусть N — разрешимая нормальная подгруппа группы G, $d(N) = n$, а G/N разрешима ступени разрешимости m. Тогда $(G/N)^{(m)} = G^{(m)}N/N = N/N$ и $G^{(m)} \subseteq N$. Теперь $G^{(m+n)} \leq N^{(n)} = E$ и G — разрешимая группа ступени не выше $n + m$.

3. Пусть $G = G_1 \times G_2$, где G_1 и G_2 — разрешимые группы ступени разрешимости n_1 и n_2 соответственно. По теореме об изоморфизме $G/G_1 \simeq G_2$, поэтому по 2 получаем, что G — разрешимая группа. Из леммы 4.2 для любого натурального i следует: $G^{(i)} = G_1^{(i)} \times G_2^{(i)}$, поэтому $d(G) = \max\{d(G_1), d(G_2)\}$.

Теорема 4.14. *1. В разрешимой неединичной группе минимальная нормальная подгруппа является элементарной абелевой p-подгруппой для некоторого простого p.*

2. В разрешимой неединичной группе максимальные подгруппы имеют примарные индексы.

3. Главные факторы разрешимой неединичной группы являются элементарными абелевыми примарными группами.

4. Композиционные факторы разрешимой неединичной группы имеют простые порядки.

$\square$ 1. Пусть G — разрешимая неединичная группа и $N \ \cdot\!\lhd G$. Так как N' — характеристическая подгруппа в N, $N' \neq N$, то $N' \lhd \ G$ и $N' = E$, т.е. подгруппа N абелева. Теперь N — элементарная абелева p-подгруппа для некоторого простого p по следствию теоремы 2.39, с. 84.

2. Воспользуемся индукцией по порядку группы. Пусть $M < \cdot\ G$. Если $N \ \cdot\!\lhd G$, то N — элементарная абелева p-группа для некоторого простого числа p. Если N не содержится в M, то $NM = G$ и $\mid G : M \mid = \mid N : N \cap M \mid = p^i$. Пусть $N \leq M$. Тогда в фактор-группе G/N по индукции максимальная подгруппа M/N имеет примарный индекс, поэтому индекс $\mid G : M \mid = \mid G/N : M/N \mid$ примарен.

3. Пусть H/K — главный фактор разрешимой неединичной группы G. Тогда H/K — минимальная нормальная подгруппа фактор-группы G/K, поэтому H/K — элементарная абелева примарная группа по 1.

4. Пусть H/K — композиционный фактор. Тогда K — наибольшая нормальная подгруппа в H и H/K — простая группа по теореме 1.61, с. 48. Так как H/K разрешима, то H/K отлична от своего коммутанта, поэтому H/K абелева и по теореме 1.54, с. 43, имеет простой порядок.

Группа с примарными индексами максимальных подгрупп может быть неразрешимой. Примером служит простая группа $PSL(2,7)$, в которой индексы максимальных подгрупп принадлежат множеству $\{7, 8\}$, см. теорему 2.54, с. 97.

Теорема 4.15. *Для группы G следующие утверждения эквивалентны:*

1) G — разрешимая группа;

2) каждая неединичная подгруппа группы G отлична от своего коммутанта;

3) группа G обладает нормальным рядом с абелевыми факторами;

4) группа G обладает субнормальным рядом с абелевыми факторами.

□ Пусть дано 1, т.е. G — разрешимая группа. Пусть ступень разрешимости группы G равна n. Тогда

$$G \;>\; G' \;>\; G'' \;>\; \ldots > \; G^{(n-1)} \;>\; G^{(n)} = E.$$

Факторы этого ряда по теореме 4.3 абелевы. Поэтому этот ряд является нормальным рядом с абелевыми факторами. Так как каждый нормальный ряд субнормален, то из 1 следует 3 и 4, а из 3 следует 4.

По лемме 4.13 в разрешимой группе каждая подгруппа разрешима. Поэтому из 1 следует 2.

Пусть дано 4, т.е. G обладает субнормальным рядом

$$G = H_0 \geq H_1 \geq H_2 \geq \ldots \geq H_{t-1} \geq H_t = E$$

с абелевыми факторами $H_i/H_{i+1},\ i = 0, \ldots, t-1$. По теореме 4.3 получаем, что

$$G' \leq H_1,\ G'' = (G')' \leq (H_1)' \leq H_2, \ldots,$$
$$G^{(t)} = (G^{(t-1)})' \leq (H_{t-1})' \leq H_t = E$$

и G разрешима. Таким образом из 4 следует 1.

Пусть дано 2, т.е. в G каждая неединичная подгруппа отлична от своего коммутанта. Тогда $G > G'$. Если $G^{(i)} \neq E$, то $G^{(i)} > G^{(i+1)}$. Поэтому существует натуральное k такое, что $G^{(k)} = E$. Следовательно, группа G разрешима и из 2 следует 1. ⊠

p-Замкнутой называют группу с нормальной силовской p-подгруппой.

Лемма 4.16. *Если G — не p-замкнутая группа и $D = P_1 \cap P_2$ — пересечение двух различных силовских p-подгрупп P_1 и P_2 наибольшего порядка, то $N_G(D)$ — не p-замкнутая группа.*

$\square$ Пусть $B_i = N_{P_i}(D)$. Так как в примарных группах собственные подгруппы отличны от своих нормализаторов, то D — собственная в B_i подгруппа. Предположим, что $N_G(D)$ — p-замкнутая группа, и пусть T — нормальная силовская p-подгруппа подгруппы $N_G(D)$. Через P обозначим силовскую в G подгруппу, содержащую T. Так как $D < B_i \leq T \cap P_i \leq P \cap P_i$ и D — пересечение силовских p-подгрупп наибольшего порядка, то $P = P_1$ и $P = P_2$, противоречие.

Теорема 4.17. *Пусть G — группа порядка $p^n q$, где p и q — различные простые числа. Тогда:*

1) если $p > q$, то силовская p-подгруппа нормальна;

2) если $q > p^n$, то силовская q-подгруппа нормальна;

3) если $q < p^n$, но $p < q$, то в группе G есть неединичная нормальная p-подгруппа.

$\square$ Пусть P и Q — силовские p-подгруппа и q-подгруппа группы G. Ясно, что $| G : N_G(P) |= 1$ или q, а по теореме Силова $| G : N_G(P) |= 1 + kp; \ \ k \in \mathbb{N} \cup \{0\}$. Аналогично, $| G : N_G(Q) |= p^t = 1 + kq; \ \ t, \ k \in \mathbb{N} \cup \{0\}$.

1. Если $p > q$, то $| G : N_G(P) |= 1$ и $P \lhd G$.

2. Если $q > p^n$, то $| G : N_G(Q) |= 1$ и $Q \lhd G$.

3. Теперь пусть $q > p$ и $q < p^n$. Если $P \lhd G$, то утверждение 3 справедливо. Пусть P не является нормальной подгруппой группы G и пусть P_1 и P_2 — различные силовские p-подгруппы группы G, для которых пересечение $D = P_1 \cap P_2$ имеет наибольший порядок. Так как $| P_1 P_2 |=| P_1 || P_2 | / | D |= p^n p^n / | D |\leq p^n q$, то $D \neq E$. Если $D \lhd \ G$, то теорема доказана. Пусть D не является нормальной подгруппой группы G. По предыдущей лемме подгруппа $T = N_G(D)$ не является p-группой, поэтому некоторая силовская q-подгруппа Q группы G содержится в T. Так как $G = P_1 Q$, то каждый элемент $g \in G$ представим в виде $g = ba$, где $a \in P_1, \ b \in Q$. Поэтому $D^g = D^{ba} = D^a \leq \langle D, P_1 \rangle = P_1$ и $E \neq D^G \leq P_1$.

Следствие. *Группа порядка $p^n q$ разрешима для любого $n \in \mathbb{N} \cup \{0\}$.*

$\square$ По теореме 4.17 группа G порядка $p^n q$ содержит неединичную примарную нормальную подгруппу N. Теперь N разрешима по лемме 4.12, а фактор-группа G/N разрешима либо по индукции, либо по лемме 4.12. Из леммы 4.13 следует, что G разрешима.

Теорема 4.18 (Бернсайда). *Группа порядка $p^n q^m$ разрешима для любых $n, m \in \mathbb{N} \cup \{0\}$.*

Доказательство теоремы 4.18 имеется в монографиях [23], [26], [27].

Теорема 4.19 (Томпсона-Фейта). *Группы нечетного порядка разрешимы.*

Доказательство теоремы 4.19 опубликовано в работе Feit W., Thompson J. Solvability of groups of odd order // Pacif. J. Math. 1963. 13, №3. P. 775-1029.

4.3. Подгруппа Фиттинга

Произведение всех нормальных нильпотентных подгрупп группы G называют *подгруппой Фиттинга* группы G и обозначают через $F(G)$. Множество простых делителей порядка группы G обозначается через $\pi(G)$, а наибольшую нормальную p-подгруппу группы G — через $O_p(G)$.

Лемма 4.20. *1. $F(G)$ — наибольшая нормальная нильпотентная подгруппа группы G.*

2. $F(G) = \prod_{p \in \pi(G)} O_p(G)$.

3. $F(G)$ char G.

☐ 1. Пусть H и K — нильпотентные нормальные подгруппы группы G и пусть H_p и K_p — силовские p-подгруппы из H и K. Так как H_p *char* H, а $H \triangleleft G$, то $H_p \triangleleft G$ по лемме 2.11, с. 64. Аналогично, $K_p \triangleleft G$, поэтому $H_p K_p \triangleleft G$. Ясно, $H_p K_p$ — p-группа. Покажем, что она силовская в HK. Для этого вычислим ее индекс:

$$| HK : H_p K_p |= \frac{| H || K || H_p \cap K_P |}{| H \cap K || H_p || K_p |} =$$

$$= \frac{| H : H_p || K : K_p |}{| H \cap K : H_p \cap K_p |}.$$

Так как числитель не делится на p, то H_pK_p — силовская p-подгруппа группы HK. Итак, произведение двух нормальных нильпотентных подгрупп есть нормальная нильпотентная подгруппа. Поэтому $F(G)$ — наибольшая нормальная нильпотентная подгруппа группы G.

2. Ясно, что $O_p(G) \leq F(G)$ для всех p, поэтому $\prod_{p\in\pi(G)} O_p(G) \subseteq F(G)$. Обратно, если P — силовская p-подгруппа группы $F(G)$, то P *char* $F(G)$ и P нормальна в G, поэтому $P \leq O_p(G)$ и $F(G) \subseteq \prod_{p\in\pi(G)} O_p(G)$.

3. Если $\alpha \in \mathrm{Aut}G$, то $\alpha(F(G)) \triangleleft G$ и $\alpha(F(G))$ нильпотентна, поэтому $F(G)\alpha(F(G)) = F(G)$ по 1 и $F(G)$ *char* G.

Лемма 4.21. *1)* $\Phi(G) \leq F(G)$*; если* G *разрешима и* $G \neq E$*, то* $\Phi(G) \neq F(G)$*;*

2) $F(G/\Phi(G)) = F(G)/\Phi(G)$;

3) если $N \cdot\!\triangleleft\, G$*, то* $F(G) \leq C_G(N)$*; если, кроме того,* N *абелева, то* $N \leq Z(F(G))$.

□ 1. Поскольку подгруппа Фраттини $\Phi(G)$ — нильпотентная нормальная подгруппа группы G, то $\Phi(G) \leq F(G)$. Пусть G — разрешимая неединичная группа. Тогда $G/\Phi(G)$ разрешима и неединична. Пусть $A/\Phi(G) \cdot\!\triangleleft\, G/\Phi(G)$. Так как $A/\Phi(G)$ — p-группа для некоторого простого p, то по следствию теоремы 3.24, с. 113, подгруппа A нильпотентна и $A \leq F(G)$. Следовательно, $F(G) \neq \Phi(G)$.

2. Если $F(G/\Phi(G)) = K/\Phi(G)$, то K — нильпотентная нормальная в G подгруппа по теореме 3.24, с. 113, поэтому $K \leq F(G)$ и $F(G/\Phi(G)) \leq F(G)/\Phi(G)$. Обратное включение следует из определения подгруппы Фиттинга.

3. Для минимальной нормальной подгруппы N либо $N \cap F(G) = E$, либо $N \leq F(G)$. Если $N \cap F(G) = E$, то $NF(G) = N \times F(G)$ и $F(G) \leq C_G(N)$. Если $N \leq F(G)$, то N — элементарная абелева p-группа для некоторого простого p. Так как $Z = Z(F(G))$ *char* $F(G)$, то $Z \triangleleft G$. С другой стороны, $N \cap Z \neq E$ по теореме 3.12, с. 106, поэтому $N \leq Z$.

Теорема 4.22. $O_p\big(C_G(F(G))F(G)/F(G)\big) = E$ *для* *любого $p \in \pi(G)$. В частности, если G разрешима, то $C_G(F(G)) \leq F(G)$.*

$\square$ Пусть $F = F(G)$, $C = C_G(F)$. Так как $C \lhd G$ по лемме 1.53, с. 43, то $CF/F \lhd G/F$. Предположим, что $O_p(CF/F) \neq E$ для некоторого $p \in \pi(G)$ и пусть $A/F \cdot\!\lhd G/F$, $A/F \leq O_p(CF/F)$. Ясно, что $A = (C \cap A)F$ и $A \cap C \lhd G$. Пусть P — силовская p-подгруппа группы $A \cap C$. Так как $A/F = (A \cap C)F/F \simeq A \cap C/C \cap F = A \cap C/Z(F)$ — p-группа, то $A \cap C = PZ(F)$, а поскольку $P \leq C$, то $N_G(P) \geq F$ и $P \lhd A \cap C$. Теперь, $A \cap C$ — нильпотентная нормальная подгруппа группы G и $A \cap C \leq F$. Таким образом, $A = (C \cap A)F = F$ и первое утверждение доказано. Если G разрешима, то CF/F разрешима, поэтому $CF/F = E$ и $C \leq F$. $\boxtimes$

Говорят, что подгруппа H группы G *дополняема* в G, если существует такая подгруппа K, что $G = HK$ и $H \cap K = E$. В этом случае подгруппу K называют *дополнением* к подгруппе H в группе G.

Теорема 4.23. *Если H — нильпотентная нормальная подгруппа группы G и $H \cap \Phi(G) = E$, то H дополняема в группе G.*

$\square$ По условию $H \leq F(G)$, а по теореме 4.4, с. 116, коммутант $H' \leq \Phi(H)$. По теореме 3.22, с. 113, подгруппа Фраттини $\Phi(H) \leq \Phi(G)$, а по условию $H \cap \Phi(G) = E$. Поэтому $H' = E$ и H абелева. Пусть T — добавление к H в G. По лемме 3.21, с. 112, $H \cap T \leq \Phi(T)$. Поскольку пересечение $H \cap T$ нормально в T и в H, то $H \cap T$ нормально в G и по теореме 3.22, с. 113, $H \cap T \leq \Phi(G) \cap H = E$. Следовательно, $H \cap T = E$ и T — дополнение к H в G.

Теорема 4.24. *Фактор-группа $F(G)/\Phi(G)$ есть прямое произведение абелевых минимальных нормальных подгрупп группы $G/\Phi(G)$.*

$\square$ Предположим вначале, что $\Phi(G) = E$ и обозначим через F подгруппу Фиттинга $F(G)$. По теореме 4.4, с. 116, коммутант $F' \leq \Phi(F)$. Но $F \lhd G$, значит $\Phi(F) \leq \Phi(G) = E$ по теореме 3.22, с. 113. Поэтому $F' = E$ и F абелева. Пусть T — прямое произведение абелевых минимальных нормальных подгрупп группы G наибольшего порядка. Тогда $T \leq F$ и по теореме 4.23 существует подгруппа S такая, что $G = [T]S$. По тождеству Дедекинда $F = [T](F \cap S)$. Но F абелева, поэтому $F = T \times (F \cap S)$, а так как $F \cap S \lhd S$, то $F \cap S \lhd G$. По выбору T пересечение $F \cap S = E$ и $F = T$.

Пусть теперь $\Phi(G) \neq E$ и $\overline{G} = G/\Phi(G)$. По лемме 4.21 $F(\overline{G}) = F(G)/\Phi(G)$. Так как $\Phi(\overline{G}) = E$, то для $\overline{G}$ утверждение уже доказано.

Следствие. *В разрешимой группе с единичной подгруппой Фраттини подгруппа Фиттинга есть прямое произведение минимальных нормальных подгрупп.*

Теорема 4.25. *Подгруппа Фиттинга совпадает с пересечением централизаторов главных факторов группы.*

☐ Пусть

$$D = \cap\{C_G(H/K) \mid H/K\text{— главный фактор } G\}.$$

По следствию леммы 2.24, с. 73, подгруппа D нормальна в G. Если $E = A_0 < A_1 < \ldots < A_{a-1} < A_a = G$ — главный ряд группы G, то $E = D \cap A_0 \leq D \cap A_1 \leq \ldots \leq D \cap A_{a-1} \leq D \cap A_a = D$ — нормальный ряд группы D. Так как подгруппа D содержится в каждой подгруппе $C_G(A_i/A_{i-1})$, то $[D \cap A_i, D] \leq D \cap [A_i, D] \leq D \cap A_{i-1}$ для $i = 1, \ldots, a$. По теореме 4.11, с. 119, подгруппа D нильпотентна, поэтому $D \leq F(G)$.

Проверим обратное включение. Пусть H/K — главный фактор группы G. Так как $H/K \cdot\!\lhd G/K$, $F(G)K/K \lhd G/K$, то по лемме 2.36, с. 82, либо $(H/K) \cap (F(G)K/K) = E$, либо $H/K \leq F(G)K/K$. В первом случае $H \cap F(G) \leq K$, поэтому $[H, F(G)] \leq H \cap F(G) \leq K$ и $F(G) \leq C_G(H/K)$. Во втором случае из нильпотентности подгруппы $F(G)K/K$ по лемме 4.21 получаем, что $(H/K) \leq Z(F(G)K/K)$. Снова $F(G) \leq C_G(H/K)$. Таким образом, $F(G) \leq D$ и $F(G) = D$.

Лемма 4.26. $F(G_1 \times G_2) = F(G_1) \times F(G_2)$.

☐ Пусть $G = G_1 \times G_2$. Ясно, что $F(G_1) \times F(G_2) \leq F(G)$ и $F(G) \cap G_i = F(G_i)$, $i = 1, 2$. Так как $G_1F(G)/G_1 \lhd G/G_1 \simeq G_2$, то $G_1F(G)/G_1 \simeq F(G)/F(G_1)$ и $F(G)/F(G_1)$ изоморфна нормальной нильпотентной подгруппе группы G_2. Поэтому $\mid F(G)/F(G_1) \mid \leq \mid F(G_2) \mid$ и $F(G_1 \times G_2) = F(G_1) \times F(G_2)$. $\boxtimes$

Пусть G — группа и пусть

$F_0(G) = E$,

$F_1(G) = F(G)$,

$F_2(G)/F_1(G) = F(G/F_1(G)), \ldots,$

$F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G)), \ldots.$

Ясно, что $E = F_0(G) \leq F_1(G) \leq F_2(G) \leq \ldots.$

В разрешимой неединичной группе подгруппа Фиттинга отлична от единичной подгруппы по лемме 4.21. Поэтому для разрешимой группы существует натуральное n такое, что $F_n(G) = G$. *Нильпотентной длиной* разрешимой группы G называют наименьшее n, для которого $F_n(G) = G$. Нильпотентную длину разрешимой группы G обозначают через $n(G)$. Таким образом, если группа G разрешима и $n = n(G)$, то

$$E = F_0(G) \; < \; F_1(G) \; < \; \ldots \; < \; F_{n-1}(G) \; < \; F_n(G) = G,$$

где $F_i(G)/F_{i-1}(G) = F(G/F_{i-1}(G))$. Поэтому построенный ряд нормальный и его факторы $F_i(G)/F_{i-1}(G)$ нильпотентны.

Ясно, что $n(G) = 1$ тогда и только тогда, когда группа G нильпотентна.

$n(S_3) = 2; \;\; n(A_4) = 2; \;\; n(S_4) = 3.$

Непосредственно из определения нильпотентной длины вытекает

Лемма 4.27. *Пусть G — разрешимая группа. Тогда:*

1) $n(G/F(G)) = n(G) - 1$;

2) $n(G/F_i(G)) = n(G) - i$.

Лемма 4.28. *1. Если G — разрешимая группа, то длина любого нормального ряда группы G с нильпотентными факторами не меньше, чем $n(G)$.*

2. Нильпотентная длина разрешимой группы совпадает с длиной самого короткого нормального ряда с нильпотентными факторами.

$\square$ 1. Применим индукцию по порядку группы G. Пусть

$$E = H_0 \; < \; H_1 \; < \; \ldots < \; H_{t-1} \; < \; H_t = G$$

— нормальный ряд группы G с нильпотентными факторами. Так как H_1 — нормальная нильпотентная подгруппа группы G, то $H_1 \leq F(G) = F_1(G)$ и $n(G/F) = n(G)-1$. Здесь $F = F(G)$. Фактор-группа $\overline{G} = G/F$ имеет порядок меньше, чем порядок группы G и обладает рядом

$$E = \overline{H}_0 = \overline{H}_1 \leq \overline{H}_2 \leq \ldots \leq \overline{H}_{t-1} \leq \overline{H}_t = \overline{G},$$

где $\overline{H}_i = H_iF/F$. Ясно, что это нормальный ряд, его длина $f \leq t-1$ и его факторы

$$\overline{H}_i/\overline{H}_{i-1} = (H_iF/F)\big/(H_{i-1}F/F) \simeq H_iF/H_{i-1}F \simeq$$

$$\simeq H_i/H_{i-1}(H_i \cap F) \simeq (H_i/H_{i-1})\big/(H_{i-1}(H_i \cap F)/H_{i-1})$$

нильпотентны. По индукции $t-1 \geq f \geq n(G/F) = n(G)-1$ и $t \geq n(G)$.

2. Утверждение следует из следует из 1.

Лемма 4.29. *Пусть G — разрешимая группа. Тогда:*

1) если $H \leq G$, то $n(H) \leq n(G)$;

2) если $K \lhd G$, то $n(G/K) \leq n(G)$;

3) если N_1 и $N_2 \lhd G$, то $n(N_1N_2) = \max\{n(N_1), n(N_2)\}$; в частности, если G_1 и G_2 — разрешимые группы, то $n(G_1 \times G_2) = \max\{n(G_1), n(G_2)\}$;

4) $n(G) = n(G/\Phi(G))$.

□ Пусть $n = n(G)$ и $F_i = F_i(G)$. Тогда $E = F_0 < F_1 < \ldots < F_{n-1} < F_n = G$.

1. Пусть $H_i = H \cap F_i$. Тогда ряд

$$E = H_0 \leq H_1 \leq \ldots \leq H_{n-1} \leq H_n = H$$

будет нормальным рядом с нильпотентными факторами $H_i/H_{i-1} = H \cap F_i\big/H \cap F_{i-1} \simeq (H \cap F_i)F_{i-1}\big/F_{i-1} \leq F_i/F_{i-1}$. По лемме 4.28 $n(H) \leq n = n(G)$.

2. Пусть $K \lhd G$ и $\overline{F}_i = F_iK/K$. Тогда ряд

$$E = \overline{F}_0 \leq \overline{F}_i \leq \ldots \overline{F}_{n-1} \leq \overline{F}_n = G/K$$

будет нормальным рядом группы G/K с нильпотентными факторами

$$\overline{F}_i/\overline{F}_{i-1} = (F_iK/K)\big/(F_{i-1}K/K) \simeq F_iK/F_{i-1}K \simeq$$

$$\simeq F_i\big/F_{i-1}(F_i \cap K) \simeq (F_i/F_{i-1})\big/(F_{i-1}(F_i \cap K)/F_{i-1}).$$

По лемме 4.28 $n(G/K) \leq n = n(G)$.

3. Ясно, что $F(N_1)F(N_2) \leq F(N_1N_2)$. Обозначим $D = F(N_1N_2)$. Тогда $n(N_1N_2/D) = n(N_1N_2) - 1$ по лемме 4.27, а по индукции

$$n(N_1N_2/D) = \max\{n(N_1D/D), n(N_2D/D)\} \leq$$
$$\leq \max\{n(N_1) - 1, n(N_2) - 1\} = \max\{n(N_1), n(N_2)\} - 1.$$

Поэтому $n(N_1N_2) \leq \max\{n(N_1), n(N_2)\}$. Так как $\max\{n(N_1), n(N_2)\} \leq n(N_1N_2)$ по 1, то имеем

$$n(N_1N_2) = \max\{n(N_1), n(N_2)\}.$$

4. Положим $\Phi = \Phi(G)$. По лемме 4.21 для неединичной разрешимой группы G имеем $\Phi \neq F$ и $F(G/\Phi) = F_1(G/\Phi) = F/\Phi = F_1/\Phi$. Поэтому $n(G) = n(G/\Phi)$. ⊠

Следующая теорема принадлежит К. Дёрку и опубликована в его работе: Doerk K., Über die nilpotente Länge maximaler Untergruppen bei endlichen auflösbaren Gruppen // Rend. Sem. Mat. Univ. Padova. 1994. Vol. 91. P.19–21.

Теорема 4.30. *Если U — максимальная подгруппа разрешимой группы G, то $n(U) = n(G) - i$, где $i \in \{0, 1, 2\}$.*

□ Воспользуемся индукцией по порядку группы G. Пусть N — минимальная нормальная подгруппа группы G. Если $N \not\subseteq U$, то $U \simeq G/N$ и $n(U) = n(G/N) = n(G) - i$, причем $i = 0$, если $N \neq F(G)$, и $i = 1$, если $N = F(G)$. Поэтому можно предположить, что все минимальные нормальные подгруппы группы G содержатся в U. По индукции

$$n(U/N) = n(G/N) - i, \ i \in \{0, 1, 2\}. \tag{4.3}$$

Если группа G содержит две различные минимальные нормальные подгруппы, то $n(G/N) = n(G)$, $n(U) = n(U/N)$, и из (4.3) получаем, что теорема справедлива. Следовательно, можно считать, что группа G содержит в точности одну минимальную нормальную подгруппу.

Предположим, что $N \leq \Phi(G)$. Тогда $N \neq F(G)$ по лемме 4.21, поэтому $n(G) = n(G/N)$. Если $N \neq F(U)$, то $n(U) = n(U/N)$ и остается применить равенство (4.3). Если $N = F(U)$, то $n(U) = n(U/N) + 1$ и из (4.3) получаем, что $n(U) = n(G) - i + 1, \ i \in \{0, 1, 2\}$, т.е. $n(U) = n(G)$ или

$n(U) = n(G) - 1$.

Итак, можно считать, что $\Phi(G) = E$ и $N = F(G)$ по следствию теоремы 4.24. Поэтому $n(G) = n(G/N)+1$. Если $n(U) > n(U/N)$, то из (4.3) получаем $n(U) > n(G)-1-i$, $i \in \{0, 1, 2\}$, и теорема доказана. Пусть $n(U) = n(U/N)$, т.е. $N \neq F(U)$. Считаем, что N — p-группа. Ясно, что $F(U)$ — p-группа, а $F_2(G)/N$ — p'-группа. Допустим, что $F_2(G) \leq U$. Тогда $F(U)/N$ и $F_2(G)/N$ — неединичные нормальные подгруппы в U/N, поэтому $E \neq F(U)/N \leq C_{G/N}(F_2(G)/N)$. Но $C_{G/N}(F_2(G)/N) \leq F_2(G)/N$ по теореме 4.22. Поскольку $F(U)/N$ — p-группа, а $F_2(G)/N$ — p'-группа, то имеем противоречие. Следовательно, $F_2(G) \not\subseteq U$. Теперь $G = UF_2(G)$ и $n(G) - 2 = n(G/F_2(G)) = n(U/U \cap F_2(G)) \leq n(U/N) = n(U)$, поэтому теорема доказана полностью.

Все три значения $i \in \{0, 1, 2\}$ в теореме 4.30 имеют место. Значение $i = 0$ выполняется на любой нильпотентной неединичной группе. Значение $i = 1$ выполняется на группе S_3 с максимальной подгруппой $\langle(12)\rangle$. Значение $i = 2$ выполняется на группе S_4, у которой силовская 2-подгруппа максимальна.

Если фактор-группа $G/F(G)$ нильпотентна, то группу G называют *метанильпотентной.*

Теорема 4.31. *1. В разрешимой группе подгруппа Фраттини совпадает с пересечением максимальных подгрупп, не содержащих подгруппу Фиттинга.*

2. В разрешимой ненильпотентной группе пересечение максимальных подгрупп, содержащих подгруппу Фиттинга, метанильпотентно.

□ Обозначим через $\Phi_{\overline{F}}(G)$ пересечение всех максимальных подгрупп группы G, не содержащих $F(G)$, а через $\Phi_F(G)$ пересечение максимальных подгрупп группы G, содержащих $F(G)$. Ясно, что подгруппы $\Phi_{\overline{F}}(G)$ и $\Phi_F(G)$ характеристические в группе G и $\Phi(G) = \Phi_F(G) \cap \Phi_{\overline{F}}(G)$.

1. В фактор-группе $G/\Phi(G)$ подгруппа Фиттинга $F(G/\Phi(G)) = F(G)/\Phi(G)$ по лемме 4.21, поэтому $\Phi_{\overline{F}}(G/\Phi(G)) = \Phi_{\overline{F}}(G)/\Phi(G)$. Предположим, что $\Phi_{\overline{F}}(G)/\Phi(G) \neq E$ и пусть $K/\Phi(G)$ — минимальная нор-

мальная подгруппа группы $G/\Phi(G)$, содержащаяся в $\Phi_{\overline{F}}(G)/\Phi(G)$. Так как подгруппа K нормальна в группе G и фактор-группа $K/\Phi(G)$ нильпотентна, то по теореме 3.24, с. 113, подгруппа K нильпотентна и $K \leq F(G)$. Но теперь $K \leq \Phi_F(G) \cap \Phi_{\overline{F}}(G) = \Phi(G)$, противоречие. Поэтому допущение неверно и $\Phi_{\overline{F}}(G)/\Phi(G) = E$, т.е. $\Phi_{\overline{F}}(G) = \Phi(G)$.

2. Пусть G — разрешимая ненильпотентная группа. Ясно, что $F(G) \leq \Phi_F(G)$ и $\Phi_F(G)/F(G) = \Phi(G/F(G))$. Поэтому $\Phi_F(G)$ метанильпотентна.

В неразрешимой группе $SL(2,5)$ центр, подгруппа Фраттини и подгруппа Фиттинга совпадают и имеют порядок 2. Поэтому в группе $SL(2,5)$ нет максимальных подгрупп, не содержащих подгруппу Фиттинга. Следовательно, утверждение 1 теоремы 4.31 в неразрешимых группах нарушается.

4.4. Теорема Шура–Цассенхауза

В этом параграфе доказывается теорема Шура–Цассенхауза, которая как и теорема Силова относится к фундаментальным результатам теории конечных групп.

Теорема 4.32 (Шура-Цассенхауза). *Пусть N — нормальная подгруппа группы G. Предположим, что $|N| = n$ и $|G : N| = m$ взаимно просты. Тогда в группе G существует подгруппа порядка m и любые две подгруппы порядка m в группе G сопряжены между собой.*

□ Заметим, что если m — примарное число, т.е. $m = p^i$ для некоторого простого p, то утверждение вытекает из теоремы Силова.

Будем следовать схеме доказательства этой теоремы в [28]. Вначале докажем теорему для абелевой подгруппы N.

1. Существование и сопряженность подгрупп порядка m в группе G, когда N — абелева подгруппа.

Пусть $Q = G/N$. Тогда каждый элемент $x \in Q$ является в группе G смежным классом по подгруппе N, поэтому $x = t_xN$, где $\{t_x \mid x \in Q\}$ — левая трансверсаль подгруппы N в группе G. Так как $t_xt_y \in t_xt_yN = t_xNt_yN = xy = t_{xy}N$, то существует элемент $c(x,y) \in N$ такой, что

$$t_xt_y = t_{xy}c(x,y). \tag{4.4}$$

Теперь, используя (4.4), для любых $x,y,z \in Q$ имеем: $(t_xt_y)t_z = t_{xy}c(x,y)t_z = t_{xy}t_zc(x,y)^{t_z} = t_{(xy)z}c(xy,z)c(x,y)^{t_z}$; $t_x(t_yt_z) = t_xt_{yz}c(y,z) = t_{x(yz)}c(x,yz)c(y,z)$. Поскольку $(t_xt_y)t_z = t_x(t_yt_z)$ и $t_{(xy)z} = t_{x(yz)}$, то

$$c(xy,z)c(x,y)^{t_z} = c(x,yz)c(y,z). \tag{4.5}$$

Равенство (4.5) справедливо для любых $x,y,z \in Q$.

Введем элемент $d(y) = \prod_{x\in Q} c(x,y)$. Ясно, что $d(y) \in N$. Поскольку $\mid Q \mid= m$ и N абелева, то из (4.5) получаем $d(z)d(y)^{t_z} = d(yz)c(y,z)^m$ или

$$d(yz) = d(y)^{t_z}d(z)c(y,z)^{-m}. \tag{4.6}$$

Так как $(n,m) = 1$, то отображение $g \mapsto g^m$, $g \in G$ является автоморфизмом группы G, см. пример в параграфе 2.2. Поэтому существует элемент $e(y) \in N$ такой, что $e(y)^m = d(y)^{-1}$. Теперь равенство (4.6) можно записать в виде: $e(yz)^{-m} = (e(y)^{-m})^{t_z}e(z)^{-m}c(y,z)^{-m} = (e(y)^{t_z}e(z)c(y,z))^{-m}$. Поэтому $e(yz) = e(y)^{t_z}e(z)c(y,z)$.

Введем элемент $s_x = t_xe(x) \in N$ и, используя (4.4), вычислим произведение: $s_ys_z = t_ye(y)t_ze(z) = t_yt_ze(y)^{t_z}e(z) = t_{yz}c(y,z)e(y)^{t_z}e(z) = t_{yz}e(yz) = s_{yz}$. Следовательно, отображение $\alpha : x \mapsto s_x$ является гомоморфизмом группы Q в группу G. Если $s_x = 1$ — единичный элемент группы G, то $t_xe(x) = 1$ и $t_x \in N$. В этом случае $x = t_xN = N$ — единичный элемент группы Q. Следовательно, α — инъекция и $Q \simeq \mathrm{Im}\alpha$ — подгруппа порядка m в группе G.

Итак, в случае, когда N — абелева подгруппа, существование подгруппы порядка m в группе G установлено.

Пусть теперь T и L — две подгруппы порядка m в группе G. Тогда $G = [N]T = [N]L$ и $Q = G/N \simeq T \simeq L$. При этих изоморфизмах $Q \to T$ и $Q \to L$ элемент $x \in Q$ переходит в элементы $t_x \in T$ и $l_x \in L$. Поэтому $T = \{t_x \mid$

$x \in Q;\ t_x t_y = t_{xy}\}$; $L = \{l_x \mid x \in Q;\ l_x l_y = l_{xy}\}$. Так как $x = t_x N = l_x N$, то существует элемент $a(x) \in N$ такой, что $l_x = t_x a(x)$. Поскольку $l_{xy} = t_{xy} a(xy)$ и $l_{xy} = l_x l_y = t_x a(x) t_y a(y) = t_{xy} a(x)^{t_y} a(y)$, то

$$a(xy) = a(x)^{t_y} a(y). \tag{4.7}$$

Введем элемент $b = \prod_{x \in Q} a(x)$. Из (4.7) получаем $b = b^{t_y} a(y)^m$. Так как $(n, m) = 1$, то существует элемент $c \in N$ такой, что $b = c^m$. Поэтому $c^m = c^{mt_y} a(y)^m$ или $c = c^{t_y} a(y)$ и $a(y) = cc^{-t_y}$. Теперь $l_y = t_y a(y) = t_y c^{-t_y} c = t_y t_y^{-1} c^{-1} t_y c = c^{-1} t_y c$. Отсюда $L = \{l_y \mid y \in Q\} = \{c^{-1} t_y c \mid y \in Q\} = c^{-1} T c$.

Таким образом, если N — абелева подгруппа, то подгруппы порядка m существуют и сопряжены между собой.

2. Существование подгрупп порядка m в группе G.

Воспользуемся индукцией по порядку группы G. Пусть p — простое число, делящее порядок подгруппы N, и P — силовская p-подгруппа из N. Положим $L = N_G(P)$ и $Z = Z(P)$. Тогда $L \le N_G(Z) = M$, т.к. Z — характеристическая подгруппа в P. По лемме Фраттини $G = NL$ и $G = NM$. Поэтому для подгруппы $N_1 = N \cap M$ получаем, что $\mid M : N_1 \mid = \mid G : N \mid = m$. Поскольку $Z \ne E$, то можно применить индукцию к фактор-группе M/Z. Пусть X/Z — подгруппа порядка m в группе M/Z, тогда $M = XN_1, \quad X \cap N_1 = Z$. Так как $\mid X : Z \mid = m$ взаимно просто с $\mid Z \mid$ и Z — абелева подгруппа, то X имеет подгруппу порядка m по 1.

Итак, в любом случае в группе G существует подгруппа порядка m.

3. Сопряженность в группе G подгрупп порядка m, когда фактор-группа G/N разрешима.

Обозначим через π множество простых делителей числа m и положим $R = O_\pi(G)$. Пусть H и K — две подгруппы из G порядка m. Тогда RH и RK являются π-подгруппами группы G, поэтому $R \le H \cap K$. Если $R \ne E$, то по индукции H/R и K/R сопряжены в G/R, поэтому подгруппы H и K сопряжены в группе G.

Пусть $R = E$ и $L/N \cdot\lhd G/N$. По условию фактор-группа G/N разрешима, поэтому L/N является элементарной абелевой p-подгруппой для некоторого простого $p \in \pi$. Пересечение $L \cap H$ будет силовской p-подгруппой в L поскольку $(L \cap H) \simeq (L \cap H)N/N \leq L/N$ и $| L : L \cap H |=| HL : H |=| G : H |= n$ есть p'-число. Аналогично, $L \cap K$ будет силовская p-подгруппой в L, поэтому $L \cap H = (L \cap K)^g = L \cap K^g$ для некоторого $g \in L$. Пусть $S = L \cap H$. Тогда $S \lhd \langle H, K^g \rangle = J$.

Если $J = G$, то S — нормальная π-подгруппа группы G, что противоречит равенству $O_\pi(G) = E$. Поэтому J — собственная подгруппа группы G. По индукции подгруппы H и K^g сопряжены в J. Следовательно, подгруппы H и K сопряжены в G.

4. Сопряженность в группе G подгрупп порядка m, когда подгруппа N разрешима.

Так как N/N' абелева и $N' \lhd G$, то подгруппы HN'/N' и KN'/N' сопряжены в группе G/N' по 1. Поэтому $H^g \leq KN' < G$ для некоторого $g \in G$. Но теперь подгруппы H^g и K сопряжены в KN' по индукции. Следовательно, подгруппы H и K сопряжены в G.

5. Сопряженность в группе G подгрупп порядка m.

Так как числа n и m взаимно просты, то одно из них нечетное и согласно теореме 4.19, с. 125, либо N, либо G/N разрешима. Следовательно, любые две подгруппы порядка m сопряжены в группе G.

Следствие. *Пусть выполняются условия теоремы 4.32. Если натуральное число m_1 делит m, то каждая подгруппа порядка m_1 содержится в некоторой подгруппе порядка m.*

□ Пусть H и H_1 — подгруппы порядков m и m_1 соответственно. Тогда $G = HN$ и $H_1N = (H_1N) \cap (HN) = ((H_1N) \cap H)N$, откуда следует, что $| (H_1N) \cap H |=| H_1N : N |=| H_1 |= m_1$. Теперь H_1 и $(H_1N) \cap H$ — две подгруппы порядка m_1 в группе H_1N порядка m_1n. По теореме 4.32 $H_1 = \big((H_1N) \cap H\big)^g \leq H^g$ для некоторого $g \in G$. ⊠

В качестве приложения теоремы 4.32 приведем одно свойство подгруппы Фраттини произвольной конечной группы.

Теорема 4.33. $\pi(G) = \pi(G/\Phi(G))$.

$\square$ Ясно, что $\pi(G/\Phi(G)) \subseteq \pi(G)$. Предположим, что существует простое $p \in \pi(G)$ такое, что $p \notin \pi(G/\Phi(G))$. Через P обозначим силовскую p-подгруппу группы G. Тогда $P \leq \Phi(G)$ и $P \lhd G$. По теореме 4.32 существует подгруппа H такая, что $G = [P]H$. Имеем противоречие со следствием 2 теоремы 3.20, с. 111. Поэтому допущение неверно и $\pi(G) = \pi(G/\Phi(G))$.

Следствие. *Если $K \lhd G$ и H — добавление к K, то $\pi(H) = \pi(G/K)$.*

$\square$ По лемме 3.21, с. 112, группа $G = HK$ и $H \cap K \leq \Phi(H)$. Так как $G/K \simeq H/H \cap K$, то $\pi(G/K) = \pi(H)$ по теореме 4.33.

4.5. Холловы подгруппы разрешимых групп

Пусть $\mathbb{P}$ — множество всех простых чисел, а π — некоторое множество простых чисел, т.е. $\pi \subseteq \mathbb{P}$. Дополнение к π во множестве $\mathbb{P}$ обозначим через π', т.е. $\pi' = \mathbb{P} \setminus \pi$.

Наряду с множеством π будем использовать функцию $\pi(m)$ — множество всех простых чисел, делящих натуральное число m. Если G — группа, то вместо $\pi(\mid G \mid)$ условимся писать $\pi(G)$. Например, $\pi(S_5) = \{2, 3, 5\}$.

Зафиксируем множество простых чисел π. Если $\pi(m) \subseteq \pi$, то число m называется *π-числом.*

Подгруппа H группы G называется *π-подгруппой*, если $\mid H \mid$ есть π-число. Подгруппа H называется *π-холловой* подгруппой, если $\mid H \mid$ есть π-число, а индекс $\mid G : H \mid$ есть π'-число. Таким образом, π-холлова подгруппа — это такая π-подгруппа, индекс которой не делится на простые числа из π.

Подгруппа H группы G называется *холловой* подгруппой, если H — π-холлова подгруппа для некоторого множества $\pi \subseteq \mathbb{P}$. Другими словами, H — холлова подгруппа тогда и только тогда, когда $(\mid H \mid, \mid G : H \mid) = 1$.

Через $\mathrm{Hall}_\pi(G)$ обозначим совокупность π-холловых подгрупп группы G. Если $\pi = \{p\}$, то $\mathrm{Hall}_\pi(G) = \mathrm{Syl}_p(G)$ — совокупность силовских p-подгрупп группы G и по теореме Силова множество $\mathrm{Syl}_p(G)$ непусто для любой неединичной группы G и любого $p \in \pi(G)$.

p'-Холлову подгруппу, если она существует в группе G, называют *p-дополнением.*

Лемма 4.34. *Пусть $H \in Hall_\pi(G)$, M и $N \lhd G$. Тогда справедливы следующие утверждения:*

1) $\alpha(H) \in Hall_\pi(G)$, для любого $\alpha \in AutG$; в частности, $H^g \in Hall_\pi(G)$, для любого $g \in G$;

2) $HN/N \in Hall_\pi(G/N)$;

3) $H \cap N \in Hall_\pi(N)$;

4) $H \cap MN = (H \cap M)(H \cap N) \in Hall_\pi(MN)$.

□ Утверждения 1) и 2) очевидны.

3) Так как H — π-подгруппа, то $H \cap N$ — π-подгруппа по теореме Лагранжа. Кроме того, $HN/N \simeq H/H \cap N$, откуда $\mid HN : H \mid = \mid N : H \cap N \mid = \mid G : H \mid / \mid G : HN \mid$ — π'-число, т.е. $H \cap N$ — π-холлова подгруппа в N.

4) $H \cap MN$, $H \cap M$, $H \cap N$ — π-холловы подгруппы в MN, M и N, кроме того, $(H \cap M)(H \cap N) \leq H \cap MN$. Так как $\pi(H \cap M) \cup \pi(H \cap N) = \pi(H \cap MN)$, то $(H \cap M)(H \cap N) = H \cap MN$.

Теорема 4.35. *Пусть G — разрешимая группа и π — множество простых чисел. Тогда справедливы следующие утверждения:*

1) π-холловы подгруппы в группе G существуют;

2) любые две π-холловы подгруппы группы G сопряжены между собой;

3) каждая π-подгруппа группы G содержится в некоторой π-холловой подгруппе.

□ Применим индукцию по порядку группы G. Если $G = E$, то теорема верна. Предположим, что $G \neq E$ и N — минимальная нормальная подгруппа группы G. По теореме 4.14, с. 122, подгруппа N — элементарная абелева p-группа для некоторого простого p.

1) По индукции в группе G/N существует π-холлова подгруппа H/N. Если $p \in \pi$, то H — π-холлова подгруппа группы G. Пусть $p \notin \pi$. По теореме Шура–Цассенхауза в

H существует подгруппа U такая, что $H=[N]U$. Легко проверить, что U — π-холлова подгруппа группы G.

2) Пусть H_1 и $H_2 \in \mathrm{Hall}_\pi(G)$. По лемме 4.34 подгруппы H_1N/N и H_2N/N — π-холловы в G/N. По индукции они сопряжены в G/N, т.е. существует $gN \in G/N$ такой, что $(H_2N/N)^{gN} = H_1N/N$, откуда $H_2^gN = H_1N$. Если $p \in \pi$, то $H_2^gN = H_1N = H_1 = H_2^g$. Если $p \notin \pi$, то $[N]H_2^g = [N]H_1$ и подгруппы H_1 и H_2^g сопряжены в $[N]H_1$ по теореме Шура–Цассенхауза.

3) Пусть U — π-подгруппа группы G и H π-холлова в G. Можно считать, что $UN/N \leq HN/N$. Если $p \in \pi$, то $UN \leq H$ и $U \leq H$. Пусть $p \notin \pi$. Тогда $[N]U \leq [N]H$ и остается применить следствие теоремы 4.32, с. 133.

Теорема 4.36. *Если группа G содержит три разрешимые подгруппы H_1,H_2 и H_3 попарно взаимно простых индексов, то G разрешима*

□ Пусть P — минимальная нормальная подгруппа группы H_1. Тогда P — элементарная абелева p-подгруппа для некоторого простого p. Так как $(\mid G:H_2 \mid, \mid G:H_3 \mid) = 1$, то можно считать, что p не делит $\mid G:H_2 \mid$ и силовская p-подгруппа S из H_2 является силовской подгруппой группы G. По теореме Силова $P \subseteq S^g$ для некоторого $g \in G$. Теперь $G = H_1H_2^g$ и $P \subseteq H_1 \cap H_2^g$. Если x — произвольный элемент группы G, то $x = ab$, где $a \in H_1$, $b \in H_2^g$ и $P^x = P^b \subseteq H_2^g$. Следовательно, $P^G = \langle P^x \mid x \in G\rangle \subseteq H_2^g$. Так как P^G — разрешимая нормальная в G подгруппа, то к фактор-группе G/P^G применима индукция, по которой G/P^G разрешима. Теперь G разрешима.

Следствие. *Если в группе G существует p-дополнение для всех $p \in \pi(G)$, то группа G разрешима.*

□ Если $\mid \pi(G) \mid > 2$, то группа G разрешима по теореме 4.36. Если $\mid \pi(G) \mid = 2$, то группа G разрешима по теореме 4.18, с. 125. Если $\mid \pi(G) \mid = 1$, то группа G разрешима по лемме 4.12, с. 121.

4.6. Примитивные группы

Группа называется *примитивной* если она содержит максимальную подгруппу с единичным ядром. В примитивной группе максимальная подгруппа с единичным ядром называется *примитиватором.*

Лемма 4.37. *1. Простая неабелева группа примитивна и любая ее максимальная подгруппа является примитиватором.*

2. Нильпотентная группа примитивна тогда и только тогда, когда она имеет простой порядок.

□ 1. Очевидно.

2. В нильпотентной группе все максимальные подгруппы нормальны. Если G — примитивная нильпотентная группа, то только единичная подгруппа E может быть примитиватором. Но если E — максимальная подгруппа группы G, то по теореме Силова G имеет простой порядок. Обратно, каждая группа простого порядка всегда примитивна.

Лемма 4.38. *1. Если $M <\cdot G$, то $G/Core_G M$ примитивна и $M/Core_G M$ — её примитиватор.*

2. Если $K \lhd G$ и G/K примитивна, то в группе G существует максимальная подгруппа M такая, что $K = Core_G M$.

□ 1. Подгруппа $\overline{M} = M/Core_G M$ максимальна в $\overline{G} = G/Core_G M$, а из того, что $Core_G M$ — наибольшая нормальная подгруппа группы G, содержащаяся в M, следует, что $Core_{\overline{G}} \overline{M} = E$ и $\overline{G}$ примитивна с примитиватором $\overline{M}$.

2. Пусть $K \lhd G$ и $\overline{G} = G/K$ примитивна. Пусть $\overline{M}$ — примитиватор группы $\overline{G}$. По лемме 3.17, с. 110, существует максимальная подгруппа M группы G такая, что $\overline{M} = M/K$. Поскольку $Core_{\overline{G}} \overline{M} = E$, то $Core_G M = K$.

Лемма 4.39. *Если M — максимальная подгруппа группы G и N — неединичная нормальная подгруппа группы G такая, что $M \cap N = E$, то N — минимальная нормальная подгруппа.*

□ Произведение MN является подгруппой группы G, отличной от M. Поэтому $MN = G$ и $|N| = |G : M|$. Если N_1 — минимальная нормальная подгруппа группы G, содержащаяся в N, то опять $MN_1 = G$ и $|N_1| = |G : M|$. Теперь $|N_1| = |N|$ и $N_1 = N$.

Теорема 4.40. *В примитивной группе подгруппа Фиттинга либо единична, либо минимальная нормальная подгруппа. В частности, в разрешимой примитивной неединичной группе подгруппа Фраттини единична, а подгруппа Фиттинга — минимальная нормальная подгруппа.*

□ Пусть G — примитивная группа, M — её примитиватор, $F = F(G) \neq E$ и $K = F \cap M$. Так как $Core_G M = E$, то F не содержится в M, поэтому K — собственная в F подгруппа. По теореме 3.12, с. 106, $N_F(K) \neq K$, а так как $K \triangleleft M$ и $G = MK$, то $K \triangleleft G$. Но теперь $K \leq Core_G M = E$ и F — минимальная нормальная подгруппа по лемме 4.39.

Если G — разрешимая примитивная неединичная группа, то $\Phi(G)$ — собственная подгруппа в $F(G)$, поэтому $\Phi(G) = E$.

Следствие. *В примитивной группе неединичная нильпотентная нормальная подгруппа совпадает с подгруппой Фиттинга и является минимальной нормальной подгруппой.*

Теорема 4.41. *Пусть G — примитивная группа и M — её примитиватор. Тогда справедливо одно из следующих утверждений:*

1) группа G содержит единственную минимальную нормальную подгруппу N, причем $N = C_G(N)$ и $G = [N]M$;

2) группа G содержит единственную минимальную нормальную подгруппу N, причем $C_G(N) = E$ и $G = NM$;

3) группа G содержит точно две минимальные нормальные подгруппы N_1 и N_2, причем $G = [N_1]M = [N_2]M$, $N_i = C_G(N_{3-i})$, $i = 1, 2$ и $N_1 \simeq N_2 \simeq N_1N_2 \cap M$. Кроме того, если V — собственная подгруппа группы G такая, что $VN_1 = VN_2 = G$, *то V — максимальная подгруппа группы G, $Core_G V = E$ и $V \cap N_1 = V \cap N_2 = E$.*

$\square$ Пусть K — произвольная неединичная нормальная подгруппа примитивной группы G с примитиватором M. Так как $Core_G M = E$, то K не содержится в M и $G = MK$. Поскольку $C = C_G(K) \lhd G$, то $C \cap M \lhd M$. Кроме того, $K \leq C_G(C \cap M) \leq N_G(C \cap M)$, поэтому $C \cap M \lhd G$. Теперь $C \cap M \subseteq Core_G M = E$ и если $C \neq E$, то $G = [C]M$ и C — минимальная нормальная в G подгруппа по лемме 4.39. Таким образом, если K — произвольная неединичная нормальная подгруппа в G, то

$$G = MK, \quad C = C_G(K) = E \qquad (4.8),$$

или

$$G = [C]M, \quad C \cdot\!\lhd G. \qquad (4.9)$$

Предположим вначале, что $F = F(G) \neq E$. По теореме 4.40 подгруппа F — минимальная нормальная в G подгруппа. Теперь F абелева по следствию теоремы 2.39, с. 84, и $F = C_G(F)$ по (4.9). Если H — другая минимальная нормальная подгруппа группы G, то $H \cap F = E$ и $HF = H \times F$, т.е. $H \leq C_G(F) = F$, противоречие. Поэтому, F — единственная минимальная нормальная подгруппа и имеем случай 1 из заключения теоремы.

Пусть $F(G) = E$ и в G единственная минимальная нормальная подгруппа N. По следствию теоремы 2.39, с. 84, подгруппа N есть прямое произведение изоморфных простых неабелевых групп, в частности, $Z(N) = E$. Теперь $C_G(N) \cap N = Z(N) = E$ и по свойству (4.9) подгруппа $C_G(N) = E$. По свойству (4.8) группа $G = MN$ и имеем случай 2 из заключения теоремы.

Пусть теперь $F(G) = E$ и в группе G имеются две различные минимальные нормальные подгруппы N_1 и N_2. Тогда $N_1 \cap N_2 = E$, $\quad N_1N_2 = N_1 \times N_2$. Поэтому $N_1 \leq C_G(N_2)$ и по свойству (4.9) $N_1 = C_G(N_2)$. Аналогично, $N_2 = C_G(N_1)$. Из (4.9) также следует, что $G = [N_1]M = [N_2]M$. Если допустить, что существует третья минимальная нормальная подгруппа N_3, то $N_3 \leq C_G(N_1) = N_2$, $\quad N_3 \leq C_G(N_2) = N_1$, что противоречит друг другу. Значит в группе G точно две минимальные нормальные подгруппы.

Пусть теперь V — собственная подгруппа группы G такая, что $VN_1 = VN_2 = G$. Предположим, что H — максимальная в G подгруппа, содержащая V. Если $K = Core_G H \neq E$, то либо $N_1 \leq K$, либо $N_2 \leq K$, что противоречит равенствам $HN_1 = HN_2 = G$. Значит, $Core_G H = E$ и к H применимы свойства (4.8) и (4.9). Поэтому $N_1 \cap H = N_2 \cap H = E$, значит $V \cap N_1 = V \cap N_2 = E$, а из равенств $|N_1| = |G : V| = |G : H|$ следует, что $V = H$ — максимальная в G подгруппа.

Далее, $N_1N_2 = N_1N_2 \cap N_iM = N_i(N_1N_2 \cap M)$, поэтому $N_{3-i} \simeq N_1N_2/N_i = N_i(N_1N_2 \cap M)/N_i \simeq N_1N_2 \cap M/N_1N_2 \cap M \cap N_i = N_1N_2 \cap M$. Итак, $N_1 \simeq N_2 \simeq N_1N_2 \cap M$.

Следствие. *В примитивной группе не более двух минимальных нормальных подгрупп.*

Обозначим через $\mathcal{P}$ класс всех примитивных групп. Разобьем его на три подкласса:

$\mathcal{P}_1$ — класс примитивных групп с абелевой минимальной нормальной подгруппой;

$\mathcal{P}_2$ — класс примитивных групп с единственной неразрешимой минимальной нормальной подгруппой;

$\mathcal{P}_3$ — класс примитивных групп с двумя неразрешимыми минимальными нормальными подгруппами.

Класс $\mathcal{P}_i$ состоит из всех групп, соответствующих заключению (i) теоремы 4.41. Эта теорема утверждает, что $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_3$. Все три класса не пусты. Например, $S_3 \in \mathcal{P}_1$; A_5, $S_5 \in \mathcal{P}_2$; $[A_5 \times A_5]Z_2 \in \mathcal{P}_3$.

Для разрешимых примитивных групп имеет место только случай 1 теоремы 4.41, т.е. каждая разрешимая примитивная группа принадлежит $\mathcal{P}_1$.

Теорема 4.42. *Пусть G — разрешимая неединичная примитивная группа и M — её примитиватор. Тогда:*

1) группа G имеет единственную минимальную нормальную подгруппу N, причем $N = C_G(N)$ и $G = [N]M$;

2) если p делит $|N|$, то $O_p(M) = E$;

3) все дополнения к подгруппе N в группе G сопряжены между собой.

$\square$ 1. Утверждение следует из теоремы 4.41. В частности, N — p-группа для некоторого простого p.

2. Пусть $K/N = O_p(G/N)$. Тогда K — нормальная p-подгруппа группы G, поэтому $K \subseteq O_p(G) \leq F(G)$. Но по теореме 4.40 подгруппа $F(G) = N$, поэтому $K/N = E$ и $O_p(G/N) \simeq O_p(M) = E$.

3. Пусть M и H — два дополнения к подгруппе N в группе G. В G/N выберем минимальную нормальную подгруппу L/N. По 2 подгруппа L/N — q-группа, $q \neq p$, поэтому $L = [N]L_q$, где L_q — силовская q-подгруппа группы L. Из того, что $G = [N]M = LM$ следует, что $L \cap M$ — силовская q-подгруппа в L. Аналогично, $G = [N]H = LH$ и $L \cap H$ — силовская q-подгруппа в L. По теореме Силова $L \cap M = (L \cap H)^l$, $l \in L$. Но $L \cap M \lhd M$, поэтому $N_G(L \cap M) = M$. Аналогично, $N_G(L \cap H) = H$. Так как нормализаторы сопряженных подгрупп сопряжены, то $M = H^l$.

Теорема 4.43. *В разрешимой группе максимальные подгруппы сопряжены тогда и только тогда, когда их ядра равны.*

$\square$ Пусть G — разрешимая группа, H и M — максимальные подгруппы. Предположим, что $H = M^y$, $y \in G$. Тогда $Core_G H = \cap_{x \in G} H^x = \cap_{x \in G} M^{xy} = Core_G M$.

Обратно, пусть $Core_G H = Core_G M$. Тогда $G/Core_G H$ — примитивная группа с примитиваторами $H/Core_G H$, $M/Core_G M$. По теореме 4.42 эти подгруппы сопряжены в $G/Core_G H$, поэтому H и M сопряжены в группе G.

Теорема 4.44. *1. Группа $G \in \mathcal{P}_1$ тогда и только тогда, когда в G существует единственная минимальная нормальная подгруппа N, причем N абелева и N не содержится в $\Phi(G)$.*

2. Разрешимая группа примитивна тогда и только тогда, когда она содержит самоцентрализуемую минимальную нормальную подгруппу.

$\square$ 1. Если $G \in \mathcal{P}_1$, то из теоремы 4.41 следует, что в группе G существует единственная минимальная нормальная подгруппа N, причем $N = C_G(N)$ и $G = [N]M$, где M — примитиватор группы G. Из того, что $N = C_G(N)$, следует, что N абелева. Из того, что $G = [N]M$, следует, что N не содержится в $\Phi(G)$.

Обратно, пусть N — единственная минимальная нормальная подгруппа, причем N абелева и N не содержится в $\Phi(G)$. Тогда существует максимальная подгруппа M такая, что N не содержится в M. Теперь $MN = G$, а так как $M \cap N \lhd M$, $M \cap N \lhd N$, то $M \cap N \lhd G$. Из минимальности N следует, что $M \cap N = E$, а из того, что N — единственная минимальная нормальная подгруппа заключаем, что $Core_G M = E$ и примитивна.

2. Если G — разрешимая примитивная группа, то $G \in \mathcal{P}_1$ и по теореме 4.41 G содержит самоцентрализуемую минимальную нормальную подгруппу.

Обратно, пусть разрешимая группа G содержит минимальную нормальную подгруппу N и $N = C_G(N)$. По лемме 4.21, с. 126, $F(G) \leq C_G(N) = N$, теперь $\Phi(G) = E$ и $F(G) = N$. Поскольку $\Phi(G) = E$, то существует максимальная в G подгруппа M такая, что N не содержится в M. Теперь $G = MN$, а так как $M \cap N \lhd M$, $M \cap N \lhd N$, то $M \cap N \lhd G$ и из минимальности N следует, что $M \cap N = E$. Поскольку $N = C_G(N)$, то $Core_G M = E$ и G примитивна.

4.7. Сверхразрешимые группы

Группа называется *сверхразрешимой*, если она обладает нормальным рядом с циклическими факторами.

Лемма 4.45. *1. Каждая подгруппа и каждая фактор-группа сверхразрешимой группы сверхразрешимы.*

2. Прямое произведение сверхразрешимых групп является сверхразрешимой группой.

3. Сверхразрешимая группа разрешима.

☐ 1. Пусть группа G сверхразрешима. Тогда группа

G обладает нормальным рядом с циклическими факторами:

$$G = G_0 \geq G_1 \geq \ldots \geq G_{r-1} \geq G_r = E, \qquad (4.10)$$

$G_i \lhd G$ и фактор-группы G_i/G_{i+1} циклические для всех i. Пусть $U \leq G$ и $U_i = U \cap G_i$. Тогда U имеет ряд

$$U = U_0 \geq U_1 \geq \ldots \geq U_{r-1} \geq G_r = E, \qquad (4.11)$$

причем $U_i = U \cap G_i \lhd U$, для всех i. Далее

$U_{i-1}/U_i = U \cap G_{i-1}/U \cap G_i \simeq (U \cap G_{i-1})G_i/G_i \leq G_{i-1}/G_i$ и фактор-группа U_{i-1}/U_i циклическая. Итак, ряд (4.11) нормальный и его факторы циклические. Поэтому подгруппа U сверхразрешима.

Пусть $N \lhd G$. Рассмотрим ряд

$$G/N \geq G_1N/N \geq \ldots \geq G_{r-1}N/N \geq G_rN/N = E. \qquad (4.12)$$

Ясно, что $G_iN/N \lhd G/N$ для всех i, поэтому ряд (4.12) нормальный. Далее, $G_{i-1}N/N/G_iN/N \simeq G_{i-1}N/G_iN \simeq G_{i-1}(G_iN)/G_iN \simeq G_{i-1}/G_{i-1} \cap G_iN = G_{i-1}/G_i(G_{i-1} \cap N) \simeq G_{i-1}/G_i/G_i(G_{i-1} \cap N)/G_i$, поэтому факторы ряда (4.12) циклические и фактор-группа G/N сверхразрешима.

2. Пусть G и H — сверхразрешимые группы. Тогда группы G и H обладают нормальными рядам с циклическими факторами:

$$G = G_0 \geq G_1 \geq \ldots \geq G_{r-1} \geq G_r = E,$$
$$H = H_0 \geq H_1 \geq \ldots \geq H_{s-1} \geq H_s = E,$$

с циклическими факторами $G_{i-1}/G_i,\ H_{i-1}/H_i$. Рассмотрим прямое произведение $G \times H$ и построим ряд $G \times H = G_0 \times H \geq G_1 \times H \geq \ldots \geq G_{r-1} \times H \geq G_r \times H = H_0 \geq H_1 \ldots \geq H_{s-1} \geq H_s$. Этот ряд нормальный и его факторы циклические.

3. Пусть группа G сверхразрешима. Тогда группа G обладает нормальным рядом (4.10) с циклическими факторами. Так как G_{r-1} циклическая, то G_{r-1} разрешима. Так как G_{r-2}/G_{r-1} и G_{r-1} циклические, то они разрешимы, поэтому G_{r-2} разрешима по лемме 4.13, с. 121. Теперь G_{r-3}/G_{r-2} и G_{r-2} разрешимы, значит и G_{r-3} разрешима

по лемме 4.13, с. 121, и т.д. Через конечное число шагов получаем, что группа G разрешима.

Лемма 4.46. *1. Если группа G содержит нормальную циклическую подгруппу K и фактор-группа G/K сверхразрешима, то G сверхразрешима.*

2. Если фактор-группа $G/Z(G)$ сверхразрешима, то группа G сверхразрешима.

3. Нильпотентная группа сверхразрешима.

□ 1. Так как G/K сверхразрешима, то имеется нормальный ряд $G/K = G_0/K \geq G_1/K \geq \ldots \geq G_r/K = E$ с циклическими факторами $G_{i-1}/K/G_i/K$. Рассмотрим ряд

$$G = G_0 \geq G_1 \geq \ldots \geq G_{r-1} \geq G_r \geq K \geq E. \tag{4.13}$$

Так как $G_i/K \lhd G/K$, то $G_i \lhd G$ и ряд (4.13) нормальный. Кроме того, факторы $G_{i-1}/G_i \simeq G_{i-1}/K/G_i/K$ циклические для $i = 1, \ldots, r$. Далее, K — циклическая группа. Значит ряд (4.13) нормальный с циклическими факторами и группа G сверхразрешима.

2. Пусть $Z = Z(G)$. Так как G/Z сверхразрешима, то имеется нормальный ряд $G/Z = G_0/Z \geq G_1/Z \geq \ldots \geq G_r/Z = E$ с циклическими факторами $G_{i-1}/Z/G_i/Z$. Поскольку в абелевой группе максимальные подгруппы имеют простые индексы, то группа Z обладает рядом $Z = Z_0 \geq Z_1 \geq \ldots \geq Z_m = E$ с факторами Z_j/Z_{j+1} простых порядков. Рассмотрим ряд

$$\begin{aligned} G = G_0 \geq G_1 \geq \ldots \geq G_{r-1} \geq G_r \geq Z = \\ = Z_0 \geq Z_1 \geq \ldots \geq Z_m = E. \end{aligned} \tag{4.14}$$

Так как $G_i/Z \lhd G/Z$, то $G_i \lhd G$. Поскольку все подгруппы из центра группы нормальны в группе, то ряд (4.14) нормальный. Кроме того, факторы $G_{i-1}/G_i \simeq G_{i-1}/Z/G_i/Z$ циклические для $i = 1, \ldots, r$, а факторы Z_j/Z_{j+1}, $j = 0, \ldots, m-1$ имеют простые порядки. Значит ряд (4.14) нормальный с циклическими факторами и группа G сверхразрешима.

3. Воспользуемся индукцией по порядку группы. Пусть G — нильпотентная группа и $K \cdot\!\lhd G$. Тогда K име-

ет простой порядок. По индукции фактор-группа G/K сверхразрешима. Теперь G сверхразрешима по 1.

Лемма 4.47. *Группа сверхразрешима тогда и только тогда, когда она обладает главным рядом с факторами простых порядков.*

□ Пусть G сверхразрешима. Тогда она имеет нормальный ряд (4.10) с циклическими факторами G_{i-1}/G_i. Так как $G_{i-1}/G_i \lhd G/G_i$ и G_{i-1}/G_i циклическая, то по лемме 2.9, с. 63, все подгруппы в G_{i-1}/G_i характеристические. Пусть $G_{i-1}^{(1)}/G_i$ — подгруппа простого индекса в G_{i-1}/G_i. Тогда $G_{i-1}^{(1)}/G_i$ *char* $G_{i-1}/G_i \lhd G/G_i$, следовательно $G_{i-1}^{(1)}/G_i \lhd G/G_i$ по лемме 2.11, с. 64, и ряд $G = G_0 \geq G_1 \geq \ldots \geq G_{i-1} \geq G_{i-1}^{(1)} \geq G_i \geq \ldots \geq G_r = E$ нормальный с циклическим фактором $G_{i-1}/G_{i-1}^{(1)}$ простого порядка. Повторяя эти действия, через конечное число шагов придем к главному ряду с факторами простых порядков.

Обратно, если группа G имеет главный ряд с факторами простых порядков, то этот ряд будет нормальным, а его факторы циклическими. Значит группа G будет сверхразрешимой.

Теорема 4.48. *1. Максимальные подгруппы сверхразрешимой группы имеют простые индексы.*

2. В сверхразрешимой группе каждая минимальная нормальная подгруппа имеет простой порядок.

□ 1. Пусть G — сверхразрешимая группа и $M <\cdot\, G$. По лемме 4.47 группа G имеет главный ряд $G = G_0 \geq G_1 \geq \ldots \geq G_{r-1} \geq G_r = E$ с факторами простых порядков. Зафиксируем число i такое, что $G_i \leq M$, но $G_{i-1} \not\leq M$. Поскольку $M <\cdot\, G$ и $G_{i-1} \lhd G$, то $G = MG_{i-1}$ и $\mid G : M \mid = \mid G_{i-1} : M \cap G_{i-1} \mid$. Но $G_i \leq M \cap G_{i-1}$ и $\mid G_{i-1} : G_i \mid = p$, поэтому либо $G_i = M \cap G_{i-1}$, либо $M \cap G_{i-1} = G_{i-1}$. Поскольку, $G_{i-1} \not\leq M$, то $G_i = M \cap G_{i-1}$ и $\mid G : M \mid = p$.

2. Воспользуемся индукцией по порядку группы. Пусть $N \cdot\!\lhd G$. По лемме 4.47 в группе G существует ми-

нимальная нормальная подгруппа K простого порядка. Если $N \cap K \neq E$, то $N = K$ и утверждение справедливо. Пусть $N \cap K = E$. По лемме 2.36, с. 82, подгруппа NK/K — минимальная нормальная подгруппа фактор-группы G/K. По индукции $\mid N \mid = \mid NK/K \mid$ — простое число.

Лемма 4.49. *Если G — сверхразрешимая группа и p — наибольший простой делитель порядка G, то силовская p-подгруппа группы G нормальна.*

□ Воспользуемся индукцией по порядку группы G. Пусть $N \cdot\!\lhd G$. Тогда $\mid N \mid = q$ — простое число по теореме 4.48. Фактор-группа G/N сверхразрешима. По индукции, $G_pN/N \lhd G/N$, т.е. $G_pN \lhd G$. Если $p = q$, то $N \leq G_p$ и $G_pN = G_p \lhd G$. Пусть $p \neq q$, тогда $p > q$. Так как фактор-группа $G/C_G(N)$ по теореме 2.8, с. 62, изоморфна подгруппе группы $\mathrm{Aut}N$, которая по теореме 2.16, с. 66, является циклической группой порядка $(q-1)$, то $G_p \leq C_G(N)$ и $G_pN = G_p \times N$. Но теперь, G_p *char* $G_pN \lhd G$, следовательно $G_p \lhd G$. ⊠

Говорят, что группа G *дисперсивна,* если она обладает нормальным рядом, факторы которого изоморфны силовским подгруппам. Более точно, пусть φ — некоторое упорядочение множества простых чисел. Запись $p\varphi q$ означает, что p предшествует q в упорядочении φ, $p \neq q$. Группа G порядка $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ называется *φ-дисперсивной*, если $p_1\varphi p_2\varphi\dots\varphi p_n$ и для любого i группа G имеет нормальную подгруппу порядка $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_i^{\alpha_i}$, т.е. группа G имеет нормальный ряд

$$E < G_1 < G_2 < \ldots < G_{n-1} < G, \qquad (4.15)$$

где $|G_1| = p_1^{\alpha_1}, |G_2| = p_1^{\alpha_1}p_2^{\alpha_2}, \ldots, |G_i| = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_i^{\alpha_i}, \ldots, |G_{n-1}| = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_{n-1}^{\alpha_{n-1}}$. В этом случае, у ряда (4.15) факторы изоморфны силовским подгруппам: $G_1/E \simeq G_{p_1}, G_2/G_1 \simeq G_{p_2}, \ldots, G_n/G_{n-1} \simeq G_{p_n}$.

Если при этом упорядочение φ таково, что $p\varphi q$ влечет $p > q$, то φ-дисперсивная группа называется *дисперсивной по Оре. Дисперсивной* группой называют группу, являющуюся φ-дисперсивной для некоторого φ. Дисперсивная по Оре группа G p-замкнута для наибольшего $p \in \pi(G)$ и q-нильпотентна для наименьшего $q \in \pi(G)$.

Нильпотентная группа φ-дисперсивна при любом φ. S_3 дисперсивна по Оре. A_4 φ-дисперсивна, где $p\varphi q$ тогда и только тогда, когда $p < q$, но A_4 не дисперсивна по Оре. Прямое произведение $S_3 \times A_4$ является недисперсивной группой.

Лемма 4.50. *1. Подгруппа и фактор-группа φ-дисперсивной группы φ-дисперсивны.*

2. Прямое произведение φ-дисперсивных групп является φ-дисперсивной группой.

3. φ-Дисперсивные группы разрешимы.

4. Если $G/\Phi(G)$ φ-дисперсивна, то группа G φ-дисперсивна.

□ Утверждения 1–3 проверяются непосредственно на основе соответствующих определений.

4. Воспользуемся индукцией по порядку группы G. Пусть $\mid G \mid = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, $p_1 \varphi p_2 \varphi \ldots \varphi p_n$. Через P_i обозначим силовскую p_i-подгруппу группы G. По условию $P_1\Phi(G) \lhd G$, а по лемме Фраттини $G = N_G(P_1)\Phi(G)$. Теперь $P_1 \lhd G$ по следствию 1 теоремы 3.20, с. 111. Так как $\Phi(G)P_1/P_1 \subseteq \Phi(G/P_1)$, то фактор-группа G/P_1 φ-дисперсивна по индукции, поэтому группа G φ-дисперсивна.

Теорема 4.51. *Сверхразрешимая группа дисперсивна по Оре.*

□ Пусть G — сверхразрешимая группа, $\mid G \mid = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, $p_1 > p_2 > \ldots > p_n$. По лемме 4.49 силовская p_1-подгруппа $P_1 \lhd G$. Фактор-группа G/P_1 имеет порядок $p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ и по индукции фактор-группа G/P_1 дисперсивна по Оре. Значит, для любого i в группе G/P_1 имеется нормальная подгруппа H_i/P_1 порядка $p_2^{\alpha_2} \ldots p_i^{\alpha_i}$, $i = 2, \ldots, n$. Пусть $H_1 = P_1$. Теперь в группе G имеется нормальная подгруппа H_i порядка $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_i^{\alpha_i}$ для любого $i = 1, 2, \ldots, n$, т.е. G дисперсивна по Оре.

Теорема 4.52. *Коммутант сверхразрешимой группы нильпотентен.*

□ Воспользуемся индукцией по порядку группы G. Пусть $K \cdot\lhd G$. По индукции фактор-группа

$(G/K)'$ нильпотентна. Но по лемме 4.6, с. 117, $(G/K)' = G'K/K \simeq G'/G' \cap K$. Если K не содержится в G', то $G' \cap K = E$, т.к. $\mid K \mid= p$ — простое число и $G'K/K \simeq G'$ нильпотентна. Пусть $K \leq G'$. Поскольку $G/C_G(K)$ — циклическая группа порядка, делящего $p-1$, то $G' \leq C_G(K)$ и K содержится в центре G'. Теперь G' нильпотентна по лемме 3.15, с. 109.

Экспонентой группы называют наименьшее общее кратное порядков всех элементов этой группы.

Говорят, что группа G линейных преобразований пространства V действует *неприводимо* на V, если в пространстве V нет G-допустимых нетривиальных подпространств, т.е. подпространств, отличных от нулевого и всего V.

Лемма 4.53. *Пусть V — векторное пространство размерности $n \geq 1$ над полем $\mathbb{Z}_p$. Пусть G — абелева группа линейных преобразований пространства V экспоненты, делящей $(p-1)$. Если G действует неприводимо на V, то $n = 1$ и G циклическая.*

□ Пусть $g \in G$. Так как группа G имеет экспоненту $(p-1)$, то g является корнем многочлена $x^{p-1} - 1$. Этот многочлен над полем $\mathbb{Z}_p$ разлагается в произведение линейных многочленов, поэтому g имеет характеристический корень $\lambda \neq 0$ в $\mathbb{Z}_p$ и подпространство $W = \{v \mid vg = \lambda v\}$ ненулевое. Пусть $x \in G$ и $v \in W$. Тогда $vxg = vgx = \lambda vx$ и $vx \in W$. Значит W — ненулевое G-допустимое подпространство пространства V. Из неприводимости группы G следует, что $V = W$. Поэтому каждый элемент группы G индуцирует скалярное умножение на V, а из неприводимости G следует, что $n = 1$. Но теперь группа G изоморфна подгруппе мультипликативной группы поля $\mathbb{Z}_p$ и поэтому циклическая. ⊠

Пусть H и $K \lhd G$ и $K \leq H$. В лемме 2.24, с. 73, введена группа $C_G(H/K) = \langle g \in G \mid g^{-1}h^{-1}gh \in K,\ h \in H\rangle$, которая является нормальной подгруппой группы G и фактор-группа $G/C_G(H/K)$ изоморфна группе $\mathrm{Aut}_G(H/K)$. Ясно, что $C_G(H/K) = \langle g \in G \mid [g, H] \subseteq K\rangle$.

Теорема 4.54. *Пусть H/K — p-главный фактор группы G. Тогда и только тогда $\mid H/K \mid = p$, когда $Aut_G(H/K)$ — абелева группа экспоненты, делящей $p-1$.*

□ Если H/K — p-главный фактор группы G порядка p, то $\mathrm{Aut}_G(H/K)$ — абелева группа экспоненты, делящей $(p-1)$ по следствию леммы 2.24, с. 73.

Обратно, пусть $\mathrm{Aut}_G(H/K)$ — абелева группа экспоненты, делящей $(p-1)$. По теореме 2.50, с. 93, элементарную абелеву p-группу H/K порядка p^n можно рассматривать как векторное пространство размерности n над полем $\mathbb{Z}_p$, а группу автоморфизмов $\mathrm{Aut}_G(H/K)$ как группу линейных преобразований. Из того, что H/K — минимальная нормальная подгруппа в G/K следует, что $\mathrm{Aut}_G(H/K)$ действует неприводимо на H/K. Теперь по лемме 4.53 получаем, что $n = 1$, т.е. $\mid H/K \mid = p$.

Следствие. *Группа G сверхразрешима тогда и только тогда, когда для каждого простого p и каждого p-главного фактора H/K группы G группа $Aut_G(H/K)$ абелева экспоненты, делящей $(p-1)$.*

□ Если группа сверхразрешима, то все ее главные факторы имеют простые порядки. Это следует из леммы 4.47 и теоремы Жордана–Гельдера, см. теорему 2.23, с. 71. Теперь $\mathrm{Aut}_G(H/K)$ — абелева группа экспоненты, делящей $p-1$ по теореме 4.54.

Обратно, если для каждого p-главного фактора H/K группа $\mathrm{Aut}_G(H/K)$ абелева экспоненты, делящей $(p-1)$, то по теореме 4.54 каждый главный фактор имеет простой порядок и G сверхразрешима по лемме 4.47.

Теорема 4.55 (Хупперта). *Если в группе G все максимальные подгруппы имеют простые индексы, то группа G сверхразрешима.*

□ Воспользуемся индукцией по порядку группы G. Ясно, что условия теоремы наследуются всеми фактор-группами группы G. Если в группе G имеются две различные минимальные нормальные подгруппы N_1 и N_2, то G/N_i сверхразрешима по индукции. Так как $N_1 \cap N_2 = E$, то группа G изоморфна подгруппе прямого произведения $(G/N_1) \times (G/N_2)$ по лемме Ремака. Теперь по лемме 4.45

группа G сверхразрешима. Поэтому в дальнейшем считаем, что в группе единственная минимальная нормальная подгруппа.

Пусть p — наибольший простой делитель порядка группы G и G_p — её силовская p-подгруппа. Предположим, что G_p не нормальна в G. Тогда $N_G(G_p) \neq G$ и существует максимальная подгруппа M группы G, содержащая $N_G(G_p)$. По теореме Силова $\mid G : N_G(G_p) \mid = 1 + kp$; $\mid M : N_G(G_p) \mid = 1 + k_1 p$. Так как по условию теоремы $\mid G : M \mid = q$ — простое число, то из равенства $\mid G : N_G(G_p) \mid = \mid G : M \mid\mid M : N_G(G_p) \mid$ следует, что $q = \mid G : M \mid = 1 + p(k - k_1 q)$, что противоречит максимальности числа p. Поэтому допущение неверно, и $G_p \triangleleft G$. По индукции фактор-группа G/G_p сверхразрешима, поэтому группа G разрешима.

Пусть $N \cdot\!\triangleleft\, G$, $N \leq G_p$. Из того, что N — единственная минимальная нормальная подгруппа следует, что подгруппа Фиттинга $F(G)$ является p-группой. Если $N \not\subseteq \Phi(G)$, то существует максимальная подгруппа M в группе G такая, что $N \not\subseteq M$. Поэтому $G = NM$ и $N \cap M = E$ по лемме 2.36, с. 82. По условию $\mid G : M \mid = \mid N \mid = p$ и группа G сверхразрешима по лемме 4.46.

Следовательно, $N \leq \Phi(G)$. По лемме 4.21, с. 126, для фактор-группы $\overline{G} = G/N$ получаем, что $F(\overline{G}) = F(G)/N$ — p-группа, а по теореме 4.52 $(\overline{G})' \leq F(\overline{G})$. Отсюда следует, что $C_{\overline{G}}(\overline{A}/\overline{B}) = \overline{G}$ для каждого главного p'-фактора $\overline{A}/\overline{B}$ группы $\overline{G}$. По теореме 4.25, с. 128, подгруппа $F(\overline{G})$ совпадает с пересечением централизаторов главных факторов группы $\overline{G}$ порядка p. По лемме Ремака и теореме 2.16, с. 66, получаем, что $\overline{G}/F(\overline{G})$ — абелева группа экспоненты, делящей $(p-1)$. Поэтому $G/F(G)$ — абелева группа экспоненты, делящей $(p-1)$.

Так как $N \cdot\!\triangleleft G$ и $N \cap Z(F(G)) \neq E$, то $N \leq Z(F(G))$ и $F(G) \leq C_G(N)$. Теперь $G/C_G(N) \simeq (G/F(G))/(C_G(N)/F(G))$ и $G/C_G(N)$ — абелева группа экспоненты, делящей $(p-1)$. По теореме 4.54 N имеет порядок p и G сверхразрешима по лемме 4.46.

Следствие. *Если фактор-группа $G/\Phi(G)$ сверхразрешима, то и группа G сверхразрешима.*

$\square$ Пусть фактор-группа $G/\Phi(G)$ сверхразрешима. По теореме 4.48 все максимальные подгруппы в $G/\Phi(G)$ имеют простые индексы. Но теперь все максимальные подгруппы в G имеют простые индексы и G сверхразрешима по теореме 4.55.

Теорема 4.56. *Пусть G — разрешимая группа. Тогда и только тогда G сверхразрешима, когда для каждой максимальной подгруппы M группы G либо $F(G) \leq M$, либо $F(G) \cap M$ — максимальная подгруппа группы $F(G)$.*

$\square$ Пусть G сверхразрешима и $M <\cdot\, G$. Тогда $| G : M |$ — простое число. Если $F(G)$ не содержится в M, то $F(G)M = G$ и $| G : M |=| F(G) : F(G) \cap M |$ — простое число. Поэтому $F(G) \cap M <\cdot\, F(G)$.

Обратно, пусть G разрешима и для каждой максимальной подгруппы M группы G либо $F(G) \leq M$, либо $F(G) \cap M <\cdot\, F(G)$. Так как $F(G/\Phi(G)) = F(G)/\Phi(G)$ по лемме 4.21, с. 126, то условия теоремы переносятся на фактор-группу $G/\Phi(G)$. Если $\Phi(G) \neq E$, то по индукции $G/\Phi(G)$ сверхразрешима, поэтому по следствию теоремы 4.55 группа G сверхразрешима. Итак, $\Phi(G) = E$, $F(G) = N_1 \times \ldots \times N_t$ — прямое произведение минимальных нормальных подгрупп N_i группы G, $i = 1, \ldots, t$. Для каждого i существует максимальная подгруппа M_i группы G, такая, что $N_i \cap M_i = E$ и $G = [N_i]M_i$. По тождеству Дедекинда $F(G) = [N_i](F(G) \cap M_i)$, а по условию теоремы $F(G) \cap M_i <\cdot\, F(G)$. Из нильпотентности $F(G)$ следует, что $| N_i |=| F(G) : F(G) \cap M_i |= p_i$ — простое число. Теперь фактор-группа $G/C_G(N_i)$ абелева порядка, делящего $p_i - 1$, поэтому $G' \subseteq \cap_{i=1}^{t} C_G(N_i) \subseteq C_G(F(G)) \leq F(G)$.

Пусть теперь $M <\cdot\, G$. Если $M \geq F(G)$, то G/M абелева и $| G : M |$ — простое число. Если $F(G)$ не содержится в M, то $MF(G) = G$ и $| G : M |=| F(G) : F(G) \cap M |$ — простое число. По теореме 4.55 группа G сверхразрешима.

Следствие 1. *Пусть G — разрешимая группа. То-*

гда и только тогда группа G сверхразрешима, когда для любой максимальной подгруппы M группы G и любой нормальной подгруппы N группы G либо $M \geq N$, либо $M \cap N < \cdot\, N$.

$\Box$ Если G сверхразрешима, то все максимальные подгруппы имеют простые индексы и если M не содержит N, то $MN = G$ и $\mid G : M \mid = \mid N : N \cap M \mid$ — простое число и $N \cap M < \cdot\, N$.

Обратно, если для любой максимальной подгруппы M и любой нормальной подгруппы N либо $N \leq M$, либо $N \cap M < \cdot\, N$, то это верно и для подгруппы Фиттинга $F(G)$. По теореме 4.56 группа G сверхразрешима.

Следствие 2. *Тогда и только тогда разрешимая группа сверхразрешима, когда индекс любой максимальной подгруппы, не содержащей подгруппу Фиттинга, является простым числом.*

$\Box$ Если группа сверхразрешима, то индекс каждой максимальной подгруппы есть простое число по теореме 4.48.

Обратно, пусть G — разрешимая группа, у которой индекс любой максимальной подгруппы, не содержащей подгруппу Фиттинга, является простым числом. Если M — максимальная подгруппа группы G и $F(G) \nsubseteq M$, то $\mid G : M \mid = p$ — простое число. Теперь $G = MF(G)$ и $p = \mid G : M \mid = \mid F(G) : F(G) \cap M \mid$. Поэтому $F(G) \cap M$ — максимальная подгруппа в $F(G)$ и по теореме 4.56 группа G сверхразрешима.

Пусть $X = \mathbb{Z}_5 \oplus \mathbb{Z}_5 = \{(a, b) \mid a, b \in \mathbb{Z}_5\}$ — аддитивная элементарная абелева группа порядка 5^2. Группу X можно рассматривать как двумерное векторное пространство над полем $\mathbb{Z}_5$, она разлагается в прямую сумму двух своих подгрупп порядка 5: $X = \langle(1,0)\rangle \oplus \langle(0,1)\rangle$. Пусть Q — группа кватернионов, см. с. 90. $Q = \langle A, B \mid A^4 = B^4 = E, A^2 = B^2, B^{-1}AB = A^{-1}\rangle \subseteq SL(2, \mathbb{Z}_5)$, где A и B — матрицы над полем $\mathbb{Z}_5$:

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}; \quad B = \begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}.$$

В силу теоремы 2.50, с. 93, Q является группой автоморфизмов для X. По теореме 2.47, с. 87, существует группа $G = [X]Q$, она имеет порядок 200, а её подгруппы $H = [X]\langle A\rangle$; $K = [X]\langle B\rangle$ имеют индекс 2 в G. Поэтому H и $K \lhd G$. Так как

$$(1,0)\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix} = (2,0) = 2(1,0) \in \langle(1,0)\rangle,$$

то $\langle(1,0)\rangle \lhd H$. Таким образом, H содержит нормальную подгруппу $H_1 = \langle(1,0)\rangle$, фактор-группа по которой H/H_1 является полупрямым произведением нормальной подгруппы X/H_1 порядка 5 и циклической подгруппы порядка 4. Поэтому H сверхразрешима. Аналогично,

$$(1,2)\begin{pmatrix}0 & 4\\ 1 & 0\end{pmatrix} = (2,4) = 2(1,2) \in \langle(1,2)\rangle,$$

т.е. K содержит нормальную подгруппу $\langle(1,2)\rangle$, фактор-группа по которой является полупрямым произведением нормальной подгруппы порядка 5 и циклической порядка 4. Поэтому K сверхразрешима. Следовательно, G является произведением нормальных сверхразрешимых подгрупп H и K. Предположим, что G сверхразрешима. Тогда по лемме 4.49 и теореме 4.48 в G имеется нормальная подгруппа $\langle(x,y)\rangle$ порядка 5. Поэтому

$$(x,y)\begin{pmatrix}2 & 0\\ 0 & 3\end{pmatrix} = (2x,3y) \in \langle(x,y)\rangle,$$

$$(x,y)\begin{pmatrix}0 & 4\\ 1 & 0\end{pmatrix} = (y,4x) \in \langle(x,y)\rangle,$$

что возможно только при $x = y = 0$. Поэтому допущение неверно и G несверхразрешима.

Таким образом, существуют несверхразрешимые группы, являющиеся произведением нормальных сверхразрешимых подгрупп.

5. ПРОЕКТОРЫ И ИНЪЕКТОРЫ

5.1. Формации и классы Шунка

Будем рассматривать множества групп, т.е. множества, элементами которого являются группы. *Класс групп* — это множество групп, которое вместе с каждой своей группой содержит все ей изоморфные группы. За некоторыми классами закреплены стандартные обозначения:

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

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

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

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

$\mathfrak{E}$ — класс всех (конечных) групп.

Если π — некоторое множество простых чисел и $\mathfrak{X}$ — класс групп, то через $\mathfrak{X}_\pi$ обозначается класс всех π-групп из $\mathfrak{X}$. Ясно, что $\mathfrak{X}_\pi = \mathfrak{X} \cap \mathfrak{E}_\pi$. Группы из класса $\mathfrak{X}$ называют также $\mathfrak{X}$*-группами.*

Класс $\mathfrak{X}$ называется *наследственным классом* или *классом, замкнутым относительно подгрупп*, если выполняется следующее требование:

1) если $G \in \mathfrak{X}$ и $H \leq G$, то $H \in \mathfrak{X}$.

Класс $\mathfrak{X}$ называется *замкнутым относительно фактор-групп* или *гомоморфом*, если выполняется требование:

2) если $G \in \mathfrak{X}$ и $N \lhd G$, то $G/N \in \mathfrak{X}$.

Класс $\mathfrak{X}$ называется *замкнутым относительно прямых произведений*, если выполняется требование:

3) если $G_1 \in \mathfrak{X}$ и $G_2 \in \mathfrak{X}$, то $G_1 \times G_2 \in \mathfrak{X}$.

Класс $\mathfrak{X}$ называется *насыщенным*, если выполняется требование:

4) если $G/N \in \mathfrak{X}$, $N \leq \Phi(G)$, то $G \in \mathfrak{X}$.

Класс $\mathfrak{X}$ называется *замкнутым относительно подпрямых произведений* если выполняется требование:

5) если $G/N_1 \in \mathfrak{X}$ и $G/N_2 \in \mathfrak{X}$, то $G/N_1 \cap N_2 \in \mathfrak{X}$.

Формацией называется класс, замкнутый относительно фактор-групп и подпрямых произведений. Таким образом, для формации выполняются требования 2) и 5).

Формация называется *насыщенной*, если она является насыщенным классом, т.е. если для неё выполняется требование 4). Ясно, что класс групп, замкнутый относительно подпрямых произведений, будет замкнут и относительно прямых произведений. В частности, каждая формация замкнута относительно прямых произведений.

Теорема 5.1. *Класс групп, замкнутый относительно подгрупп, фактор-групп и прямых произведений, является формацией.*

□ Пусть для класса $\mathfrak{F}$ выполняются требования 1),2), 3). Необходимо проверить, что выполняется требование 5). Пусть $G/N_1 \in \mathfrak{F}$ и $G/N_2 \in \mathfrak{F}$. По лемме Ремака (лемма 2.33, с. 79,) фактор-группа $G/N_1 \cap N_2$ изоморфна подгруппе прямого произведения $G/N_1 \times G/N_2$. Так как выполняется требование 3), то $G/N_1 \times G/N_2 \in \mathfrak{F}$. Поскольку выполняется требование 1), то каждая подгруппа из прямого произведения также принадлежит $\mathfrak{F}$. В частности, $G/N_1 \cap N_2 \in \mathfrak{F}$.

$\mathfrak{A}$ — класс всех абелевых групп. Подгруппы и фактор-группы абелевых групп являются абелевыми группами. Прямые произведения абелевых групп, также являются абелевыми группами. Поэтому условия теоремы 5.1 для класса $\mathfrak{A}$ выполняются. Следовательно, $\mathfrak{A}$ — формация. Но эта формация не является насыщенной. Действительно, все группы порядка 4 абелевы, поэтому все они принадлежат $\mathfrak{A}$. В неабелевой группе Q кватернионов порядка 8 подгруппа Фраттини $\Phi(Q)$ имеет порядок 2, поэтому $Q/\Phi(Q) \in \mathfrak{A}$, но Q не содержится в $\mathfrak{A}$.

Для $\mathfrak{N}$ выполняются условия теоремы 5.1. Если $G/N \in \mathfrak{N}$, $N \leq \Phi(G)$, то $G \in \mathfrak{N}$ по следствию теоремы 3.24, с. 113. Поэтому $\mathfrak{N}$ — насыщенная формация.

Для $\mathfrak{U}$ выполняются условия теоремы 5.1, а по следствию теоремы 4.55, с. 152, $\mathfrak{U}$ — насыщенная формация.

Для $\mathfrak{S}$ выполняются условия теоремы 5.1, а из леммы 4.13, с. 121, следует, что выполняется требование 4). Поэтому $\mathfrak{S}$ — насыщенная формация.

Класс $\mathfrak{E}_\pi$ всех π-групп является формацией поскольку он замкнут относительно подгрупп, фактор-групп и прямых произведений. Если $G/\Phi(G) \in \mathfrak{E}_\pi$, то $\pi(G) = \pi(G/\Phi(G))$ по теореме 4.33, с. 137, поэтому $G \in \mathfrak{E}_\pi$ и $\mathfrak{E}_\pi$ — насыщенная формация.

Поскольку пересечение насыщенных формаций является насыщенной формацией, то насыщенными формациями являются следующие классы групп:

$\mathfrak{S}_\pi = \mathfrak{S} \cap \mathfrak{E}_\pi$ — класс всех разрешимых π-групп;

$\mathfrak{U}_\pi = \mathfrak{U} \cap \mathfrak{E}_\pi$ — класс всех сверхразрешимых π-групп;

$\mathfrak{N}_\pi = \mathfrak{N} \cap \mathfrak{E}_\pi$ — класс всех нильпотентных π-групп.

Класс $\mathfrak{X}$ называется *примитивно замкнутым классом*, если выполняется требование:

6) если все примитивные фактор-группы группы G принадлежат $\mathfrak{X}$, то $G \in \mathfrak{X}$.

В силу того, что примитивная фактор-группа может быть получена, как фактор-группа группы G по ядру некоторой максимальной подгруппы, то требование 6) эквивалентно следующему требованию:

6$'$) если $G/Core_G M \in \mathfrak{X}$ для всех $M <\cdot\, G$, то $G \in \mathfrak{X}$.

Классом Шунка называется класс групп, который одновременно замкнут относительно фактор-групп и является примитивно замкнутым классом. Таким образом, для класса Шунка выполняются требования 2) и 6).

Теорема 5.2. *Всякий класс Шунка является насыщенным классом.*

□ Предположим, что $\mathfrak{X}$ — класс Шунка и пусть N — нормальная подгруппа группы G, $N \leq \Phi(G)$ и $G/N \in \mathfrak{X}$. Требуется проверить, что $G \in \mathfrak{X}$. По лемме 3.18, с. 111, подгруппа Фраттини $\Phi(G)$ совпадает с пересечением ядер всех максимальных подгрупп, т.е. $\Phi(G) = \bigcap_{M<\cdot\, G} Core_G M$. Так как $N \leq \Phi(G)$, то $N \leq Core_G M$ для всех $M <\cdot\, G$. Следовательно, $G/N/Core_G M/N \simeq G/Core_G M \in \mathfrak{X}$ ввиду того, что $G/N \in \mathfrak{X}$ и $\mathfrak{X}$ — гомоморф. Теперь $G \in \mathfrak{X}$, поскольку класс $\mathfrak{X}$ примитивно замкнут.

Следствие. *Если класс Шунка $\mathfrak{X}$ является формацией, то $\mathfrak{X}$ — насыщенная формация.*

Теорема 5.3. *Насыщенная формация является классом Шунка.*

□ Пусть $\mathfrak{F}$ — насыщенная формация. Тогда для $\mathfrak{F}$ выполняются требования 2), 4) и 5). Надо показать, что для $\mathfrak{F}$ выполняется требование $6'$). Пусть $G/Core_G M \in \mathfrak{F}$ для всех $M < \cdot\, G$. По лемме 3.18, с. 111, подгруппа Фраттини $\Phi(G)$ совпадает с пересечением ядер всех максимальных подгрупп, т.е. $\Phi(G) = \bigcap_{M<\cdot\, G} Core_G M$. Так как $\mathfrak{F}$ — формация, то $G/\Phi(G) = G/\bigcap_{M<\cdot\, G} Core_G M \in \mathfrak{F}$, а т.к. $\mathfrak{F}$ насыщена, то $G \in \mathfrak{F}$.

Классы $\mathfrak{N}$; $\mathfrak{N}_\pi$, $\mathfrak{U}$; $\mathfrak{U}_\pi$; $\mathfrak{S}$; $\mathfrak{S}_\pi$, $\mathfrak{E}$; $\mathfrak{E}_\pi$ являются насыщенными формациями, следовательно они являются классами Шунка.

Поскольку класс $\mathfrak{A}$ всех абелевых групп является ненасыщенной Формацией, то он не является классом Шунка.

Теорема 5.4. *Класс всех разрешимых групп, у которых коммутанты имеют нечетные индексы, является классом Шунка и не является формацией.*

□ Вначале проверим, что класс $\mathfrak{X} = \{G \in \mathfrak{S} \mid 2$ не делит $\mid G : G' \mid\}$ является классом Шунка. Пусть $G \in \mathfrak{X}$ и $N \lhd G$. Так как $(G/N)' = G'N/N$, то $\mid G/N : G'N/N \mid = \mid G : G'N \mid = \mid G \mid\mid G' \cap N \mid / \mid G' \mid\mid N \mid = \mid G : G' \mid / \mid N : G' \cap N \mid$ и 2 не делит $\mid G/N : (G/N)' \mid$, т.е. $G/N \in \mathfrak{X}$. Пусть $G \in \mathfrak{S}$ и $G/Core_G M \in \mathfrak{X}$ для всех $M < \cdot\, G$. Предположим, что 2 делит $\mid G/G' \mid$. Тогда в группе G существует нормальная подгруппа K индекса 2. Ясно, что $K = Core_G K < \cdot\, G$ и $G/K \notin \mathfrak{X}$, противоречие. Таким образом, $\mathfrak{X}$ — класс Шунка.

Пусть $G = \langle a \rangle \times SL(2,3)$, $a^2 = e$. Группа $SL(2,3)$ имеет порядок 24, а ее центр имеет порядок 2, см. теорему 2.51, с. 93, и теорему 2.52, с. 94. Поэтому в группе $SL(2,3)$ имеется нормальная подгруппа $\langle b \rangle = Z(SL(2,3))$ порядка 2 и $SL(2,3)/\langle b \rangle \simeq A_4$ по теореме 2.54, с. 97. Подгруппа $\langle ab \rangle \lhd G$ и $G/\langle ab \rangle \simeq SL(2,3) \in \mathfrak{X}$. Кроме того, $G/\langle a \rangle \simeq SL(2,3) \in \mathfrak{X}$, но $G \simeq G/\langle a \rangle \cap \langle ab \rangle \notin \mathfrak{X}$. Поэтому $\mathfrak{X}$ не является формацией.

Теорема 5.5. *Если класс Шунка $\mathfrak{X}$ содержит неединичную р-группу, то $\mathfrak{X}$ содержит все р-группы.*

□ Предположим, что неединичная p-группа $P \in \mathfrak{X}$. В p-группах максимальные подгруппы нормальны и имеют простые индексы, т.е. если $P_1 < \cdot\, P$, то $P_1 \lhd P$ и $\mid P : P_1 \mid = p$. Так как $\mathfrak{X}$ — гомоморф, то $P/P_1 \in \mathfrak{X}$.

Следовательно в $\mathfrak{X}$ имеется группа порядка p. Допустим теперь, что G — произвольная p-группа. Рассмотрим произвольную максимальную подгруппу M группы G. Тогда для M справедливо: $M \triangleleft G$ и $\mid G/M \mid = p$. В этом случае $M = Core_G M$, $G/Core_G M \in \mathfrak{X}$. Так как $\mathfrak{X}$ — класс Шунка, то требование $6'$) из его определения позволяет заключить, что $G \in \mathfrak{X}$. ⊠

Характеристикой класса $\mathfrak{X}$ называется множество простых чисел p, для которых в $\mathfrak{X}$ имеется неединичная p-группа. Характеристику класса $\mathfrak{X}$ обозначают через $\chi(\mathfrak{X})$.

Теорема 5.6. *Если $\mathfrak{X}$ — класс Шунка, то $\mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$.*

☐ Предположим, что $G \in \mathfrak{X} \cap \mathfrak{N}$ и $p \in \pi(G)$. Тогда в нильпотентной группе G существует максимальная подгруппа M индекса p. Поскольку пересечение классов Шунка $\mathfrak{X}$ и $\mathfrak{N}$ вновь является классом Шунка, то $G/M \in \mathfrak{X} \cap \mathfrak{N}$ и $p \in \chi(\mathfrak{X})$. Поэтому $\pi(G) \subseteq \chi(\mathfrak{X})$ и $G \in \mathfrak{N}_{\chi(\mathfrak{X})}$, т.е. $\mathfrak{X} \cap \mathfrak{N} \subseteq \mathfrak{N}_{\chi(\mathfrak{X})}$.

Обратно, пусть $G \in \mathfrak{N}_{\chi(\mathfrak{X})}$. Рассмотрим произвольную максимальную подгруппу M группы G. Так как G нильпотентна, то M нормальна в G и $\mid G/M \mid = p$. Но $p \in \chi(\mathfrak{X})$, поэтому $G/M \in \mathfrak{X}$, а т.к. $\mathfrak{X}$ — класс Шунка, то $G \in \mathfrak{X}$ и $\mathfrak{N}_{\chi(\mathfrak{X})} \subseteq \mathfrak{X} \cap \mathfrak{N}$.

Следствие. *Если $\mathfrak{X}$ — насыщенная формация, то $\mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$.*

Пусть $\mathfrak{F}$ — формация и G — группа. Пересечение всех нормальных подгрупп группы G, фактор-группы по которым принадлежат $\mathfrak{F}$, обозначим через $G^{\mathfrak{F}}$ и назовем $\mathfrak{F}$-*корадикалом* группы G. Таким образом, $G^{\mathfrak{F}} = \bigcap_{N \triangleleft G,\ G/N \in \mathfrak{F}} N$.

Лемма 5.7. *Пусть $\mathfrak{F}$ — формация и G — группа. Тогда:*

1) если $N \triangleleft G$ и $G/N \in \mathfrak{F}$, то $G^{\mathfrak{F}} \leq N$;

2) $G/G^{\mathfrak{F}} \in \mathfrak{F}$;

3) $G^{\mathfrak{F}}$ — наименьшая нормальная подгруппа группы G, для которой $G/G^{\mathfrak{F}} \in \mathfrak{F}$;

4) $G \in \mathfrak{F}$ тогда и только тогда, когда $G^{\mathfrak{F}} = E$.

□ 1. Если $N \lhd G$ и $G/N \in \mathfrak{F}$, то по определению $\mathfrak{F}$-корадикала $G^{\mathfrak{F}} \le N$.

2. Из определения формации следует, что $G/G^{\mathfrak{F}} = G/(\bigcap_{N \lhd G,\ G/N \in \mathfrak{F}} N) \in \mathfrak{F}$.

3. Из 1 и 2 следует, что $G^{\mathfrak{F}}$ — единственная нормальная подгруппа группы G, для которой $G/G^{\mathfrak{F}} \in \mathfrak{F}$.

4. Если $G \in \mathfrak{F}$, то $G^{\mathfrak{F}} = E$. Если $G^{\mathfrak{F}} = E$, то $G \simeq G/E \in \mathfrak{F}$.

$G^{\mathfrak{A}} = G'$ — коммутант группы G.

Пусть $\mathfrak{X}$ — класс всех элементарных абелевых p-групп. По теореме 5.1 класс $\mathfrak{X}$ — формация. По лемме 3.25, с. 114, для каждой p-группы P подгруппа $P^{\mathfrak{X}}$ совпадает с подгруппой Фраттини группы P.

Лемма 5.8. *Пусть $\mathfrak{F}$ — формация, G — группа, $H \le G$ и $K \lhd G$. Тогда:*

1) $(G/K)^{\mathfrak{F}} = G^{\mathfrak{F}}K/K$;

2) если ψ — эпиморфизм G, то $\psi(G)^{\mathfrak{F}} = \psi(G^{\mathfrak{F}})$;

3) если $G = HK$, то $H^{\mathfrak{F}}K = G^{\mathfrak{F}}K$;

4) если $G = HK$ и $K \le G^{\mathfrak{F}}$, то $H^{\mathfrak{F}}K = G^{\mathfrak{F}}$.

□ 1. Пусть $(G/K)^{\mathfrak{F}} = N/K$. Тогда $(G/K)/(N/K) \simeq G/N \in \mathfrak{F}$ и $G^{\mathfrak{F}} \le N$ по лемме 5.7, поэтому $G^{\mathfrak{F}}K/K \le N/K$. С другой стороны, $(G/K)/(G^{\mathfrak{F}}K/K) \simeq G/G^{\mathfrak{F}}K \simeq (G/G^{\mathfrak{F}})/(G^{\mathfrak{F}}K/G^{\mathfrak{F}}) \in \mathfrak{F}$ т.к. $G/G^{\mathfrak{F}} \in \mathfrak{F}$ и $\mathfrak{F}$ — гомоморф. По лемме 5.7 $N/K \le G^{\mathfrak{F}}K/K$, т.е. $G^{\mathfrak{F}}K/K = N/K = (G/K)^{\mathfrak{F}}$.

2. Пусть ψ — эпиморфизм и $K = \mathrm{Ker}\psi$. Тогда $\psi(G) = G/K$ и $\psi(G)^{\mathfrak{F}} = (G/K)^{\mathfrak{F}} = G^{\mathfrak{F}}K/K = \psi(G^{\mathfrak{F}})$.

3. Пусть $H \le G$ и δ — естественный эпиморфизм группы G на G/K, т.е. $\delta : g \mapsto gK$, для всех $g \in G$. Так как $\mathrm{Ker}\delta = K$, $\delta(G) = G/K$ и $G = HK$, то $\delta(H) = HK/K = G/K = \delta(G)$. Поскольку $\delta(H^{\mathfrak{F}}) = H^{\mathfrak{F}}K/K$, то $\delta(G^{\mathfrak{F}}) = G^{\mathfrak{F}}K/K = (G/K)^{\mathfrak{F}} = \delta(G)^{\mathfrak{F}} = \delta(H)^{\mathfrak{F}} = \delta(H^{\mathfrak{F}}) = H^{\mathfrak{F}}K/K$, поэтому $G^{\mathfrak{F}}K/K = H^{\mathfrak{F}}K/K$ и $G^{\mathfrak{F}}K = H^{\mathfrak{F}}K$.

4. Если $K \le G^{\mathfrak{F}}$, то $H^{\mathfrak{F}}K = G^{\mathfrak{F}}K = G^{\mathfrak{F}}$. ⊠

Пусть $\mathfrak{X}$ — класс групп и $\mathfrak{F}$ — формация. *Корадикальным произведением* $\mathfrak{X}$ и $\mathfrak{F}$ называется класс

$$\mathfrak{X} \circ \mathfrak{F} = \{\ G \in \mathfrak{E} \ \mid \ G^{\mathfrak{F}} \in \mathfrak{X}\ \},$$

состоящий из всех групп, у которых $\mathfrak{F}$-корадикал принадлежит $\mathfrak{X}$.

Лемма 5.9. *Пусть $\mathfrak{X}$ — класс групп, $\mathfrak{F}$ — формация. Тогда:*

1) если $\mathfrak{X}$ — нормально наследственный класс, то $\mathfrak{X} \subseteq \mathfrak{X} \circ \mathfrak{F}$;

2) если $\mathfrak{X}$ содержит единичную группу (например, $\mathfrak{X}$ — непустой гомоморф), то $\mathfrak{F} \subseteq \mathfrak{X} \circ \mathfrak{F}$;

3) если $\mathfrak{X}$ и $\mathfrak{F}$ — формации, то группа $G \in \mathfrak{X} \circ \mathfrak{F}$ тогда и только тогда, когда $(G^{\mathfrak{F}})^{\mathfrak{X}} = E$.

□ 1. Если $G \in \mathfrak{X}$ и $\mathfrak{X}$ — нормально наследственный класс, то $G^{\mathfrak{F}} \in \mathfrak{X}$ и $G \in \mathfrak{X} \circ \mathfrak{F}$, т.е. $\mathfrak{X} \subseteq \mathfrak{X} \circ \mathfrak{F}$.

2. Если $G \in \mathfrak{F}$, то $G^{\mathfrak{F}} = E \in \mathfrak{X}$ и $G \in \mathfrak{X} \circ \mathfrak{F}$, т.е. $\mathfrak{F} \subseteq \mathfrak{X} \circ \mathfrak{F}$.

3. Пусть $\mathfrak{X}$ и $\mathfrak{F}$ — формации. Допустим, что $G \in \mathfrak{X} \circ \mathfrak{F}$. Тогда $G^{\mathfrak{F}} \in \mathfrak{X}$ и $(G^{\mathfrak{F}})^{\mathfrak{X}} = E$ по лемме 5.7. Обратно, если $(G^{\mathfrak{F}})^{\mathfrak{X}} = E$, то $G^{\mathfrak{F}} \in \mathfrak{X}$ и $G \in \mathfrak{X} \circ \mathfrak{F}$.

Теорема 5.10. *1. Если $\mathfrak{X}$ — гомоморф, а $\mathfrak{F}$ — формация, то $\mathfrak{X} \circ \mathfrak{F}$ — гомоморф.*

2. Если $\mathfrak{X}$ и $\mathfrak{F}$ — формации, то $\mathfrak{X} \circ \mathfrak{F}$ — формация.

3. Если $\mathfrak{X}$ и $\mathfrak{F}$ — наследственные формации, то $\mathfrak{X} \circ \mathfrak{F}$ — наследственная формация.

4. Если $\mathfrak{X}$ и $\mathfrak{F}$ — нормально наследственные формации, то $\mathfrak{X} \circ \mathfrak{F}$ — нормально наследственная формация.

□ 1. Пусть $G \in \mathfrak{X} \circ \mathfrak{F}$ и $N \lhd G$. Тогда $(G/N)^{\mathfrak{F}} = G^{\mathfrak{F}}N/N \simeq G^{\mathfrak{F}}/(G^{\mathfrak{F}} \cap N) \in \mathfrak{X}$, т.к. $G^{\mathfrak{F}} \in \mathfrak{X}$ и $\mathfrak{X}$ — гомоморф. Поэтому $G/N \in \mathfrak{X} \circ \mathfrak{F}$ и $\mathfrak{X} \circ \mathfrak{F}$ — гомоморф.

2. Пусть $\mathfrak{X}$ и $\mathfrak{F}$ — формации. По 1) произведение $\mathfrak{X} \circ \mathfrak{F}$ — гомоморф. Пусть $N_i \lhd G$, $G/N_i \in \mathfrak{X} \circ \mathfrak{F}$, $i = 1, 2$. Тогда $(G/N_i)^{\mathfrak{F}} = G^{\mathfrak{F}}N_i/N_i \simeq G^{\mathfrak{F}}/(G^{\mathfrak{F}} \cap N_i) \in \mathfrak{X}$. Так как $\mathfrak{X}$ — формация, то $(G/N_1 \cap N_2)^{\mathfrak{F}} = G^{\mathfrak{F}}(N_1 \cap N_2)/N_1 \cap N_2 \simeq G^{\mathfrak{F}}/(G^{\mathfrak{F}} \cap N_1 \cap N_2) \in \mathfrak{X}$ и $G/(N_1 \cap N_2) \in \mathfrak{X} \circ \mathfrak{F}$. Итак, $\mathfrak{X} \circ \mathfrak{F}$ — формация.

3. Пусть $\mathfrak{F}$ и $\mathfrak{X}$ — наследственные формации, $G \in \mathfrak{X} \circ \mathfrak{F}$ и $H \le G$. Тогда $HG^{\mathfrak{F}}/G^{\mathfrak{F}} \le G/G^{\mathfrak{F}} \in \mathfrak{F}$, поэтому $HG^{\mathfrak{F}}/G^{\mathfrak{F}} \in \mathfrak{F}$. Так как $HG^{\mathfrak{F}}/G^{\mathfrak{F}} \simeq H/(H \cap G^{\mathfrak{F}})$, то $H^{\mathfrak{F}} \le G^{\mathfrak{F}}$. Но $G^{\mathfrak{F}} \in \mathfrak{X}$, поэтому $H^{\mathfrak{F}} \in \mathfrak{X}$ и $H \in \mathfrak{X} \circ \mathfrak{F}$.

4. Пусть $\mathfrak{X}$ и $\mathfrak{F}$ — нормально наследственные формации. Пусть $G \in \mathfrak{X} \circ \mathfrak{F}$ и $N \lhd G$. Тогда $G^{\mathfrak{F}} \in \mathfrak{X}$. Рассмотрим подгруппу $K = NG^{\mathfrak{F}}$. Ясно, что $K \lhd G$. Поскольку, $K/G^{\mathfrak{F}} \lhd G/G^{\mathfrak{F}} \in \mathfrak{F}$, то $K/G^{\mathfrak{F}} \in \mathfrak{F}$ и $K/G^{\mathfrak{F}} = NG^{\mathfrak{F}}/G^{\mathfrak{F}} \simeq N/(N \cap G^{\mathfrak{F}}) \in \mathfrak{F}$, т.е. $N^{\mathfrak{F}} \leq N \cap G^{\mathfrak{F}}$. Так как $N \cap G^{\mathfrak{F}} \lhd G^{\mathfrak{F}} \in \mathfrak{X}$ и $\mathfrak{X}$ — нормально наследственная формация, то $N \cap G^{\mathfrak{F}} \in \mathfrak{X}$. Но $N^{\mathfrak{F}}$ нормальна в $N \cap G^{\mathfrak{F}}$, поэтому $N^{\mathfrak{F}} \in \mathfrak{X}$ и $N \in \mathfrak{X} \circ \mathfrak{F}$.

Теорема 5.11. *Пусть $\mathfrak{X}$, $\mathfrak{Y}$ и $\mathfrak{Z}$ — формации. Тогда:*

1) $G^{(\mathfrak{X}\circ\mathfrak{Y})} = (G^{\mathfrak{Y}})^{\mathfrak{X}}$ для любой группы G;

2) $(\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z} = \mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z})$.

□ 1. По теореме 5.10 произведение $\mathfrak{X}\circ\mathfrak{Y}$ — формация. Пусть $N = G^{(\mathfrak{X}\circ\mathfrak{Y})}$ — $\mathfrak{X} \circ \mathfrak{Y}$-корадикал группы G. Так как $G/N \in \mathfrak{X} \circ \mathfrak{Y}$, то $(G/N)^{\mathfrak{Y}} = G^{\mathfrak{Y}}N/N \simeq G^{\mathfrak{Y}}/(G^{\mathfrak{Y}} \cap N) \in \mathfrak{X}$, поэтому $(G^{\mathfrak{Y}})^{\mathfrak{X}} \leq N = G^{(\mathfrak{X}\circ\mathfrak{Y})}$.

Рассмотрим фактор-группу $G/(G^{\mathfrak{Y}})^{\mathfrak{X}}$. Так как $(G/(G^{\mathfrak{Y}})^{\mathfrak{X}})^{\mathfrak{Y}} = G^{\mathfrak{Y}}(G^{\mathfrak{Y}})^{\mathfrak{X}}/(G^{\mathfrak{Y}})^{\mathfrak{X}} \simeq G^{\mathfrak{Y}}/((G^{\mathfrak{Y}})^{\mathfrak{X}} \cap G^{\mathfrak{Y}}) = G^{\mathfrak{Y}}/(G^{\mathfrak{Y}})^{\mathfrak{X}} \in \mathfrak{X}$, то $G/(G^{\mathfrak{Y}})^{\mathfrak{X}} \in \mathfrak{X} \circ \mathfrak{Y}$ и $G^{(\mathfrak{X}\circ\mathfrak{Y})} \leq (G^{\mathfrak{Y}})^{\mathfrak{X}}$. Таким образом, $(G^{\mathfrak{Y}})^{\mathfrak{X}} = G^{(\mathfrak{X}\circ\mathfrak{Y})}$.

2. Из 1 следует, что $G^{(\mathfrak{X}\circ\mathfrak{Y})\circ\mathfrak{Z}} = (G^{\mathfrak{Z}})^{(\mathfrak{X}\circ\mathfrak{Y})} = ((G^{\mathfrak{Z}})^{\mathfrak{Y}})^{\mathfrak{X}} = (G^{(\mathfrak{Y}\circ\mathfrak{Z})})^{\mathfrak{X}} = G^{\mathfrak{X}\circ(\mathfrak{Y}\circ\mathfrak{Z})}$ для любой группы G. Теперь, если $G \in (\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z}$, то $G^{(\mathfrak{X}\circ\mathfrak{Y})\circ\mathfrak{Z}} = E = G^{\mathfrak{X}\circ(\mathfrak{Y}\circ\mathfrak{Z})}$ и $G \in \mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z})$, поэтому $(\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z} \subseteq \mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z})$. Обратно, если $G \in \mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z})$, то $G^{\mathfrak{X}\circ(\mathfrak{Y}\circ\mathfrak{Z})} = E = G^{(\mathfrak{X}\circ\mathfrak{Y})\circ\mathfrak{Z}}$ и $G \in (\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z}$. Поэтому $\mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z}) \subseteq (\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z}$ и $\mathfrak{X} \circ (\mathfrak{Y} \circ \mathfrak{Z}) = (\mathfrak{X} \circ \mathfrak{Y}) \circ \mathfrak{Z}$.

5.2. Проекторы

Пусть G — группа и $\mathfrak{X}$ — класс групп. Если H — подгруппа группы G и $H \in \mathfrak{X}$, то H называют $\mathfrak{X}$-*подгруппой.* $\mathfrak{X}$-*максимальной* подгруппой группы G называется такая $\mathfrak{X}$-подгруппа H из G, которая не содержится ни в какой большей $\mathfrak{X}$-подгруппе. Таким образом, H $\mathfrak{X}$-максимальна в G, если $H \in \mathfrak{X}$ и из условий $H \leq K \leq G$, $K \in \mathfrak{X}$ следует, что $H = K$.

Подгруппа H группы G называется $\mathfrak{X}$-*проектором* группы G, если HN/N — $\mathfrak{X}$-максимальная подгруппа группы G/N для любой нормальной подгруппы N группы G.

Пусть $\mathfrak{N}_p$ — класс всех p-групп. Рассмотрим произвольную группу G и пусть G_p — силовская p-подгруппа в G. Так как $G_p \in \mathfrak{N}_p$ и индекс G_p в группе G не делится на p, то G_p — $\mathfrak{N}_p$-максимальная подгруппа группы G. Для любой нормальной подгруппы N группы G по теореме 1.65, с. 53, фактор-группа G_pN/N — силовская p-подгруппа в G/N, поэтому G_pN/N $\mathfrak{N}_p$-максимальна в G/N и G_p — $\mathfrak{N}_p$-проектор группы G. Таким образом, $\mathfrak{N}_p$-проектор группы G совпадает с силовской p-подгруппой группы G.

Лемма 5.12. *Пусть $\mathfrak{X}$ — класс групп. Если H — $\mathfrak{X}$-проектор группы G и $N \lhd G$, то HN/N — $\mathfrak{X}$-проектор фактор-группы G/N.*

☐ Пусть $K/N \lhd G/N$. Тогда $(HN/N \cdot K/N)/K/N = HK/N/K/N \simeq HK/K$. Так как H — $\mathfrak{X}$-проектор в G, то HK/K $\mathfrak{X}$-максимальна в G/K. Поэтому $(HN/N \cdot K/N)/K/N$ $\mathfrak{X}$-максимальна в $G/N/K/N \simeq G/K$ и HN/N — $\mathfrak{X}$-проектор в G/N.

Лемма 5.13. *Пусть $\mathfrak{X}$ — класс групп. Подгруппа H группы G является $\mathfrak{X}$-проектором группы G тогда и только тогда, когда H $\mathfrak{X}$-максимальна в G и для любой минимальной нормальной подгруппы N группы G подгруппа HN/N — $\mathfrak{X}$-проектор группы G/N.*

☐ Если H — $\mathfrak{X}$-проектор группы G, то H $\mathfrak{X}$-максимальна в G и по лемме 5.12 подгруппа HN/N — $\mathfrak{X}$-проектор группы G/N для любой минимальной нормальной подгруппы N группы G.

Обратно, пусть H $\mathfrak{X}$-максимальна в G и HN/N — $\mathfrak{X}$-проектор группы G/N для каждой минимальной нормальной подгруппы N группы G. Пусть K — произвольная нормальная неединичная подгруппа группы G и пусть K_1 — минимальная нормальная подгруппа группы G, содержащаяся в K. По условию леммы HK_1/K_1 — $\mathfrak{X}$-проектор группы G/K_1, поэтому $(HK_1/K_1 \cdot K/K_1)/K/K_1 \simeq HK/K$ $\mathfrak{X}$-максимальна в $G/K_1/K/K_1 \simeq G/K$. Следовательно, H — $\mathfrak{X}$-проектор группы G.

Лемма 5.14. *Пусть $\mathfrak{X}$ — гомоморф, $H \leq G$, $N \lhd G$ и $N \leq H$. Если H/N — $\mathfrak{X}$-проектор фактор-группы G/N, то каждый $\mathfrak{X}$-проектор подгруппы H является $\mathfrak{X}$-проектором группы G.*

□ Пусть K — $\mathfrak{X}$-проектор подгруппы H. Тогда KN/N $\mathfrak{X}$-максимальна в H/N, а т.к. H/N — $\mathfrak{X}$-проектор группы G/N, то $KN = H$.

Пусть $K \leq L \in \mathfrak{X}$, $L \leq G$. Тогда $KN/N = H/N \leq LN/N \simeq L/L\cap N$. Поскольку $\mathfrak{X}$ — гомоморф, то $L/L\cap N \in \mathfrak{X}$ и $KN = H = LN$, т.е. $L \leq H$. Из $\mathfrak{X}$-максимальности K в H следует, что $K = L$ и K $\mathfrak{X}$-максимальна в G.

Предположим, что подгруппа K не является $\mathfrak{X}$-проектором группы G. Это означает, что существует нормальная подгруппа A в группе G такая, что AK/A не $\mathfrak{X}$-максимальна в G/A, т.е. существует подгруппа $S/A \in \mathfrak{X}$ и $AK/A < S/A$. Поскольку H/N — $\mathfrak{X}$-проектор группы G/N и $AN/N \lhd G/N$, то $(H/N \cdot AN/N)/(AN/N) = (HA/N)/(AN/N)$ $\mathfrak{X}$-максимальна в $(G/N)/(AN/N)$ и HA/AN $\mathfrak{X}$-максимальна в G/AN. Кроме того, $(S/A \cdot AN/A)/(AN/A) \simeq SN/AN \simeq (S/A)/(S/A \cap AN/A) \in \mathfrak{X}$, а т.к. $HA/AN = KNA/AN \leq SN/AN$, то из $\mathfrak{X}$-максимальности HA/AN в G/AN получаем, что $HA = KNA = SN$. Теперь $S = AK(S \cap N) \leq AH$, а т.к. K — $\mathfrak{X}$-проектор подгруппы H, то $K/K\cap A \simeq K(A\cap H)/A\cap H$ $\mathfrak{X}$-максимальна в $H/A\cap H$. Но $K/K\cap A \simeq KA/A \leq S/A \leq AH/A \simeq H/A \cap H$, где $K/K \cap A \in \mathfrak{X}$ и $S/A \in \mathfrak{X}$. Поэтому $KA = S$, что противоречит допущению.

Теорема 5.15. *Пусть $\mathfrak{X}$ — класс групп, а $\mathfrak{Y}$ — класс Шунка. Если в каждой $\mathfrak{Y}$-группе существует $\mathfrak{X}$-проектор, то $\mathfrak{X} \cap \mathfrak{Y}$ — класс Шунка.*

□ Пусть $G \in \mathfrak{X} \cap \mathfrak{Y}$ и $N \lhd G$. Тогда $G/N \in \mathfrak{Y}$, т.к. $\mathfrak{Y}$ — гомоморф. Поскольку $G \in \mathfrak{X}$, то G является своим $\mathfrak{X}$-проектором, значит $G/N \in \mathfrak{X}$ и $\mathfrak{X} \cap \mathfrak{Y}$ — гомоморф.

Пусть $G/Core_G M \in \mathfrak{X} \cap \mathfrak{Y}$ для всех $M < \cdot\, G$. Так как $\mathfrak{Y}$ — класс Шунка, то $G \in \mathfrak{Y}$. Пусть H — $\mathfrak{X}$-проектор группы G, он существует по условию теоремы. Предположим, что $H \neq G$. Тогда существует в группе G максимальная подгруппа A такая, что $H \leq$

A. Так как $HCore_GA \leq A$, то $HCore_GA \neq G$. Но $HCore_GA/Core_GA$ $\mathfrak{X}$-максимальна в $G/Core_GA$ по определению $\mathfrak{X}$-проектора, поэтому $G/Core_GA$ не принадлежит $\mathfrak{X}$. Противоречие. Значит $H = G$, $G \in \mathfrak{X}$ и требование $(6)'$ для класса $\mathfrak{X} \cap \mathfrak{Y}$ выполняется. Следовательно, $\mathfrak{X} \cap \mathfrak{Y}$ — класс Шунка.

Разрешимым классом называется класс, состоящий из разрешимых групп.

СЛЕДСТВИЕ. *1. Пусть $\mathfrak{X}$ — класс групп. Если в каждой группе существует $\mathfrak{X}$-проектор, то $\mathfrak{X}$ — класс Шунка.*

2. Разрешимый класс $\mathfrak{X}$, для которого каждая разрешимая группа обладает $\mathfrak{X}$-проектором, является классом Шунка.

☐ 1. Утверждение следует из теоремы в случае, когда $\mathfrak{Y} = \mathfrak{E}$ — класс всех групп.

2. Утверждение следует из теоремы в случае, когда $\mathfrak{Y} = \mathfrak{S}$ — класс всех разрешимых групп.

ТЕОРЕМА 5.16. *Если $\mathfrak{X}$ — класс Шунка, то в каждой группе существует $\mathfrak{X}$-проектор.*

☐ Предположим, что существуют группы в которых нет $\mathfrak{X}$-проекторов. Среди таких групп выберем группу наименьшего порядка и обозначим ее через G. Итак, в группе G нет $\mathfrak{X}$-проектора, но в каждой группе меньшего порядка существует $\mathfrak{X}$-проектор.

Если группа G простая, то каждая $\mathfrak{X}$-максимальная подгруппа является $\mathfrak{X}$-проектором группы G. Значит группа G непростая. Пусть $N \lhd G$, $N \neq E$. Тогда $|G/N| < |G|$ и в G/N есть $\mathfrak{X}$-проектор. Обозначим его через H/N. Если H — собственная подгруппа, то $|H| < |G|$ и в H по индукции имеется $\mathfrak{X}$-проектор, который по лемме 5.14 будет $\mathfrak{X}$-проектором группы G. Получили противоречие. Следовательно, $H = G$ и $G/N \in \mathfrak{X}$ для всех неединичных нормальных подгрупп N группы G. Если G не примитивна, то все примитивные фактор-группы группы G отличны от G и принадлежат $\mathfrak{X}$. Но $\mathfrak{X}$ — класс Шунка, поэтому $G \in \mathfrak{X}$ и сама группа G является $\mathfrak{X}$-проектором, противоречие. Следовательно, G примитивна. По теореме 4.41, с. 141, в группе G не более двух минимальных нормальных подгрупп.

Случай 1. *В группе G единственная минимальная нормальная подгруппа.*

Пусть $N \cdot\lhd G$. Если $N \le \Phi(G)$, то $G/N \in \mathfrak{X}$ и по теореме 5.2 группа $G \in \mathfrak{X}$, противоречие. Следовательно, N не содержится в $\Phi(G)$. Поэтому существует максимальная подгруппа M группы G такая, что $G = MN$. Пусть K — $\mathfrak{X}$-проектор подгруппы M, он существует по индукции, и A — $\mathfrak{X}$-максимальная подгруппа группы G, содержащая K. Так как $G/N = MN/N \simeq M/M \cap N \in \mathfrak{X}$, то $K(M \cap N) = M$ и $G = K(M \cap N)N = KN = AN$.

Пусть теперь L — произвольная неединичная нормальная подгруппа группы G. В нашем случае N — единственная минимальная нормальная подгруппа, поэтому $N \le L$ и $AL/L = G/L \in \mathfrak{X}$, т.е. AL/L $\mathfrak{X}$-максимальна в G/L и A — $\mathfrak{X}$-проектор группы G.

Случай 2. *В группе G две минимальные нормальные подгруппы N_1 и N_2.*

По теореме 4.41, с. 141, $G = [N_1]M = [N_2]M$, где $M < \cdot\, G$. Так как $G/N_1 \simeq M \in \mathfrak{X}$ и $M < \cdot\, G$, то M $\mathfrak{X}$-максимальна в G. Пусть L — произвольная неединичная нормальная подгруппа группы G. Тогда минимальная нормальная подгруппа в группе G из L совпадает с N_1 или N_2. Пусть $L \ge N_1$. Тогда $ML \ge MN_1 = G$ и $ML/L = G/L$ $\mathfrak{X}$-максимальна в G/L, т.е. M — $\mathfrak{X}$-проектор группы G. ⊠

Соединяя следствие теоремы 5.15 и теорему 5.16 получаем

Следствие 1. *Класс $\mathfrak{X}$ является классом Шунка тогда и только тогда, когда в каждой группе существует $\mathfrak{X}$-проектор.*

Следствие 2. *Если $\mathfrak{F}$ — насыщенная формация, то каждая группа обладает $\mathfrak{F}$-проектором.*

□ По теореме 5.3 каждая насыщенная формация является классом Шунка. Теперь утверждение следует из теоремы 5.16.

Формация $\mathfrak{A}$ не является классом Шунка и в диэдральной группе порядка 8 нет $\mathfrak{A}$-проекторов.

Пусть $\mathfrak{X}$ — класс групп. Подгруппа H называется $\mathfrak{X}$-*покрывающей подгруппой* группы G, если H является $\mathfrak{X}$-проектором каждой подгруппы группы G, в которой H содержится.

В знакопеременной группе A_5 степени 5 силовская 2-подгруппа P является $\mathfrak{N}$-проектором, но не является $\mathfrak{N}$-покрывающей подгруппой. Действительно, в A_5 имеется подгруппа, изоморфная A_4. Пусть H — подгруппа группы A_5, содержащая P, и изоморфная A_4. Тогда P нормальна в H и $H/P \in \mathfrak{N}$, т.е. подгруппа P не является $\mathfrak{N}$-проектором подгруппы H. Значит подгруппа P не является $\mathfrak{N}$-покрывающей подгруппой группы A_5. Обратим внимание на то, что подгруппа P является $\mathfrak{N}_2$-покрывающей подгруппой.

Лемма 5.17. *Пусть $\mathfrak{X}$ — гомоморф. Подгруппа H является $\mathfrak{X}$-покрывающей подгруппой группы G тогда и только тогда, когда $H \in \mathfrak{X}$ и из условий:*

$$H \leq U \leq G, \quad U_0 \lhd U, \quad U/U_0 \in \mathfrak{X} \tag{5.1}$$

следует, что $HU_0 = U$.

□ Пусть H — $\mathfrak{X}$-покрывающая подгруппа группы G и пусть выполняются условия (5.1). Так как H — $\mathfrak{X}$-проектор подгруппы U, то HU_0/U_0 $\mathfrak{X}$-максимальна в U/U_0. Но $U/U_0 \in \mathfrak{X}$, поэтому $HU_0/U_0 = U/U_0$ и $HU_0 = U$.

Обратно, пусть $H \in \mathfrak{X}$ и для всех подгрупп U и U_0, удовлетворяющих условиям (5.1) следует, что $HU_0 = U$. Предположим, что подгруппа H не является $\mathfrak{X}$-покрывающей подгруппой группы G. Тогда подгруппа H не является $\mathfrak{X}$-проектором некоторой подгруппы X, $H \leq X \leq G$. Это означает, что для некоторой нормальной подгруппы X_0 группы X подгруппа HX_0/X_0 не $\mathfrak{X}$-максимальна в X/X_0. Пусть U/X_0 — $\mathfrak{X}$-максимальная подгруппа в X/X_0, содержащая HX_0/X_0. Тогда $HX_0 < U$, а т.к. $H \in \mathfrak{X}$ и $\mathfrak{X}$ — гомоморф, то $HX_0/X_0 \simeq H/H \cap X_0 \in \mathfrak{X}$. Для подгруппы U выполняются условие (5.1), поэтому $HX_0 = U$, противоречие. Следовательно допущение неверно, подгруппа H — $\mathfrak{X}$-проектор подгруппы

X, а т.к. X — произвольная подгруппа группы G, содержащая H, то H — $\mathfrak{X}$-покрывающая подгруппа группы G. ⊠

Лемма 5.17 позволяет дать следующее определение $\mathfrak{X}$-покрывающей подгруппы, эквивалентное исходному.

Пусть $\mathfrak{X}$ — класс групп. Подгруппа H называется *$\mathfrak{X}$-покрывающей подгруппой* группы G, если выполняются следующие требования:

1) $H \in \mathfrak{X}$;

2) из условий $H \leq U \leq G,\ \ U_0 \lhd U,\ \ U/U_0 \in \mathfrak{X}$ следует, что, $U = HU_0$.

Лемма 5.18. *Для любого гомоморфа $\mathfrak{X}$ и любой группы G справедливы следующие утверждения:*

1) если H — $\mathfrak{X}$-проектор группы G и H максимальна в G, то H — $\mathfrak{X}$-покрывающая подгруппа группы G;

2) если H — $\mathfrak{X}$-покрывающая подгруппа в группе G и $H \leq X \leq G$, то H — $\mathfrak{X}$-покрывающая подгруппа в X;

3) если H — $\mathfrak{X}$-покрывающая подгруппа группы G и $N \lhd G$, то HN/N — $\mathfrak{X}$-покрывающая подгруппа фактор-группы G/N;

4) если $N \lhd G$ и H/N — $\mathfrak{X}$-покрывающая подгруппа фактор-группы G/N, то каждая $\mathfrak{X}$-покрывающая подгруппа из H является $\mathfrak{X}$-покрывающей подгруппой группы G.

□ Утверждения 1 и 2 непосредственно вытекают из определения $\mathfrak{X}$-покрывающей подгруппы.

3. По лемме 5.12 подгруппа HN/N — $\mathfrak{X}$-проектор фактор-группы G/N. Пусть X/N — произвольная подгруппа группы G/N, содержащая HN/N. Тогда $H \leq X$, а т.к. H — $\mathfrak{X}$-проектор подгруппы X, то опять по лемме 5.12 подгруппа HN/N — $\mathfrak{X}$-проектор X/N. Поэтому HN/N — $\mathfrak{X}$-покрывающая подгруппа группы G/N.

4. Пусть B — $\mathfrak{X}$-покрывающая подгруппа в H. Тогда BN/N $\mathfrak{X}$-максимальна в H/N. Но $H/N \in \mathfrak{X}$, значит $BN = H$. По лемме 5.14 подгруппа B — $\mathfrak{X}$-проектор группы G. Пусть $B \leq U \leq G,\ \ U_0 \lhd U,\ \ U/U_0 \in \mathfrak{X}$. Докажем, что $U_0B = U$, тогда по лемме 5.17 подгруппа B будет $\mathfrak{X}$-покрывающей подгруппой группы G.

Так как $H = BN \leq UN$ и H/N — $\mathfrak{X}$-покрывающая подгруппа группы G/N, то H/N — $\mathfrak{X}$-покрывающая подгруппа в UN/N. Но $U_0N/N \lhd UN/N$ и $UN/N\big/U_0N/N \simeq UN/U_0N \simeq U/U_0(U \cap N) \in \mathfrak{X}$, поэтому $HU_0N = HU_0 = UN$, откуда получаем, что $BNU_0 = UN$. По тождеству Дедекинда $U = BU_0(U \cap N)$, а поскольку $B(U \cap N) = U \cap H$, то $U = U_0(U \cap H)$. Теперь $U/U_0 \simeq U \cap H\big/U_0 \cap H \in \mathfrak{X}$, а т.к. B — $\mathfrak{X}$-покрывающая подгруппа из $U \cap H$, то $U \cap H = B(U_0 \cap H)$ и $U = U_0(U \cap H) = U_0B(U_0 \cap H) = U_0B$. ⊠

Напомним, что подгруппа H группы G называется *дополнением* к подгруппе K, если $HK = G$ и $H \cap K = E$.

Для класса $\mathfrak{X}$ введем следующие подмножества подгрупп группы G: $Proj_{\mathfrak{X}}(G)$ — совокупность всех $\mathfrak{X}$-проекторов группы G; $Cov_{\mathfrak{X}}(G)$ — совокупность всех $\mathfrak{X}$-покрывающих подгрупп группы G.

Ясно, что $Cov_{\mathfrak{X}}(G) \subseteq Proj_{\mathfrak{X}}(G)$. Если A — нормальная подгруппа группы G, то через $Comp_G(A)$ обозначим совокупность всех дополнений к подгруппе A в группе G.

Теорема 5.19. *Пусть $\mathfrak{X}$ — класс Шунка, A — минимальная нормальная подгруппа группы G, причем $G \notin \mathfrak{X}$, а $G/A \in \mathfrak{X}$. Если A абелева, то $Comp_G(A) = Proj_{\mathfrak{X}}(G) = Cov_{\mathfrak{X}}(G)$.*

□ Применим индукцию по порядку группы G. По теореме 5.16 в группе G существуют $\mathfrak{X}$-проекторы, поэтому $Proj_{\mathfrak{X}}(G) \neq \emptyset$. Пусть H — произвольный $\mathfrak{X}$-проектор группы G. По лемме 5.12 подгруппа HA/A является $\mathfrak{X}$-проектором группы G/A. Так как $G/A \in \mathfrak{X}$, то $HA = G$. Из того, что $G \notin \mathfrak{X}$ получаем, что $H \neq G$. Поскольку $H \cap A \lhd H$ и A абелева, то $H \cap A \lhd G$, и из минимальности подгруппы A следует, что $H \cap A = E$ и H — максимальная подгруппа группы G. Таким образом, доказано, что

$$Proj_{\mathfrak{X}}(G) = Cov_{\mathfrak{X}}(G) \subseteq Comp_G(A). \tag{5.2}$$

Пусть теперь B — произвольное дополнение к подгруппе A в группе G. Тогда $G = [A]H = [A]B$. Предположим, что существует минимальная нормальная подгруппа N группы G такая, что $N \leq H \cap B$. Рассмотрим фактор-группу G/N. Так как $AN = A \times N$, то AN/N —

минимальная нормальная подгруппа группы G/N. Подгруппа H/N является $\mathfrak{X}$-проектором группы G/N, поэтому $G/N \notin \mathfrak{X}$, но $G/N/AN/N \in \mathfrak{X}$. Таким образом, все условия теоремы выполняются для фактор-группы G/N. По индукции B/N — $\mathfrak{X}$-покрывающая подгруппа группы G/N, а по лемме 5.18 подгруппа B — $\mathfrak{X}$-покрывающая подгруппа группы G.

Пусть теперь пересечение $H \cap B$ не содержит неединичных нормальных подгрупп группы G. Допустим, что $Core_G B \neq E$, и пусть K — минимальная нормальная подгруппа группы G, содержащаяся в B. Тогда $AK = A \times K \subseteq C_G(A)$, поэтому $AK \cap H$ — нормальная подгруппа группы G. В нашем случае $AK \cap H$ не содержится в B, поэтому $(AK \cap H)B = G$, $G/AK \cap H \simeq B/B \cap AK \cap H \in \mathfrak{X}$. Так как $H/AK \cap H$ — $\mathfrak{X}$-проектор группы $G/AK \cap H$, то получили противоречие. Поэтому $Core_G B = E$.

Теперь, если L — произвольная нормальная подгруппа группы G, то L не содержится в B и $BL/L = G/L$ $\mathfrak{X}$-максимальна в G/L, т.е. B является $\mathfrak{X}$-проектором группы G. Итак, $Comp_G(A) \subseteq Proj_{\mathfrak{X}}(G)$ и из (5.2) следует, что $Proj_{\mathfrak{X}}(G) = Cov_{\mathfrak{X}}(G) = Comp_G(A)$.

Лемма 5.20. *Пусть $\mathfrak{X}$ — класс Шунка и N — нильпотентная нормальная подгруппа группы G. Если H — $\mathfrak{X}$-подгруппа, для которой $HN = G$, то H содержится в некоторой $\mathfrak{X}$-покрывающей подгруппе группы G. В частности, если H — $\mathfrak{X}$-максимальная подгруппа группы G, для которой $HN = G$, то H — $\mathfrak{X}$-покрывающая подгруппа группы G.*

□ Воспользуемся индукцией по порядку группы G. Пусть A — минимальная нормальная подгруппа группы G, содержащаяся в N. Тогда для фактор-группы G/A условия леммы выполнены. По индукции $\mathfrak{X}$-подгруппа HA/A содержится в некоторой $\mathfrak{X}$-покрывающей подгруппе F^*/A группы G/A.

Условию леммы удовлетворяет группа F^* с нильпотентной нормальной подгруппой $F^* \cap N$ и $\mathfrak{X}$-подгруппой H. Если $F^* \neq G$, то по индукции подгруппа H содержится в некоторой $\mathfrak{X}$-покрывающей подгруппе F группы F^*, которая по лемме 5.18 будет $\mathfrak{X}$-покрывающей подгруппой группы G.

Поэтому следует считать, что $G/A \in \mathfrak{X}$. По теореме 5.19 подгруппа A имеет дополнение F в группе G и F является $\mathfrak{X}$-покрывающей подгруппой группы G. Ясно, что F — максимальная подгруппа группы G. Так как $N \cap F \triangleleft F$ и N нильпотентна, то $N \cap F \triangleleft G$.

Если $N \cap F \neq E$, то можно считать подгруппу A, содержащейся в $N \cap F$. Тогда $F = G$ и $H \leq F$.

Если $N \cap F = E$, то $A = N$ и из условия $HN = G$ следует, что H — дополнение к N в G и по теореме 5.19 H будет $\mathfrak{X}$-покрывающей подгруппой группы G.

Теорема 5.21. *Для любого класса Шунка $\mathfrak{X}$ в каждой разрешимой группе G любой $\mathfrak{X}$-проектор является $\mathfrak{X}$-покрывающей подгруппой и любые две $\mathfrak{X}$-покрывающие подгруппы группы G сопряжены между собой.*

□ Воспользуемся индукцией по порядку группы G. Заметим, что по теореме 5.16 в каждой группе существует $\mathfrak{X}$-проектор.

Пусть G — разрешимая группа и A — минимальная нормальная подгруппа группы G. Тогда A абелева. Пусть H — $\mathfrak{X}$-проектор группы G. По лемме 5.12 подгруппа HA/A является $\mathfrak{X}$-проектором группы G/A. По индукции можно считать, что HA/A — $\mathfrak{X}$-покрывающая подгруппа группы G/A.

Рассмотрим подгруппу HA и применим к группе HA лемму 5.20. По этой лемме подгруппа H является $\mathfrak{X}$-покрывающей подгруппой группы HA. По лемме 5.18 подгруппа H является $\mathfrak{X}$-покрывающей подгруппой группы G. Итак, каждый $\mathfrak{X}$-проектор группы G является $\mathfrak{X}$-покрывающей подгруппой группы G.

Пусть теперь H_1 и H_2 — две $\mathfrak{X}$-покрывающие подгруппы группы G. Тогда H_1A/A и H_2A/A — $\mathfrak{X}$-покрывающие подгруппы фактор-группы G/A и по индукции они сопряжены между собой, т.е. существует элемент $g \in G$ такой, что $H_1A/A = (H_2A/A)^{gA}$. Отсюда получаем, что $H_1A = H_2^gA$.

По лемме 5.18 подгруппы H_1 и H_2^g — $\mathfrak{X}$-покрывающие подгруппы группы H_1A. Если H_1A — собственная подгруппа группы G, то по индукции подгруппы H_1 и H_2^g сопряжены в H_1A, т.е. существует элемент $ha \in H_1a$, где $h \in H$, $a \in A$ такой, что $H_1 = H_2^{gha}$. Значит H_1 и H_2 сопряжены в G.

Поэтому будем считать, что $H_1A = H_2^gA = G$. Подгруппа A выбиралась произвольно. Если $Core_GH_1 \neq E$, то A можно считать содержащейся в H_1 и $H_1 = G$. В этом случае теорема верна.

Пусть $Core_GH_1 = E$. Тогда $Core_GH_2 = E$. Но в разрешимой группе максимальные подгруппы с единичными ядрами сопряжены между собой по теореме 4.43, с. 144. Поэтому $H_1 = H_2^x$ для некоторого $x \in G$.

По теореме 5.3 каждая насыщенная формация является классом Шунка. Поэтому справедливо

Следствие. *Для любой насыщенной формации $\mathfrak{F}$ в каждой разрешимой группе G любой $\mathfrak{F}$-проектор является $\mathfrak{F}$–покрывающей подгруппой и любые две $\mathfrak{F}$-покрывающие подгруппы группы G сопряжены между*

Поскольку в разрешимых группах понятия $\mathfrak{F}$-проектора и $\mathfrak{F}$-покрывающей подгруппы совпадают, то в дальнейшем для разрешимых групп будем использовать термин $\mathfrak{F}$-проектор.

Теорема 5.22. *Если $\mathfrak{X}$ — разрешимый класс Шунка, а $\mathfrak{F}$ — разрешимая насыщенная формация, то $\mathfrak{X} \circ \mathfrak{F}$ — разрешимый класс Шунка.*

□ По теореме 5.10 произведение $\mathfrak{X} \circ \mathfrak{F}$ — гомоморф. Ясно, что $\mathfrak{X} \circ \mathfrak{F}$ — разрешимый класс. Пусть $G/N \in \mathfrak{X} \circ \mathfrak{F}$ для всех примитивных фактор-групп G/N группы G и пусть S — $\mathfrak{X}$-проектор подгруппы $G^{\mathfrak{F}}$. Так как группа G разрешима, то $\mathfrak{X}$-проекторы в $G^{\mathfrak{F}}$ существуют и сопряжены между собой. По лемме Фраттини $G = N_G(S)G^{\mathfrak{F}}$.

Предположим, что существует максимальная подгруппа M в группе G такая, что $S \leq M$ и $G^{\mathfrak{F}} \not\subseteq M$. Пусть $Core_GM$ — ядро подгруппы M в группе G. Фактор-группа $G/Core_GM$ примитивна, поэтому $G/Core_GM \in \mathfrak{X} \circ \mathfrak{F}$ и $(G/Core_GM)^{\mathfrak{F}} = G^{\mathfrak{F}}Core_GM/Core_GM \simeq G^{\mathfrak{F}}/(G^{\mathfrak{F}} \cap$

$Core_G M) \in \mathfrak{X}$. Но теперь $G^{\mathfrak{F}} = S(G^{\mathfrak{F}} \cap Core_G M) \leq SCore_G M \leq M$, что противоречит выбору M.

Следовательно, для любой максимальной подгруппы H группы G такой, что $S \leq H$, выполняется включение $G^{\mathfrak{F}} \leq H$. Так как $G = N_G(S)G^{\mathfrak{F}}$, то $S \lhd G$, $G^{\mathfrak{F}}/S \leq \Phi(G/S)$. Поскольку формация $\mathfrak{F}$ насыщенна и $G/G^{\mathfrak{F}} \simeq (G/S)/(G^{\mathfrak{F}}/S) \in \mathfrak{F}$, то $G/S \in \mathfrak{F}$ и $G^{\mathfrak{F}} = S \in \mathfrak{X}$, поэтому $G \in \mathfrak{X} \circ \mathfrak{F}$.

Следствие. *Если $\mathfrak{X}$ и $\mathfrak{F}$ — разрешимые насыщенные формации, то $\mathfrak{X} \circ \mathfrak{F}$ — разрешимая насыщенная формация.*

$\square$ По теореме 5.10 произведение $\mathfrak{X} \circ \mathfrak{F}$ — формация. Так как каждая насыщенная формация является классом Шунка, то по теореме 5.22 произведение $\mathfrak{X} \circ \mathfrak{F}$ — класс Шунка. Но класс Шунка — насыщенный класс, поэтому $\mathfrak{X} \circ \mathfrak{F}$ — насыщенная формация. $\boxtimes$

В нильпотентных и сверхразрешимых группах $\mathfrak{X}$-проекторы допускают описание для любого класса Шунка $\mathfrak{X}$.

Теорема 5.23. *Пусть $\mathfrak{X}$ — класс Шунка и G — нильпотентная группа. Подгруппа H группы G тогда и только тогда $\mathfrak{X}$-максимальна, когда H — $\chi(\mathfrak{X})$-холлова подгруппа.*

$\square$ Согласно теореме 5.6, с. 161, пересечение $\mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$. Пусть H — $\mathfrak{X}$-максимальная подгруппа группы G. Ясно, что H будет $\chi(\mathfrak{X})$-подгруппой. Если K — $\chi(\mathfrak{X})$-холлова подгруппа группы G, то $H \leq K$. Так как $K \in \mathfrak{N}_{\chi(\mathfrak{X})} = \mathfrak{X} \cap \mathfrak{N}$, то K — $\mathfrak{X}$-подгруппа и $H = K$. Обратно, если H — $\chi(\mathfrak{X})$-холлова подгруппа, то $H \in \mathfrak{N}_{\chi(\mathfrak{X})} = \mathfrak{X} \cap \mathfrak{N}$. Если K $\mathfrak{X}$-максимальна в G и $K \geq H$, то $K \in \mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$ и K — $\chi(\mathfrak{X})$-подгруппа. Поэтому $H = K$. $\boxtimes$

Поскольку в каждой группе $\mathfrak{X}$-проектор является $\mathfrak{X}$-максимальной подгруппой, то имеем

Следствие. *1. Пусть $\mathfrak{X}$ — класс Шунка и G — нильпотентная группа. Подгруппа H тогда и только тогда является $\mathfrak{X}$-проектором группы G, когда H — $\chi(\mathfrak{X})$-холлова подгруппа.*

2. Пусть $\mathfrak{F}$ *— насыщенная формация и* G *— нильпотентная группа. Подгруппа* H *тогда и только тогда является* $\mathfrak{X}$*-проектором группы* G*, когда* H *—* $\chi(\mathfrak{X})$*-холлова подгруппа.*

Теорема 5.24. *Пусть* $\mathfrak{X}$ *— класс Шунка и* G *— метанильпотентная группа. Подгруппа* H *тогда и только тогда является* $\mathfrak{X}$*-проектором группы* G*, когда* H $\mathfrak{X}$*-максимальна в* G *и* $HF(G)/F(G)$ *—* $\chi(\mathfrak{X})$*-холлова подгруппа фактор-группы* $G/F(G)$*.*

$\square$ Пусть H — $\mathfrak{X}$-проектор группы G. Тогда H $\mathfrak{X}$-максимальна в группе G и $HF(G)/F(G)$ — $\mathfrak{X}$-проектор фактор-группы $G/F(G)$ по лемме 5.18. Так как $G/F(G)$ по условию нильпотентна, то $HF(G)/F(G)$ — $\chi(\mathfrak{X})$-холлова подгруппа фактор-группы $G/F(G)$ по следствию теоремы 5.23.

Обратно, пусть H $\mathfrak{X}$-максимальна в группе G и $HF(G)/F(G)$ — $\mathfrak{X}$-холлова подгруппа фактор-группы $G/F(G)$. Пусть K — $\mathfrak{X}$-проектор группы G. Тогда $KF(G)/F(G)$ — $\mathfrak{X}$-проектор фактор-группы $G/F(G)$. По следствию теоремы 5.23 подгруппа $KF(G)/F(G)$ является $\chi(\mathfrak{X})$-холловой подгруппой нильпотентной группы $G/F(G)$. Поэтому $HF(G) = KF(G)$. Поскольку подгруппа H $\mathfrak{X}$-максимальна в $HF(G)$, то по лемме 5.20 подгруппа H является $\mathfrak{X}$-проектором группы $HF(G)$. Так как подгруппа K также является $\mathfrak{X}$-проектором группы $HF(G)$, то H и K сопряжены. Следовательно, подгруппа H является $\mathfrak{X}$-проектором группы G.

Следствие 1. *Пусть* $\mathfrak{X}$ *— насыщенная формация и* G *— метанильпотентная группа. Подгруппа* H *тогда и только тогда является* $\mathfrak{X}$*-проектором группы* G*, когда* H $\mathfrak{X}$*-максимальна в* G *и* $HF(G)/F(G)$ *является* $\chi(\mathfrak{X})$*-холловой подгруппой фактор-группы* $G/F(G)$*.*

Поскольку по теореме 4.52, с. 150, каждая сверхразрешимая группа имеют нильпотентный коммутант, то получаем

Следствие 2. *1. Пусть* $\mathfrak{X}$ *— класс Шунка и* G *— сверхразрешимая группа. Подгруппа* H *тогда и только тогда является* $\mathfrak{X}$*-проектором группы* G*, когда* H $\mathfrak{X}$-

максимальна в G и HG'/G' является $\chi(\mathfrak{X})$-холловой подгруппой фактор-группы G/G'.

2. Пусть $\mathfrak{X}$ — насыщенная формация и G — сверхразрешимая группа. Подгруппа H тогда и только тогда является $\mathfrak{X}$-проектором группы G, когда H $\mathfrak{X}$-максимальна в G и HG'/G' является $\chi(\mathfrak{X})$-холловой подгруппой фактор-группы G/G'.

5.3. Картеровы и гащюцевы подгруппы разрешимых групп

Лемма 5.25. *Пусть $\mathfrak{X}$ — класс Шунка характеристики π и пусть H — $\mathfrak{X}$-проектор группы G. Тогда $N_G(H)/H$ — π'-группа.*

□ Если $N_G(H)/H$ не является π'-группой, то существует простое число $p \in \pi$, которое делит порядок $N_G(H)/H$. По теореме Силова в группе $N_G(H)/H$ имеется подгруппа K/H порядка p. Так как в $\mathfrak{X}$ имеется подгруппа порядка p, то $K/H \in \mathfrak{X}$ и H не является $\mathfrak{X}$-проектором K, противоречие.

Лемма 5.26. *Пусть $\mathfrak{X}$ — класс Шунка. Тогда и только тогда в каждой разрешимой группе $\mathfrak{X}$-проектор самонормализуем, когда $\mathfrak{N} \subseteq \mathfrak{X}$.*

□ Пусть в каждой разрешимой группе $\mathfrak{X}$-проектор совпадает со своим нормализатором. Предположим, что $\mathfrak{N}$ не содержится в $\mathfrak{X}$. Тогда существует группа $G \in \mathfrak{N} \setminus \mathfrak{X}$. Пусть H — $\mathfrak{X}$-проектор группы G. Так как $G \notin \mathfrak{X}$, то $H \neq G$. Но в нильпотентных группах собственные подгруппы отличны от своих нормализаторов, поэтому $N_G(H) \neq H$, получили противоречие. Значит допущение неверно и $\mathfrak{N} \subseteq \mathfrak{X}$.

Обратно, пусть $\mathfrak{N} \subseteq \mathfrak{X}$ и допустим, что существует разрешимая группа G, в которой $\mathfrak{X}$-проектор H — собственная подгруппа в своем нормализаторе. Пусть простое число p делит порядок $N_G(H)/H$. Тогда в $N_G(H)/H$ существует подгруппа K/H порядка p. Так как $K/H \in \mathfrak{N} \subseteq \mathfrak{X}$, то H не будет $\mathfrak{X}$-проектором подгруппы K, противоречие. ⊠

Картеровой подгруппой называют нильпотентную самонормализуемую подгруппу группы.

Теорема 5.27. *В любой разрешимой группе множество $\mathfrak{N}$-проекторов совпадает с множеством картеровых подгрупп.*

□ Пусть H — $\mathfrak{N}$-проектор разрешимой группы G. Тогда H нильпотентна и по лемме 5.26 совпадает со своим нормализатором, т.е. H является картеровой подгруппой группы G.

Обратно, пусть H — картерова подгруппа разрешимой группы G. Воспользуемся индукцией по порядку группы. Так как в нильпотентных группах собственные подгруппы отличны от своих нормализаторов, то H — $\mathfrak{N}$-максимальная подгруппа группы G. По лемме 5.20, с. 172, существует нильпотентная нормальная подгруппа N группы G такая, что HN — собственная подгруппа. По индукции H — $\mathfrak{N}$-проектор группы HN. Пусть $xN \in N_{G/N}(HN/N)$. Тогда H^x — картерова подгруппа группы $(HN)^x = HN$ и по индукции подгруппа H^x — $\mathfrak{N}$-проектор группы HN. Поэтому подгруппы H и H^x сопряжены в HN, т.е. существует элемент $y \in HN$ такой, что $H^x = H^y$. Теперь $xy^{-1} \in N_G(H) = H$, $x \in Hy \subseteq HN$. Таким образом, HN/N — самонормализуемая нильпотентная подгруппа группы G/N. По индукции подгруппа HN/N — $\mathfrak{N}$-проектор группы G/N, а по лемме 5.18, с. 170, подгруппа H — $\mathfrak{N}$-проектор группы G.

Следствие. *В любой разрешимой группе картеровы подгруппы существуют и сопряжены между собой.* ⊠

Лемма 5.28. *Если в примитивной разрешимой группе G примитиватор имеет простой индекс, то группа G сверхразрешима.*

□ Пусть G — примитивная группа, M — её примитиватор и $| G : M |= p$ — простое число. Пусть $N \cdot\!\lhd G$. По теореме 4.42, с. 143, группа $G = [N]M$ и $N = C_G(N)$. Теперь $| N |= p$ и G/N изоморфна группе автоморфизмов группы N, которая является циклической группой порядка, делящего $p-1$. Поэтому M циклическая и группа G

сверхразрешима по лемме 4.46, с. 147. ⊠

Гащюцевой подгруппой группы G называется подгруппа H группы G, удовлетворяющая следующим двум требованиям:

1) H сверхразрешима;

2) если $H \leq H_1 < T \leq G$, то $\mid T : H_1 \mid$ — не простое число.

Теорема 5.29. *В любой разрешимой группе множество* $\mathfrak{U}$*-проекторов совпадает с множеством гащюцевых подгрупп.*

□ Пусть H — $\mathfrak{U}$-проектор разрешимой группы G. Тогда H сверхразрешима. Предположим, что существуют подгруппы H_1 и T такие, что $H \leq H_1 < \cdot\, T$, $\mid T : H_1 \mid = p$ — простое число. Тогда $T/Core_T(H_1)$ — примитивная группа с примитиватором $H_1/Core_T(H_1)$ индекса p в $T/Core_T(H_1)$. По лемме 5.28 группа $T/Core_T(H_1)$ сверхразрешима. Так как H — $\mathfrak{U}$-проектор T, то $T = HCore_T(H_1) = H_1$, противоречие. Поэтому допущение неверно и если $H \leq H_1 < \cdot\, T$, то $\mid T : H_1 \mid$ — не простое число.

Обратно, пусть выполняются оба требования из определения гащюцевой подгруппы. Если $H < \cdot\, T$ и $T \in \mathfrak{U}$, то $\mid T : H \mid$ — простое число по теореме 4.48, с. 148, что противоречит второму требованию. Поэтому H — $\mathfrak{U}$-максимальная подгруппа группы G. По лемме 5.20, с. 172, существует нильпотентная нормальная неединичная подгруппа N группы G такая, что HN — собственная подгруппа. Рассмотрим фактор-группу G/N. Ясно, что HN/N сверхразрешима. Если $HN/N \leq H_1/N < \cdot\, T/N \leq G/N$, то $H \leq H_1 < \cdot\, T \leq G$ и $\mid T : H_1 \mid$ не простое число. Таким образом, HN/N — гащюцева подгруппа фактор-группы G/N. По индукции HN/N является $\mathfrak{U}$-проектором фактор-группы G/N, а по лемме 5.18, с. 170, подгруппа H — $\mathfrak{U}$-проектор группы G.

Следствие. *В любой разрешимой группе гащюцевы подгруппы существуют и сопряжены между собой.*

В § 4.5 для произвольного множества π простых чисел в каждой разрешимой группе установлено существование и сопряженность π-холловых подгрупп. Эти утверждения являются частными случаями следствия теоремы 5.21, с. 173.

Теорема 5.30. *В любой разрешимой группе множество $\mathfrak{S}_\pi$-проекторов совпадает со множеством π-холловых подгрупп.*

□ Воспользуемся индукцией по порядку группы. Поскольку класс $\mathfrak{S}_\pi$ всех разрешимых π-групп является насыщенной формацией, то $\mathfrak{S}_\pi$-проекторы существуют и сопряжены в каждой разрешимой группе в силу следствия теоремы 5.21, с. 173. Пусть H — $\mathfrak{S}_\pi$-проектор разрешимой группы G и пусть N — минимальная нормальная подгруппа группы G. Тогда H — π-подгруппа группы G. Так как HN/N — $\mathfrak{S}_\pi$-проектор группы G/N, то по индукции HN/N — π-холлова подгруппа группы G/N. Если $HN \neq G$, то по индукции H — π-холлова подгруппа группы HN, поэтому из равенства $\mid G : H \mid = \mid G : HN \mid\mid HN : H \mid$ следует, что H — π-холлова подгруппа группы G. Если $HN = G$, то H — максимальная подгруппа группы G и $H \cap N = E$. Если N — p-группа для $p \in \pi$, то G — π-группа и $G = H \in \mathfrak{S}_\pi$. Если $p \notin \pi$, то $\mid G : H \mid = \mid N \mid$ — π'-число и H — π-холлова подгруппа группы G. Итак, каждый $\mathfrak{S}_\pi$-проектор разрешимой группы G является π-холловой подгруппой.

Обратно, пусть H — π-холлова подгруппа группы G. Тогда из леммы 4.34, с. 138, следует, что H — $\mathfrak{S}_\pi$-проектор группы G.

Следствие. *Для произвольного множества π простых чисел в каждой разрешимой группе G π-холловы подгруппы существуют и сопряжены между собой.*

5.4. Классы Фиттинга

Класс $\mathfrak{X}$ называется *нормально наследственным* или классом, *замкнутым относительно нормальных подгрупп*, если выполняется следующее требование:

1) если $G \in \mathfrak{X}$ и $N \triangleleft G$, то $N \in \mathfrak{X}$.

Очевидно, что если класс $\mathfrak{X}$ замкнут относительно нормальных подгрупп, то $\mathfrak{X}$ замкнут относительно субнормальных подгрупп, т. е. если $G \in \mathfrak{X}$ и $N \lhd\lhd G$, то $N \in \mathfrak{X}$.

Класс $\mathfrak{X}$ называется *замкнутым относительно произведений нормальных* $\mathfrak{X}$*-подгрупп*, если выполняется следующее требование:

2) если N_1 и $N_2 \lhd G$, N_1 и $N_2 \in \mathfrak{X}$, то $N_1N_2 \in \mathfrak{X}$.

Классом Фиттинга называется класс $\mathfrak{X}$, замкнутый относительно нормальных подгрупп и произведений нормальных $\mathfrak{X}$-подгрупп. Класс Фиттинга называют также *радикальным* классом. Радикальная формация — это формация, являющаяся классом Фиттинга.

Классы $\mathfrak{S}$, $\mathfrak{N}$, $\mathfrak{S}_\pi$, $\mathfrak{N}_\pi$ для любого множества простых чисел π будут классами Фиттинга.

Для каждого натурального k класс $\mathfrak{N}^k$ всех разрешимых групп нильпотентной длины $\leq k$ будет согласно лемме 4.29, с. 130, классом Фиттинга.

Классы $\mathfrak{A}$ и $\mathfrak{U}$ не являются классами Фиттинга. Действительно, для классов $\mathfrak{A}$ и $\mathfrak{U}$ условие 1 определения класса Фиттинга выполняется, а 2 нарушается. Например, неабелева диэдральная подгруппа D_8 порядка 8 является произведением двух абелевых подгрупп A и B порядка 4. Поэтому $D_8 = AB \notin \mathfrak{A}$, но A и $B \in \mathfrak{A}$. Для класса сверхразрешимых групп $\mathfrak{U}$ соответствующий пример имеется в конце главы 4.

Теорема 5.31. *Если класс $\mathfrak{X}$ замкнут относительно произведений нормальных $\mathfrak{X}$-подгрупп, то каждая субнормальная $\mathfrak{X}$-подгруппа группы G содержится в некоторой нормальной $\mathfrak{X}$-подгруппе.*

□ Пусть H — субнормальная $\mathfrak{X}$-подгруппа группы G. Применим индукцию по индексу $|\ G : H\ |$. Заметим, что $H \neq N_G(H)$ и $N_G(H) \neq G$. Выберем подгруппу L в группе G, обладающую следующим свойством: подгруппа L порождается всеми субнормальными подгруппами X группы G такими, что $H \leq X \leq N_G(H)$.

Ясно, что $H \leq L \leq N_G(H)$. Так как по теореме 2.43, с. 85, подгруппа, порожденная субнормальными подгруппами, является субнормальной подгруппой, то L субнормальна и существует субнормальная подгруппа M в группе G такая, что $L \triangleleft M$ и $M \neq L$. По выбору L подгруппа M не содержится в $N_G(H)$. Поэтому существует элемент $x \in M \setminus N_G(H)$. Ясно, что $H \neq H^x$, $H^x \in \mathfrak{X}$ и H^x — субнормальная подгруппа группы G. Поскольку $H \triangleleft L$, то $H^x \triangleleft L^x = L$. Теперь HH^x — подгруппа группы L и $HH^x \in \mathfrak{X}$ по требованию 2. Кроме того, $HH^x \neq H$, поэтому к подгруппе HH^x применима индукция. По индукции существует нормальная подгруппа N в группе G такая, что $N \in \mathfrak{X}$ и $HH^x \leq N$. Теперь $H \leq N$.

Следствие 1. *Пусть класс $\mathfrak{X}$ замкнут относительно произведений нормальных $\mathfrak{X}$-подгрупп. Если H_1 и H_2 — субнормальные $\mathfrak{X}$-подгруппы группы G, то $\langle H_1, H_2\rangle$ — субнормальная $\mathfrak{X}$-подгруппа.*

□ Пусть $M = \langle H_1, H_2\rangle$. По теореме 5.31 существуют в группе M нормальные $\mathfrak{X}$-подгруппы N_1 и N_2 такие, что $H_1 \leq N_1$, $H_2 \leq N_2$. По требованию 2) произведение $N_1N_2 \in \mathfrak{X}$. Поэтому $M = \langle H_1, H_2\rangle \leq N_1N_2 \leq M$ и $M = N_1N_2 \in \mathfrak{X}$.

В силу следствия 1 требование 2) стало эквивалентным требованию

3) если N_1 и $N_2 \triangleleft\triangleleft\, G$, N_1 и $N_2 \in \mathfrak{X}$, то $\langle N_1, N_2\rangle \in \mathfrak{X}$.

Следствие 2. *Пусть класс $\mathfrak{X}$ замкнут относительно произведений нормальных $\mathfrak{X}$-подгрупп. Если H — субнормальная $\mathfrak{X}$-подгруппа группы G, то $H^G \in \mathfrak{X}$.*

□ Подгруппа H^G порождается всеми сопряженными с H подгруппами группы G, т.е. $H^G = \langle H^g \mid g \in G\rangle$. По следствию 1 получаем, что $H^G \in \mathfrak{X}$.

Применяя следствие 2 к классам всех разрешимых и нильпотентных групп, получаем

Следствие 3. *Пусть H — субнормальная подгруппа группы G. Тогда:*

1) если H разрешима, то H^G разрешима;

2) если H нильпотентна, то H^G нильпотентна.

Пусть $\mathfrak{X}$ — класс Фиттинга. Произведение всех нормальных $\mathfrak{X}$-подгрупп группы G называется *$\mathfrak{X}$-радикалом* группы G и обозначается через $G_{\mathfrak{X}}$. Ясно, что $\mathfrak{X}$-радикал $G_{\mathfrak{X}}$ является наибольшей нормальной подгруппой группы

G, содержащейся в $\mathfrak{X}$.

Если G — группа, то $\mathfrak{N}$-радикал $G_{\mathfrak{N}}$ совпадает с подгруппой Фиттинга $F(G)$.

Лемма 5.32. *Пусть $\mathfrak{X}$ — класс Фиттинга, G — группа и $H \lhd\lhd G$. Тогда и только тогда $H \in \mathfrak{X}$, когда $H \leq G_{\mathfrak{X}}$.*

□ Пусть $H \lhd \lhd G$ и $H \in \mathfrak{X}$. По следствию 1 теоремы 5.31 получаем, что $H \leq H^G \in \mathfrak{X}$ и $H^G \leq G_{\mathfrak{X}}$.

Обратно, пусть $H \lhd \lhd G$ и $H \leq G_{\mathfrak{X}}$. Так как $G_{\mathfrak{X}} \in \mathfrak{X}$ и выполняется требование 1), то $H \in \mathfrak{X}$.

Лемма 5.33. *Если $\mathfrak{X}$ — класс Фиттинга и $N \lhd \lhd G$, то $N_{\mathfrak{X}} = G_{\mathfrak{X}} \cap N$.*

□ Так как $G_{\mathfrak{X}} \cap N \lhd \lhd G_{\mathfrak{X}}$ и $G_{\mathfrak{X}} \in \mathfrak{X}$, то $G_{\mathfrak{X}} \cap N \in \mathfrak{X}$. Поскольку $G_{\mathfrak{X}} \cap N \lhd N$, то $G_{\mathfrak{X}} \cap N \subseteq N_{\mathfrak{X}}$.

Обратно, $N_{\mathfrak{X}} \lhd N \lhd \lhd G$, поэтому $N_{\mathfrak{X}} \lhd \lhd G$ и $N_{\mathfrak{X}} \subseteq G_{\mathfrak{X}}$ по лемме 5.32. Итак, $G_{\mathfrak{X}} \cap N = N_{\mathfrak{X}}$.

Лемма 5.34. *Пусть группа G содержит нормальную подгруппу N индекса p, где p — простое число. Если Z — циклическая группа порядка p, то прямое произведение $G \times Z$ содержит нормальную подгруппу K, изоморфную G, и отличную от G.*

□ Так как $(G \times Z)/N \simeq E_{p^2}$, где E_{p^2} — элементарная абелева группа порядка p^2, то в $(G \times Z)/N$ существует $(p^2 - 1)$ элементов порядка p, которые распадаются на $(p^2 - 1)/(p - 1) = (p + 1)$ подгрупп порядка p. Поэтому существует в $(G \times Z)/N$ подгруппа K/N порядка p такая, что $K/N \neq G/N$ и $Z \not\subseteq K$. Подгруппа K нормальна в группе $G \times Z$, $K \neq G$. Кроме того, $G \times Z = K \times Z$ и $(G \times Z)/Z \simeq G \simeq (K \times Z)/Z \simeq K$.

Теорема 5.35. *Если класс Фиттинга $\mathfrak{X}$ содержит разрешимую группу G, то $\mathfrak{N}_{\pi(G)} \subseteq \mathfrak{X}$.*

□ Пусть $G \in \mathfrak{X} \cap \mathfrak{S}$ и $p \in \pi(G)$. У разрешимой группы факторы композиционного ряда имеют простые порядки. Поэтому существуют подгруппы $N \lhd H \lhd \lhd G$ такие, что $\mid H/N \mid = p$. Пусть Z — циклическая группа порядка p. По лемме 5.34 существует группа K, изоморфная H такая, что $K \lhd H \times Z$, $K \neq H$. Теперь $HK = H \times Z \in \mathfrak{X}$. Итак, класс $\mathfrak{X}$ содержит группу порядка p.

Пусть P — произвольная p-группа. По индукции можно считать, что все собственные подгруппы группы P содержатся в $\mathfrak{X}$. Если в группе P имеются две различные подгруппы P_1 и P_2 индекса p, то P_1 и $P_2 \in \mathfrak{X}$ по индукции, а так как для $\mathfrak{X}$ выполняется требование 2), то $P = P_1P_2 \in \mathfrak{X}$. Пусть в P только одна подгруппа индекса p. В этом случае группа P циклическая. Пусть $\mid P \mid= p^n$, $\mid P_1 \mid= p^{n-1}$. Построим группу $B = A_1 \times \ldots \times A_p$, $A_i \simeq P_1$. Пусть $A_i = \langle a_i \rangle$. Рассмотрим отображение $\gamma : B \mapsto B$ такое, что $\gamma(a_i) = a_{i+1}$, $i = 1, \ldots, p-1$, $\gamma(a_p) = a_1$. Легко проверить, что $\gamma \in AutB$, $\mid \gamma \mid= p$. Поэтому существует группа $M = \langle a_1, \ldots, a_p, \gamma \rangle = B \times \langle \gamma \rangle$. Теперь $\mid M \mid= p^{(n-1)p+1}$, значит все подгруппы в M субнормальны. Так как $B \in \mathfrak{X}$ и $\langle \gamma \rangle \in \mathfrak{X}$, то $M \in \mathfrak{X}$. Вычислим порядок элемента $a_1\gamma$. Так как $(a_1\gamma)^p = a_1\gamma a_1\gamma \ldots a_1\gamma = a_1(\gamma a_1\gamma^{-1})(\gamma^2 a_1\gamma^{-2}) \ldots (\gamma^{p-1}a_1\gamma^{1-p}) = a_1a_2 \ldots a_p$ и $a_1a_2 \ldots a_p$ имеет порядок p^{n-1}, то элемент $a_1\gamma$ имеет порядок p^n. Таким образом, $P \in \mathfrak{X}$. Итак, $\mathfrak{N}_p \subseteq \mathfrak{X}$ для всех $p \in \pi(G)$. Поэтому $\mathfrak{N}_{\pi(G)} \subseteq \mathfrak{X}$.

Следствие 1. *Если $\mathfrak{X}$ — класс Фиттинга, то* $\mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$.

☐ По теореме 5.35 имеем включение $\mathfrak{N}_p \subseteq \mathfrak{X}$ для всех $p \in \chi(\mathfrak{X})$. Поэтому $\mathfrak{N}_{\chi(\mathfrak{X})} \subseteq \mathfrak{X} \cap \mathfrak{N}$. Обратно, если $G \in \mathfrak{X} \cap \mathfrak{N}$, то $\mathfrak{N}_{\pi(G)} \subseteq \mathfrak{X}$ по теореме 5.35. Поэтому $\pi(G) \subseteq \chi(\mathfrak{X})$ и $G \in \mathfrak{N}_{\chi(\mathfrak{X})}$. Итак, $\mathfrak{N} \cap \mathfrak{X} = \mathfrak{N}_{\chi(\mathfrak{X})}$.

Следствие 2. *Если $\mathfrak{X}$ — класс Фиттинга, то*

$$\chi(\mathfrak{X}) = \bigcup_{G \in \mathfrak{X} \cap \mathfrak{S}} \pi(G).$$

☐ Пусть $\tau = \bigcup_{G \in \mathfrak{X} \cap \mathfrak{S}} \pi(G)$. Если $p \in \chi(\mathfrak{X})$, то существует группа Z_p простого порядка, принадлежащая $\mathfrak{X}$. Так как $Z_p \in \mathfrak{X} \cap \mathfrak{S}$, то $p \in \tau$. Обратно, если $p \in \tau$, то существует разрешимая группа $G \in \mathfrak{X}$ такая, что $p \in \pi(G)$. По теореме 5.35 получаем, что $\mathfrak{N}_{\pi(G)} \subseteq \mathfrak{X}$ и $p \in \chi(\mathfrak{X})$. Итак, $\chi(\mathfrak{X}) = \tau$. ⊠

Пусть $\mathfrak{X}$ — класс Фиттинга и $\mathfrak{Y}$ — класс групп. *Радикальным произведением* $\mathfrak{X}$ и $\mathfrak{Y}$ называется класс $\mathfrak{X} \diamond \mathfrak{Y} =$

$\{G \in \mathfrak{E} \mid G/G_{\mathfrak{X}} \in \mathfrak{Y}\}$.

Теорема 5.36. *Если $\mathfrak{X}$ и $\mathfrak{Y}$ — классы Фиттинга, то $\mathfrak{X} \diamond \mathfrak{Y}$ — класс Фиттинга и $\mathfrak{X} \subseteq \mathfrak{X} \diamond \mathfrak{Y}$.*

□ Пусть $G \in \mathfrak{X} \diamond \mathfrak{Y}$ и $H \lhd G$. Тогда $H_{\mathfrak{X}} = H \cap G_{\mathfrak{X}}$ и $H/H_{\mathfrak{X}} \simeq HG_{\mathfrak{X}}/G_{\mathfrak{X}} \lhd G/G_{\mathfrak{X}}$. Так как $G/G_{\mathfrak{X}} \in \mathfrak{Y}$ и $\mathfrak{Y}$ — класс Фиттинга, то $H/H_{\mathfrak{X}} \in \mathfrak{Y}$ и $H \in \mathfrak{X} \diamond \mathfrak{Y}$.

Пусть $H_i \in \mathfrak{X} \diamond \mathfrak{Y}$, $H_i \lhd G$, $i = 1, 2$, и $G = H_1H_2$. Тогда $H_iG_{\mathfrak{X}}/G_{\mathfrak{X}} \simeq H_i/H_i \cap G_{\mathfrak{X}} = H_i/(H_i)_{\mathfrak{X}} \in \mathfrak{Y}$ и $G/G_{\mathfrak{X}} = H_1H_2/G_{\mathfrak{X}} = (H_1G_{\mathfrak{X}}/G_{\mathfrak{X}})(H_2G_{\mathfrak{X}}/G_{\mathfrak{X}}) \in \mathfrak{Y}$. Поэтому $G \in \mathfrak{X} \diamond \mathfrak{Y}$ и $\mathfrak{X} \diamond \mathfrak{Y}$ — класс Фиттинга.

Если $G \in \mathfrak{X}$, то $G = G_{\mathfrak{X}}$ и $G/G_{\mathfrak{X}} = E \in \mathfrak{Y}$, т.е. $G \in \mathfrak{X} \diamond \mathfrak{Y}$. Таким образом, $\mathfrak{X} \subseteq \mathfrak{X} \diamond \mathfrak{Y}$.

Теорема 5.37. *Пусть $\mathfrak{X}, \mathfrak{Y}$ и $\mathfrak{Z}$ — классы Фиттинга. Тогда*

1) $(G/G_{\mathfrak{X}})_{\mathfrak{Y}} = G_{\mathfrak{X} \diamond \mathfrak{Y}}/G_{\mathfrak{X}}$;

2) $(\mathfrak{X} \diamond \mathfrak{Y}) \diamond \mathfrak{Z} = \mathfrak{X} \diamond (\mathfrak{Y} \diamond \mathfrak{Z})$.

□ 1. По теореме 5.36 произведение $\mathfrak{X} \diamond \mathfrak{Y}$ — класс Фиттинга и $\mathfrak{X} \subseteq \mathfrak{X} \diamond \mathfrak{Y}$. Поэтому $G_{\mathfrak{X}} \subseteq G_{\mathfrak{X} \diamond \mathfrak{Y}}$, а так как $G_{\mathfrak{X} \diamond \mathfrak{Y}} \in \mathfrak{X} \diamond \mathfrak{Y}$, то $G_{\mathfrak{X} \diamond \mathfrak{Y}}/G_{\mathfrak{X}} \in \mathfrak{Y}$. Отсюда следует, что $G_{\mathfrak{X} \diamond \mathfrak{Y}}/G_{\mathfrak{X}} \subseteq (G/G_{\mathfrak{X}})_{\mathfrak{Y}}$.

Проверим обратное включение. Обозначим $(G/G_{\mathfrak{X}})_{\mathfrak{Y}} = H/G_{\mathfrak{X}}$. Так как $H \lhd G$, то $H_{\mathfrak{X}} \subseteq G_{\mathfrak{X}}$, поэтому $H_{\mathfrak{X}} = G_{\mathfrak{X}}$. Но $H/G_{\mathfrak{X}} \in \mathfrak{Y}$, значит $H \in \mathfrak{X} \diamond \mathfrak{Y}$, т.е. $H/G_{\mathfrak{X}} \subseteq G_{\mathfrak{X} \diamond \mathfrak{Y}}/G_{\mathfrak{X}}$. Таким образом, $(G/G_{\mathfrak{X}})_{\mathfrak{Y}} = (G_{\mathfrak{X} \diamond \mathfrak{Y}})/G_{\mathfrak{X}}$.

2. Пусть $G \in (\mathfrak{X} \diamond \mathfrak{Y}) \diamond \mathfrak{Z}$. Это означает, что $G/G_{\mathfrak{X} \diamond \mathfrak{Y}} \in \mathfrak{Z}$. Но $G/G_{\mathfrak{X} \diamond \mathfrak{Y}} \simeq (G/G_{\mathfrak{X}})/(G_{\mathfrak{X} \diamond \mathfrak{Y}}/G_{\mathfrak{X}}) = (G/G_{\mathfrak{X}})/(G/G_{\mathfrak{X}})_{\mathfrak{Y}}$. Из того, что $(G/G_{\mathfrak{X}})/(G/G_{\mathfrak{X}})_{\mathfrak{Y}} \in \mathfrak{Z}$ следует, что $G/G_{\mathfrak{X}} \in \mathfrak{Y} \diamond \mathfrak{Z}$, $G \in \mathfrak{X} \diamond (\mathfrak{Y} \diamond \mathfrak{Z})$. Аналогично проверяется, что $\mathfrak{X} \diamond (\mathfrak{Y} \diamond \mathfrak{Z}) \subseteq (\mathfrak{X} \diamond \mathfrak{Y}) \diamond \mathfrak{Z}$. ⊠

Пусть $\mathfrak{X}$ и $\mathfrak{Y}$ — произвольные классы групп. Через $Ext_{\mathfrak{X}}\mathfrak{Y}$ обозначим совокупность всех групп, в которых имеется нормальная $\mathfrak{X}$-подгруппа и фактор-группа по ней принадлежит $\mathfrak{Y}$, т.е.

$$Ext_{\mathfrak{X}}\mathfrak{Y} = \{G \in \mathfrak{E} \mid \exists N \lhd G,\ N \in \mathfrak{X},\ G/N \in \mathfrak{Y}\}.$$

Теорема 5.38. *Если $\mathfrak{X}$ — класс групп, замкнутый относительно нормальных подгрупп, и $\mathfrak{Y}$ — формация,* *то* $\mathfrak{X} \circ \mathfrak{Y} = Ext_{\mathfrak{X}}\mathfrak{Y}$.

$\square$ По определению корадикального произведения имеем $\mathfrak{X} \circ \mathfrak{Y} = \{G \in \mathfrak{E} \mid G^{\mathfrak{Y}} \in \mathfrak{X}\}$. Поэтому ясно, что $\mathfrak{X} \circ \mathfrak{Y} \subseteq Ext_{\mathfrak{X}}\mathfrak{Y}$.

Обратно, пусть $G \in Ext_{\mathfrak{X}}\mathfrak{Y}$. Тогда существует нормальная подгруппа $N \in \mathfrak{X}$, для которой $G/N \in \mathfrak{Y}$. Поскольку $\mathfrak{Y}$ — формация, то $G^{\mathfrak{Y}} \subseteq N$, а так как $\mathfrak{X}$ замкнут относительно нормальных подгрупп, то $G^{\mathfrak{Y}} \in \mathfrak{X}$ и $G \in \mathfrak{X} \circ \mathfrak{Y}$.

Теорема 5.39. *Если* $\mathfrak{X}$ *— класс Фиттинга и* $\mathfrak{Y}$ *— гомоморф, то* $\mathfrak{X} \diamond \mathfrak{Y} = Ext_{\mathfrak{X}}\mathfrak{Y}$.

$\square$ По определению радикального произведения имеем $\mathfrak{X} \diamond \mathfrak{Y} = \{G \in \mathfrak{E} \mid G/G_{\mathfrak{X}} \in \mathfrak{Y}\}$. Поэтому ясно, что $\mathfrak{X} \diamond \mathfrak{Y} \subseteq Ext_{\mathfrak{X}}\mathfrak{Y}$.

Обратно, пусть $G \in Ext_{\mathfrak{X}}\mathfrak{Y}$. Тогда существует нормальная подгруппа $N \in \mathfrak{X}$ такая, что $G/N \in \mathfrak{Y}$. Так как $\mathfrak{X}$ — класс Фиттинга, то $N \subseteq G_{\mathfrak{X}}$. Теперь $G/G_{\mathfrak{X}} \simeq (G/N)/(G_{\mathfrak{X}}/N)$, а поскольку $\mathfrak{Y}$ — гомоморф и $G/N \in \mathfrak{Y}$, то $G/G_{\mathfrak{X}} \in \mathfrak{Y}$ и $G \in \mathfrak{X} \diamond \mathfrak{Y}$.

Следствие 1. *Если* $\mathfrak{X}$ *— класс Фиттинга, а* $\mathfrak{Y}$ *— формация, то* $\mathfrak{X} \diamond \mathfrak{Y} = \mathfrak{X} \circ \mathfrak{Y} = Ext_{\mathfrak{X}}\mathfrak{Y}$.

Следствие 2. *Если* $\mathfrak{X}$ *и* $\mathfrak{Y}$ *— радикальные формации, то* $\mathfrak{X} \diamond \mathfrak{Y} = \mathfrak{X} \circ \mathfrak{Y} = Ext_{\mathfrak{X}}\mathfrak{Y}$.

5.5. Инъекторы

Пусть $\mathfrak{X}$ — класс групп. Подгруппа H группы G называется $\mathfrak{X}$-*инъектором*, если для каждой субнормальной подгруппы K группы G пересечение $H \cap K$ является $\mathfrak{X}$-максимальной подгруппой в K.

Лемма 5.40. *Пусть* $\mathfrak{X}$ *— класс групп. Если* H *—* $\mathfrak{X}$*-инъектор группы* G *и* $K \lhd\lhd G$, *то* $H \cap K$ *—* $\mathfrak{X}$*-инъектор подгруппы* K.

$\square$ Пусть $N \lhd\lhd K$. Тогда $N \lhd\lhd G$ и $(H \cap K) \cap N = H \cap N$ $\mathfrak{X}$-максимальна в N. Это означает, что $H \cap K$ — $\mathfrak{X}$-инъектор подгруппы K.

Лемма 5.41. *Пусть $\mathfrak{X}$ — класс групп. Подгруппа H является $\mathfrak{X}$-инъектором группы G тогда и только тогда, когда H $\mathfrak{X}$-максимальна в G и $H \cap K$ — $\mathfrak{X}$-инъектор подгруппы K для всех максимальных нормальных подгрупп K группы G.*

$\square$ Пусть H — $\mathfrak{X}$-инъектор группы G. Тогда H $\mathfrak{X}$-максимальна в G и по лемме 5.40 подгруппа $H \cap K$ — $\mathfrak{X}$-инъектор подгруппы K.

Обратно, пусть H — $\mathfrak{X}$-максимальная подгруппа группы G и $H \cap K$ — $\mathfrak{X}$-инъектор подгруппы K для всех максимальных нормальных подгрупп K группы G. Пусть $N \lhd \lhd G$ и $N \leq L$, L — максимальная нормальная подгруппа группы G. Так как $H \cap L$ — $\mathfrak{X}$-инъектор подгруппы L, то $H \cap L \cap N = H \cap N$ $\mathfrak{X}$-максимальна в N и H — $\mathfrak{X}$-инъектор группы G.

Теорема 5.42. *Пусть $\mathfrak{X}$ — класс групп и $\mathfrak{Y}$ — класс Фиттинга. Если в каждой $\mathfrak{Y}$-группе существует $\mathfrak{X}$-инъектор, то $\mathfrak{X} \cap \mathfrak{Y}$ — класс Фиттинга.*

$\square$ Пусть $G \in \mathfrak{X} \cap \mathfrak{Y}$, $N \lhd \lhd G$. Тогда группа G является своим $\mathfrak{X}$-инъектором. Из определения $\mathfrak{X}$-инъектора получаем, что $G \cap N = N$ — $\mathfrak{X}$-максимальная подгруппа группы N для всех $N \lhd \lhd G$. Поэтому $N \in \mathfrak{X}$, а так как $\mathfrak{Y}$ — класс Фиттинга, то $N \in \mathfrak{X} \cap \mathfrak{Y}$ и первое требование определения класса Фиттинга для $\mathfrak{X} \cap \mathfrak{Y}$ выполняется.

Пусть $N_1, N_2 \lhd G$, $N_1, N_2 \in \mathfrak{X} \cap \mathfrak{Y}$. Тогда $N_1 N_2 \in \mathfrak{Y}$ поскольку $\mathfrak{Y}$ — класс Фиттинга. По условию в группе $N_1 N_2$ существует $\mathfrak{X}$-инъектор, который обозначим через H. По определению $\mathfrak{X}$-инъектора подгруппа $N_i \cap H$ $\mathfrak{X}$-максимальна в N_i, поэтому $N_i \cap H = N_i$ и $N_1 N_2 = H \in \mathfrak{X} \cap \mathfrak{Y}$. Значит для $\mathfrak{X} \cap \mathfrak{Y}$ выполняется и второе требование определения класса Фиттинга.

Следствие. *1. Пусть $\mathfrak{X}$ — класс групп. Если в каждой группе существует $\mathfrak{X}$-инъектор, то $\mathfrak{X}$ — класс Фиттинга.*

2. Разрешимый класс $\mathfrak{X}$, для которого каждая разрешимая группа обладает $\mathfrak{X}$-инъектором, является классом Фиттинга.

$\square$ 1. Утверждение следует из теоремы в случае, когда

$\mathfrak{Y}$ — класс всех групп.

2. Утверждение следует из теоремы в случае, когда $\mathfrak{Y} = \mathfrak{S}$ — класс всех разрешимых групп.

Лемма 5.43. *Пусть $\mathfrak{X}$ — класс Фиттинга и H — $\mathfrak{X}$-максимальная подгруппа группы G. Если $H \leq L \leq N_G(H)$, то $N_G(L) \leq N_G(H)$. В частности, нормализатор $\mathfrak{X}$-максимальной подгруппы самонормализуем.*

□ Если $x \in N_G(L)$, то $H^x \lhd L^x = L$ и $HH^x \in \mathfrak{X}$. Так как H $\mathfrak{X}$-максимальна, то $H = H^x$ и $x \in N_G(H)$.

Лемма 5.44. *Пусть $\mathfrak{X}$ — класс Фиттинга, G — разрешимая группа, N — нормальная подгруппа группы G с абелевой фактор-группой G/N. Пусть W — $\mathfrak{X}$-максимальная подгруппа из N и пусть V_1 и V_2 — $\mathfrak{X}$-максимальные подгруппы группы G, содержащие W. Тогда V_1 и V_2 сопряжены в G.*

□ Воспользуемся индукцией по порядку группы. Так как $N \cap V_i \in \mathfrak{X}$, то $W = N \cap V_i$ и $V_i \leq N_G(W)$ для каждого $i = 1, 2$. Если $N_G(W) \neq G$, то по индукции подгруппы V_1 и V_2 сопряжены в $N_G(W)$ и лемма справедлива. Поэтому следует считать, что подгруппа W нормальна в G. Пусть C_i/W — картерова подгруппа из $M_i/W = N_{G/W}(V_i/W) = N_G(V_i)/W$. По условию леммы фактор-группа G/N абелева. Значит $G' = [G, G] \leq N$ и $[V_i, M_i] \leq N \cap V_i = W$. Отсюда заключаем, что подгруппа V_i/W содержится в центре M_i/W. Но C_i/W самонормализуема в M_i/W, поэтому $V_i \leq C_i$. По лемме 5.43 нормализатор $N_G(C_i) \leq M_i$, поэтому

$$N_G(C_i)/W = N_{M_i}(C_i)/W = N_{M_i/W}(C_i/W) = C_i/W$$

и C_i/W — подгруппа Картера группы G/W. Следовательно, $C_1^x = C_2$ для некоторого элемента $x \in G$. Теперь V_1^x и V_2 — нормальные $\mathfrak{X}$-подгруппы из C_2, поэтому $V_1^x V_2 \in \mathfrak{X}$, $V_1^x = V_2$.

Теорема 5.45. *Если $\mathfrak{X}$ — класс Фиттинга, то в каждой разрешимой группе G существует $\mathfrak{X}$-инъектор и любые два $\mathfrak{X}$-инъектора группы G сопряжены.*

□ Воспользуемся индукцией по порядку группы G. Так как группу G можно считать неединичной, то её коммутант G' по индукции имеет $\mathfrak{X}$-инъектор, который обозначим через W. Через V обозначим $\mathfrak{X}$-максимальную подгруппу группы G, содержащую W. Пусть M — максимальная нормальная подгруппа группы G. Ясно, что $G' \leq M$. По индукции подгруппа M содержит $\mathfrak{X}$-инъектор U. По лемме 5.40 подгруппа $U \cap G'$ — $\mathfrak{X}$-инъектор подгруппы G'. По индукции $U \cap G' = W^x$ для некоторого $x \in G'$. Пусть T — $\mathfrak{X}$-максимальная подгруппа группы G, содержащая U. Теперь $U \leq T \cap M \in \mathfrak{X}$, поэтому $U = T \cap M$. Подгруппы T и V^x содержат $\mathfrak{X}$-максимальную подгруппу W^x коммутанта G'. По лемме 5.44 они сопряжены, т.е. $T^y = V^x$ для некоторого $y \in G$. Теперь $U^y = (T \cap M)^y = T^y \cap M = V^x \cap M$. Следовательно, $V^x \cap M$ — $\mathfrak{X}$-инъектор G по лемме 5.41. Итак, существование $\mathfrak{X}$-инъектора в группе G доказано.

Пусть V_1 и V_2 — $\mathfrak{X}$-инъекторы группы G. Тогда $V_1 \cap G'$ и $V_2 \cap G'$ — $\mathfrak{X}$-инъекторы подгруппы G'. По индукции $V_1 \cap G' = (V_2 \cap G')^g$ для некоторого $g \in G'$. Применяя лемму 5.44 для подгрупп $W = V_1 \cap G' \leq V_1 \cap V_2^g$, получаем, что V_1 и V_2 сопряжены в G.

Теорема 5.46. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — разрешимая группа. Подгруппа H тогда и только тогда является $\mathfrak{X}$-инъектором группы G, когда H $\mathfrak{X}$-максимальна в G и $H \cap G'$ — $\mathfrak{X}$-инъектор коммутанта G'.*

□ Если H — $\mathfrak{X}$-инъектор группы G, то H $\mathfrak{X}$-максимальна в группе G и $H \cap G'$ — $\mathfrak{X}$-инъектор подгруппы G' по лемме 5.40.

Пусть H — $\mathfrak{X}$-максимальная подгруппа группы G и $H \cap G'$ — $\mathfrak{X}$-инъектор в G'. Пусть K — $\mathfrak{X}$-инъектор группы G, он существует по теореме 5.45. По лемме 5.40 пересечение $K \cap G'$ — $\mathfrak{X}$-инъектор подгруппы G'. По теореме 5.45 подгруппы $K \cap G'$ и $H \cap G'$ сопряжены между собой, т.е. существует элемент $g \in G'$ такой, что $H \cap G' = (K \cap G')^g = K^g \cap G'$. Теперь подгруппы H и K^g $\mathfrak{X}$-максимальны в G и содержат $\mathfrak{X}$-максимальную подгруппу $K^g \cap G'$. По лемме 5.44 подгруппы H и K^g сопряжены, поэтому H — $\mathfrak{X}$-инъектор группы G.

Следствие 1. *Пусть $\mathfrak{X}$ — класс Фиттинга и пусть $E = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G$ — ряд с абелевыми факторами G_i/G_{i+1}. Подгруппа H тогда и только тогда является $\mathfrak{X}$-инъектором группы G, когда $H \cap G_i$ является $\mathfrak{X}$-максимальной подгруппой в G_i для всех i.*

$\square$ Если H — $\mathfrak{X}$-инъектор группы G, то $H \cap G_i$ — $\mathfrak{X}$-инъектор подгруппы G_i по лемме 5.40, поэтому $H \cap G_i$ является $\mathfrak{X}$-максимальной подгруппой в G_i для всех i.

Обратно, пусть $H \cap G_i$ является $\mathfrak{X}$-максимальной подгруппой в G_i для всех i. По индукции $H \cap G_1$ — $\mathfrak{X}$-инъектор в G_1. Так как G/G_1 абелева, то $G' \leq G_1$ и подгруппа H — $\mathfrak{X}$-инъектор в G по теореме 5.46.

Следствие 2. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — разрешимая группа. Подгруппа H тогда и только тогда является $\mathfrak{X}$-инъектором в G, когда для любой нормальной подгруппы N группы G пересечение $H \cap N$ является $\mathfrak{X}$-максимальной подгруппой в N.*

$\square$ Пусть H — $\mathfrak{X}$-инъектор в G. Из определения инъектора следует, что пересечение $H \cap N$ $\mathfrak{X}$-максимальна в N для всех $N \lhd G$.

Обратно, пусть для любой нормальной подгруппы N группы G пересечение $H \cap N$ является $\mathfrak{X}$-максимальной подгруппой в N. Тогда, в частности, $H \cap G^{(i)}$ — $\mathfrak{X}$-максимальная подгруппа в $G^{(i)}$ для всех i, где $G^{(i)}$ — i-й коммутант. Теперь для разрешимой группы G и её производного ряда $E = G^{(n)} \lhd G^{(n-1)} \lhd \ldots \lhd G' \lhd G$ выполняются условия следствия 1, поэтому H — $\mathfrak{X}$-инъектор в G.

Следствие 3. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — разрешимая группа. Если H — $\mathfrak{X}$-инъектор группы G и $H \leq K \leq G$, то H — $\mathfrak{X}$-инъектор в K.*

$\square$ Пусть $E = G_n \lhd G_{n-1} \lhd \ldots \lhd G_1 \lhd G_0 = G$ — ряд с абелевыми факторами G_i/G_{i+1} и $K_i = K \cap G_i$. Тогда ряд $E = K_n \lhd K_{n-1} \lhd \ldots \lhd K_1 \lhd K_0 = K$ имеет абелевы факторы K_i/K_{i+1}. Кроме того, $H \cap G_i \leq K \cap G_i \leq G_i$ и $H \cap G_i$ $\mathfrak{X}$-максимальна в G_i. Поэтому $H \cap G_i = H \cap (K \cap G_i) = H \cap K_i$ $\mathfrak{X}$-максимальна в $K \cap G_i = K_i$. Применяя следствие 1 получаем, что H — $\mathfrak{X}$-инъектор в K.

Теорема 5.47. *Пусть $\mathfrak{X}$ — класс Фиттинга и G*

— нильпотентная группа. Подгруппа H группы G $\mathfrak{X}$-максимальна тогда и только тогда, когда H — $\chi(\mathfrak{X})$-холлова подгруппа.

□ Пусть H — $\mathfrak{X}$-максимальная подгруппа группы G. Так как $H \in \mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$, то H будет $\chi(\mathfrak{X})$-подгруппой. Если K — $\chi(\mathfrak{X})$-холлова подгруппа, то $H \leq K \in \mathfrak{N}_{\chi(\mathfrak{X})} = \mathfrak{X} \cap \mathfrak{N}$ и K — $\mathfrak{X}$-подгруппа. Поэтому $H = K$.

Обратно, если H — $\chi(\mathfrak{X})$-холлова подгруппа группы G, то $H \in \mathfrak{N}_{\chi(\mathfrak{X})} = \mathfrak{X} \cap \mathfrak{N}$. Если K $\mathfrak{X}$-максимальна в G и $K \geq H$, то $K \in \mathfrak{X} \cap \mathfrak{N} = \mathfrak{N}_{\chi(\mathfrak{X})}$ и K — $\chi(\mathfrak{X})$-подгруппа. Поэтому $H = K$.

Следствие. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — нильпотентная группа. Подгруппа H группы G является $\mathfrak{X}$-инъектором тогда и только тогда, когда H — $\chi(\mathfrak{X})$-холлова подгруппа.*

Теорема 5.48. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — группа с нильпотентным коммутантом G'. Подгруппа H тогда и только тогда является $\mathfrak{X}$-инъектором группы G, когда H $\mathfrak{X}$-максимальна в G и содержит $\chi(\mathfrak{X})$-холлову подгруппу из G'.*

□ Пусть H — $\mathfrak{X}$-инъектор группы G. Тогда H $\mathfrak{X}$-максимальна в группе G и $H \cap G'$ — $\mathfrak{X}$-инъектор подгруппы G'. Так как подгруппа G' по условию нильпотентна, то $H \cap G' = G'_{\chi(\mathfrak{X})}$ — $\chi(\mathfrak{X})$-холлова подгруппа в G' по следствию теоремы 5.47.

Обратно, пусть H $\mathfrak{X}$-максимальная подгруппа группы G и H содержит $\chi(\mathfrak{X})$-холлову подгруппу группы G'. Пусть K $\mathfrak{X}$-инъектор группы G, он существует по теореме 5.45. Тогда по лемме 5.40 пересечение $K \cap G'$ — $\mathfrak{X}$-инъектор подгруппы G'. По следствию теоремы 5.47 пересечение $K \cap G' = G'_{\chi(\mathfrak{X})}$ является $\chi(\mathfrak{X})$-холловой подгруппой. Теперь K и H сопряжены по лемме 5.44. Значит H — $\mathfrak{X}$-инъектор в G.

Следствие. *Пусть $\mathfrak{X}$ — класс Фиттинга и G — сверхразрешимая группа. Подгруппа H тогда и только тогда является $\mathfrak{X}$-инъектором группы G, когда H $\mathfrak{X}$-максимальна в группе G и содержит $\chi(\mathfrak{X})$-холлову под-*

группу коммутанта.

В группе $S_3 \times Z_2$ подгруппа $H = Z_3 \times Z_2$ является $\mathfrak{N}$-инъектором, где Z_3 — силовская 3-подгруппа из S_3. Но H не является холловой подгруппой.

Пусть $\mathfrak{X}$ — класс групп. Подгруппа H группы G называется $\mathfrak{X}$-*биектором*, если $H \cap N$ $\mathfrak{X}$-максимальна в N для каждой субнормальной подгруппы N, а HK/K $\mathfrak{X}$-максимальна в G/K для каждой нормальной подгруппы K. Ясно, что $\mathfrak{X}$-биектор одновременно является $\mathfrak{X}$-проектором и $\mathfrak{X}$-инъектором группы G. Примерами $\mathfrak{X}$-биекторов служат силовские p-подгруппы групп для класса $\mathfrak{X} = \mathfrak{N}_p$ всех p-групп.

В группе S_4 силовская 2-подгруппа является $\mathfrak{N}$-биектором.

Для класса Шунка $\mathfrak{F}$ каждая разрешимая группа G обладает единственным классом сопряженных $\mathfrak{F}$-проекторов. Если $\mathfrak{F}$ — радикальный класс, т.е. класс Фиттинга, то каждая разрешимая группа содержит единственный класс сопряженных $\mathfrak{F}$-инъекторов. Но наиболее употребительные классы групп являются одновременно и классами Шунка и радикальными классами. Поэтому вполне естественно возникает вопрос о существовании $\mathfrak{F}$-биекторов в разрешимых группах для радикального класса Шунка $\mathfrak{F}$.

Теорема 5.49. *Пусть $\mathfrak{F}$ — радикальный класс Шунка. Тогда в каждой нильпотентной группе G существует $\mathfrak{F}$-биектор H и подгруппа H является $\chi(\mathfrak{F})$-холловой подгруппой.*

□ Утверждение вытекает из следствия теоремы 5.23, с. 175, и следствия теоремы 5.47.

Следствие. *Пусть $\mathfrak{F}$ — радикальная насыщенная формация. Тогда в каждой нильпотентной группе G существует $\mathfrak{F}$-биектор H и подгруппа H является $\chi(\mathfrak{F})$-холловой подгруппой.*

Обозначим через $Proj_{\mathfrak{F}}(G)$ совокупность всех $\mathfrak{F}$-проекторов группы G, а через $Inj_{\mathfrak{F}}(G)$ совокупность всех $\mathfrak{F}$-инъекторов.

Напомним, что метанильпотентной группой называют группу G, в которой имеется нильпотентная нормальная подгруппа N такая, что фактор-группа G/N нильпотентна.

Теорема 5.50. *Пусть $\mathfrak{F}$ — радикальный класс Шунка. Если в метанильпотентной группе G существует $\mathfrak{F}$-биектор H, то H является $\chi(\mathfrak{F})$-холловой подгруппой группы G.*

$\square$ Пусть $H \in Inj_{\mathfrak{F}}(G) \cap Proj_{\mathfrak{F}}(G)$. Так как в разрешимой группе все $\mathfrak{F}$-проекторы и все $\mathfrak{F}$-инъекторы сопряжены между собой, то $Inj_{\mathfrak{F}}(G) = Proj_{\mathfrak{F}}(G)$.

Пусть $K = F(G)$ — подгруппа Фиттинга. Так как $K \cap H$ — $\mathfrak{F}$-инъектор в K, то по следствию теоремы 5.47 подгруппа $K \cap H$ является $\chi(\mathfrak{F})$-холловой подгруппой в K. Так как G/K нильпотентна и HK/K является $\mathfrak{F}$-проектором в G/K, то HK/K будет $\chi(\mathfrak{F})$-холловой подгруппой в G/K по следствию теоремы 5.23, с. 175. Поскольку $HK/K \simeq H/(H \cap K)$, то H — $\chi(\mathfrak{F})$-подгруппа. Кроме того, $\mid G : H \mid = \mid K : (H \cap K) \mid\mid (G/K) : (HK/K) \mid$ и $\mid G : H \mid$ есть $\chi(\mathfrak{F})'$-число. Значит, H — $\chi(\mathfrak{F})$-холлова подгруппа.

Следствие. *Пусть $\mathfrak{F}$ — радикальная насыщенная формация. Если в метанильпотентной группе G существует $\mathfrak{F}$-биектор H, то H является $\chi(\mathfrak{F})$-холловой подгруппой.*

Группа $S_4 \times Z_3$ не является метанильпотентной, но $\mathfrak{N}$-проекторы и $\mathfrak{N}$-инъекторы совпадают между собой и являются нехолловыми подгруппами порядка 24.

Теорема 5.51. *Пусть $\mathfrak{F}$ — радикальный класс Шунка и $\mathfrak{M}$ — нормально наследственный гомоморф, состоящий из разрешимых групп. Если в каждой группе $G \in \mathfrak{M}$ существует $\mathfrak{F}$-биектор, то $\mathfrak{M}_{\chi(\mathfrak{F})} \subseteq \mathfrak{F}$.*

$\square$ Предположим, что $\mathfrak{M}_{\chi(\mathfrak{F})}$ не содержится в $\mathfrak{F}$, и пусть G — группа наименьшего порядка из разности $\mathfrak{M}_{\chi(\mathfrak{F})} \setminus \mathfrak{F}$. Если G имеет простой порядок p, то $p \in \chi(\mathfrak{F})$ и $G \in \mathfrak{N}_p \subseteq \mathfrak{F}$, противоречие. Значит, G — группа непростого порядка и можно выбрать нетривиальную нормальную в G подгруппу N. Так как $N \in \mathfrak{M}$ и N — $\chi(\mathfrak{F})$-подгруппа в G, то $N \in \mathfrak{M}_{\chi(\mathfrak{F})}$ и $N \in \mathfrak{F}$.

Пусть H — $\mathfrak{F}$-биектор в G. Тогда H — $\mathfrak{F}$-инъектор в

G и $N \leq H$. Поскольку H является $\mathfrak{F}$-проектором в G, то H/N $\mathfrak{F}$-максимальна в G/N. Так как $\mathfrak{M}$ — гомоморф, то $G/N \in \mathfrak{M}_{\chi(\mathfrak{F})}$, а по выбору группы G получаем, что $G/N \in \mathfrak{F}$, т.е. $H = G$ и $G \in \mathfrak{F}$, противоречие. Значит, допущение неверно и $\mathfrak{M}_{\chi(\mathfrak{F})} \subseteq \mathfrak{F}$.

Следствие 1. *Если $\mathfrak{F}$ — радикальный класс Шунка, для которого в каждой разрешимой группе существует $\mathfrak{F}$-биектор, то $\mathfrak{F} = \mathfrak{S}_{\chi(\mathfrak{F})}$.*

Следствие 2. *Если $\mathfrak{F}$ — радикальная насыщенная формация, для которой в каждой разрешимой группе существует $\mathfrak{F}$-биектор, то $\mathfrak{F} = \mathfrak{S}_{\chi(\mathfrak{F})}$.*

Для натурального числа k через $\mathfrak{N}^k$ обозначим класс всех разрешимых групп нильпотентной длины $\leq k$. При $k = 1$ имеем класс всех нильпотентных групп, а при $k = 2$ — класс всех метанильпотентных групп.

Лемма 5.52. *Для любого натурального числа k класс $\mathfrak{N}^k$ является радикальной насыщенной наследственной формацией.*

$\square$ Применим индукцию по k. При $k = 1$ имеем класс $\mathfrak{N}$ всех нильпотентных групп, он является насыщенной наследственной формацией и классом Фиттинга. Пусть утверждение справедливо для $k = t$. По следствию 2 теоремы 5.39, с. 186,

$$\mathfrak{N}^t \diamond \mathfrak{N} = \mathfrak{N}^t \circ \mathfrak{N} = Ext_{\mathfrak{N}^t}\mathfrak{N}.$$

Но класс $Ext_{\mathfrak{N}^t}\mathfrak{N}$ состоит из всех разрешимых групп нильпотентной длины $\leq t + 1$, т.е. $Ext_{\mathfrak{N}^t}\mathfrak{N} = \mathfrak{N}^{t+1}$, поэтому

$$\mathfrak{N}^t \diamond \mathfrak{N} = \mathfrak{N}^t \circ \mathfrak{N} = \mathfrak{N}^{t+1}.$$

По следствию теоремы 5.22, с. 174, класс $\mathfrak{N}^{t+1}$ — насыщенная формация, а по теореме 5.36, с. 185, класс $\mathfrak{N}^{t+1}$ радикальный. В силу леммы 4.29, с. 130, $\mathfrak{N}^{t+1}$ — наследственный класс. Следовательно, класс $\mathfrak{N}^{t+1}$ является радикальной насыщенной наследственной формацией.

Лемма 5.53. *Пусть G — разрешимая группа и $1 \leq k \leq n(G)$. Если A — $\mathfrak{N}^k$-проектор группы G, то $n(A) = k$.*

$\square$ Поскольку $\mathfrak{N}^k$ — насыщенная формация, то $\mathfrak{N}^k$-проектор в группе G существует по следствию теоремы 5.21, с. 173. Поскольку $A \in \mathfrak{N}^k$, то $n(A) \leq k$. Если $k = n(G)$, то $A = G$ и утверждение доказано. Пусть $k < n(G)$ и $l = n(G) - k$. По лемме 4.27, с. 129, $G/F_l(G) = k$, а поскольку $AF_l(G)/F_l(G)$ — $\mathfrak{N}^k$-проектор группы $G/F_l(G)$, то $AF_l(G) = G$. Теперь $G/F_l(G) \simeq A/A \cap F_l(G)$, поэтому $n(A/A \cap F_l(G)) = k$ и $n(A) = k$.

Теорема 5.54. *Если в разрешимой группе G существует $\mathfrak{N}^k$-биектор и $k \geq 2$, то $G \in \mathfrak{N}^k$.*

□ Применим индукцию по порядку группы. Пусть B — $\mathfrak{N}^k$-биектор группы G. Нам надо доказать, что $B = G$. Предположим, что $B \neq G$ и пусть $B \leq M \leq \cdot\, G$. Тогда B является $\mathfrak{N}^k$-биектором подгруппы M по лемме 5.18, с. 170, и следствию 3 теоремы 5.46. По индукции $B = M$, следовательно, B — максимальная подгруппа группы G.

Так как B — $\mathfrak{N}^k$-инъектор группы G, то $\mathfrak{N}^k$-радикал $G_{\mathfrak{N}^k} \subseteq B$ и $n(B) = k$. По теореме 4.30, с. 131,

$$n(G) - k = i, \quad i \in \{1, 2\}. \tag{5.3}$$

Поскольку $B/G_{\mathfrak{N}^k}$ — $\mathfrak{N}^k$-проектор группы $G/G_{\mathfrak{N}^k}$, то $n(G/G_{\mathfrak{N}^k}) > k$ и $n(B/G_{\mathfrak{N}^k}) = k$ по лемме 5.53. По теореме 4.30, с. 131,

$$n(G/G_{\mathfrak{N}^k}) - k = j \in \{1, 2\}. \tag{5.4}$$

По лемме 4.27, с. 129, $n(G) = k + n(G/G_{\mathfrak{N}^k})$, а из равенств (5.3) и (5.4) получаем, что $k = i - j \in \{0, -1, 1\}$, противоречие.

Заметим, что в условии теоремы 5.54 требование $k \geq 2$ не является лишним. Для $k = 1$ в симметрической группе S_4 силовская 2-подгруппа является $\mathfrak{N}$-биектором и $S_4 \notin \mathfrak{N}$.

Использованная литература

1. Ведерников В.А. Элементы теории классов групп. Учебное пособие по спецкурсу. — Смоленск: Смоленский гос. пед. ин-т, 1988. 95 с.
2. Милованов М.В., Тышкевич Р.И., Феденко А.С. Алгебра и аналитическая геометрия // Мн.: Аламфея. 2001. — 401с.
3. Монахов В.С. Введение в теорию групп. Тексты лекций по курсу "Алгебра и теория чисел". — Минск: Белорусский гос. ун-т, 1990. 72 с.
4. Шеметков Л.А. Формации конечных групп. — М.: Наука, 1978. 272 с.
5. Шеметков Л.А. Классические факторизации групп и колец. Учебное пособие. — Гомель: Гомельский гос. ун-т, 1979. 64 с.
6. Gaschütz W. Lectures of subgroups of Sylow type in finite soluble groups. Notes on pure mathematics; № 11. — Canberra, Australian National University, 1979. 100 p.
7. Huppert B. Endliche Gruppen I. — Berlin, Heidelberg, New York, 1967. 793 s.

Рекомендуемая литература

8. Белоногов В.А. Задачник по теории групп. — М.: Наука, 2000. 239 с.
9. Богопольский О.В. Введение в теорию групп. — Москва-Ижевск: Ин-т компьютерных исследований, 2002. 148 с.
10. Горенстейн Д., Конечные простые группы: Введение в их классификацию. — М.: Мир, 1985. 352 с.
11. Каморников С.Ф., Селькин М.В. Подгрупповые функторы и классы конечных групп. — Минск: Беларуская навука, 2003. 254 с.
12. Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. — М.: Наука, 1982. 288 с.
13. Кондратьев А.С., Махнев А.А., Старостин А.И. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. Т.24. (Итоги науки и техники. ВИНИТИ АН СССР). М., 1986. С.3-120.
14. Кострикин А.И. Конечные группы. — В сб.: Алгебра. Топология. Геометрия, 1964. (Итоги науки. Серия: Математика. ВИНИТИ АН СССР). М., 1966. С.7-46.

15. Мазуров В.Д. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. Т.14. (Итоги науки и техники. ВИНИТИ АН СССР). М., 1976. С.5-56.
16. Нерешенные вопросы теории групп. Коуровская тетрадь. — Новосибирск: Новосиб. гос. ун-т, 2002. 172 с.
17. Селькин М.В. Максимальные подгруппы в теории классов конечных групп. — Мн.: Беларуская навука, 1997. 144 с.
18. Скиба А.Н. Алгебра формаций. — Мн.: Беларуская навука, 1997. 240 с.
19. Холл Ф. Теория групп. — М.: ИЛ, 1962. 468 с.
20. Чунихин С. А. Подгруппы конечных групп.— Минск: Наука и техника, 1964. 158 с.
21. Чунихин С.А., Шеметков Л.А. Конечные группы. — В сб.: Алгебра. Топология. Геометрия. (Итоги науки и техники. ВИНИТИ АН СССР). М., 1971. С.7-70.
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. Guo W. The Theory of Classes of Groups. — Science Press-Kluwer Academic Publishers, Beijing-New York-Dordrecht-Boston-London, 2000. 258 p.
25. Huppert B., Blackburn N. Finite groups, II. — Berlin–Heidelberg–New York: Springer, 1982. 531 p.
26. Huppert B., Blackburn N. Finite groups, III. — Berlin-Heidelberg-New York: Springer, 1982. 454 p.
27. Kurzweil H., Stellmacher B., Theorie der endlichen Gruppen. Eine Einführung. — Springer-Verlag, Berlin-Heidelberg-New York, 1998. 341 s.
28. Robinson D.J.S. A course in the theory of groups. — Springer-Verlag, Berlin-Heidelberg-New York, 1982. 481 p.
29. 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

$\mathfrak{X}$-биектор, 188
$\mathfrak{X}$-подгруппа, 161
$\mathfrak{X}$-проектор, 161
$\mathfrak{X}$-группа, 154
$\mathfrak{X}$-радикал, 179
π'-подгруппа, 134
π'-число, 134
π-подгруппа, 134
π-число, 134
p-группа, 47
  абелева
    элементарная, 81

автоморфизм, 29, 58
  внутренний, 59
  центральный, 61

гомоморф, 154
гомоморфизм, 54
группа, 7
  p-замкнутая, 120
  абелева, 7
  дисперсивная, 146
  диэдральная, 87
  знакопеременная, 13
  кватернионов, 89
  конечная, 7
  линейная
    общая, 11
    полная , 11
    специальная, 11
  неразрешимая, 118
  нильпотентная, 102
  примарная, 47, 100
  примитивная, 137
  проективная, 93
  простая, 41
  разрешимая, 118
  сверхразрешимая, 142
  симметрическая, 13
  циклическая, 21
    бесконечная, 22
    конечная, 22

длина
  нильпотентная, 126
  производная, 118
добавление, 109
дополнение, 124

изоморфизм, 25
  рядов, 68
инволюция, 87
индекс
  подгруппы, 31
инъектор, 183

класс
  групп, 154
  замкнутый
    относительно нормальных подгрупп, 177
    относительно подгрупп, 154
    относительно подпрямых произведений, 154
    относительно произведений нормальных $\mathfrak{X}$-подгрупп, 177
    относительно прямых произведений, 154
    относительно фактор-групп, 154
  наследственный, 154
    нормально, 177
  насыщенный, 154

примитивно замкнутый, 156
радикальный, 177
смежный
двойной, 33
левый, 30
правый, 30
сопряженных элементов, 10
Фиттинга, 177
Шунка, 156
коммутант, 112
взаимный, 114
коммутатор, 112
корадикал, 158

матрица
верхняя унитреугольная, 89
перестановки, 26
мономорфизм, 55

нормализатор, 37

образ
гомоморфизма, 54
оператор, 64
операция
ассоциативная, 5
бинарная, 5
коммутативная, 5

перестановка, 11
подгруппа, 15
$\mathfrak{X}$-максимальная, 161
$\mathfrak{X}$-покрывающая, 165
π-холлова, 134
гащюцева, 175
дополняемая, 124
допустимая, 64
единичная, 16
картерова, 174
максимальная, 107
максимальная нормальная, 45
нетривиальная, 16
нормальная, 39
минимальная , 79
порожденная множеством, 17
силовская, 51
собственная, 16
сопряженная, 16
субнормальная, 82
тривиальная, 16
Фиттинга, 122
Фраттини, 107
характеристическая, 60
характеристически простая, 60
холлова, 61
циклическая, 20
подмножество
сопряженное, 16
полугруппа, 5
порядок
группы, 7
элемента, 21
преобразование
аффинное прямой, 13
примитиватор, 137
произведение
корадикальное, 159
подгрупп, 35
подпрямое, 76
полупрямое, 87
внешнее, 86
прямое, 71
внешнее , 75
радикальное классов, 181
центральное, 88

решетка
подгрупп, 18
ряд, 67

нормальный, 67
субнормальный, 67
центральный, 106

ступень
нильпотентности, 107
разрешимости, 118

трансверсаль
левая, 32
правая, 31

фактор
главный, 67
композиционный, 67
ряда, 67
фактор-группа, 43
формация, 154
насыщенная, 154

характеристика класса, 158

центр, 19
централизатор, 18
цоколь группы, 79

экспонента, 148
элемент
единичный, 5
необразующий, 108
обратный, 5
сопряженный, 10
эндоморфизм, 62
нулевой, 62
тождественный или единичный, 62
эпиморфизм, 55

ядро
гомоморфизма, 54
подгруппы, 107

Содержание

Условные обозначения **5**

1. Группы и их подгруппы **7**

1 Группы. Примеры групп **7**

2 Подгруппы **17**

3 Циклические группы **22**

4 Изоморфизм групп **27**

5 Смежные классы **32**

6 Нормальные подгруппы и фактор-группы **42**

7 Силовские подгруппы конечных групп **49**

2. Гомоморфизмы и произведения **57**

1 Гомоморфизмы групп **57**

2 Автоморфизмы **61**

3 Эндоморфизмы и операторы **65**

4 Композиционные ряды **70**

5 Прямые произведения **74**

6 Минимальные нормальные подгруппы **82**

7 Полупрямые произведения **87**

8 Линейные группы **92**

3. Абелевы и нильпотентные группы **99**

1 Строение конечных абелевых групп **99**

2 Примарные группы **103**

3 Нильпотентные группы 105

4 Подгруппа Фраттини 110

4. Разрешимые и сверхразрешимые группы 115

1 Коммутант 115

2 Разрешимые группы 120

3 Подгруппа Фиттинга 125

4 Теорема Шура–Цассенхауза 133

5 Холловы подгруппы разрешимых групп 137

6 Примитивные группы 140

7 Сверхразрешимые группы 145

5. Проекторы и инъекторы 157

1 Формации и классы Шунка 157

2 Проекторы 164

3 Картеровы и гащюцевы подгруппы разрешимых групп 177

4 Классы Фиттинга 180

5 Инъекторы 186

Использованная литература 196

Рекомендуемая литература 196

Предметный указатель 198