ФЕДЕРАЛЬНАЯ ЦЕЛЕВАЯ ПРОГРАММА
«ГОСУДАРСТВЕННАЯ ПОДДЕРЖКА ИНТЕГРАЦИИ
ВЫСШЕГО ОБРАЗОВАНИЯ
И ФУНДАМЕНТАЛЬНОЙ НАУКИ
НА 1997-2000 ГОДЫ»

РОССИЙСКАЯ
АКАДЕМИЯ НАУК
УРАЛЬСКОЕ ОТДЕЛЕНИЕ
ИНСТИТУТ
МАТЕМАТИКИ И МЕХАНИКИ

В. А. Белоногов

ЗАДАЧНИК ПО ТЕОРИИ ГРУПП

Рекомендовано
Министерством образования Российской Федерации
в качестве учебного пособия
для студентов высших учебных заведений,
обучающихся по специальности «Математика»

МОСКВА
«НАУКА»
2000

УДК 512
ББК 22.144
Б 43

Издание осуществлено при финансовой поддержке Федеральной целевой программы "Государственная поддержка интеграции высшего образования и фундаментальной науки на 1997–2000 годы"

Белоногов В.А.

Задачник по теории групп. – М.: Наука, 2000. – 239 с.
ISBN 5-02-002533-X

Книга содержит большое число задач по различным разделам теории групп с изложением (без доказательств) основных результатов. Преимущественное внимание уделено теории конечных групп. Автор надеется, что решение предлагаемых задач будет способствовать более глубокому проникновению в теорию.

Для студентов, аспирантов и научных работников, интересующихся теорвей групп в, в частности, для специализирующихся по теории групп.

Без объявления

ISBN 5-02-002533-X © Центр "Интеграция", 2000 год

Содержание

Предисловие 4
Предварительные обозначения 5
§ 1. Определение группы. Изоморфизм 7
§ 2. Подгруппы и смежные классы 18
§ 3. Элемеиты и порождающие множества группы 26
§ 4. Нормальные подгруппы и гомоморфизмы 36
§ 5. Сопряжённость 45
§ 6. Кольца, и группы матриц 55
§ 7. Симметрические и знакопеременные группы 67
§ 8. Группы перестановок. Представления перестановками 75
§ 9. Факторизации групп 84
§ 10. Силовские подгруппы 91
§ 11. Автоморфизмы и эндоморфизмы 99
§ 12. Коммутаторы и коммутант 107
§ 13. Ряды подгрупп. Разрешимые и нильпотентные группы 113
§ 14. Прямые и центральные произведения 122
§ 15. Полупрямые произведения и сплетения 135
§ 16. Свободные группы и определяющие соотношения 142
§ 17. Конечные p-группы 151
§ 18. Автоморфизмы p-групп. Действия групп на p-группах 161
§ 19. Линейные группы 167
§ 20. π-разрешимые и π-скованные группы. Теорема Шура–Цассенхауза 176
§ 21. Перенос и нормальные p-дополнения. Слияние p-элементов 183
§ 22. Представления и характеры конечных групп 190
§ 23. Разные задачи 210
Ответы и подсказки 218
Список обозначений и терминов 231
Литература 239

Предисловие

Эта книга есть сборник задач по различным разделам теории групп.

В начале каждого параграфа имеется небольшое введение, в котором приводятся основные понятия и обозначения, встречающиеся в формулировках задач. Некоторые термины объясняются в задачах. Формулировка задачи либо содержит задание типа "найти...", "вычислить...", "описать..." и т. п., либо представляет собой некоторое утверждение. В последнем случае предполагается, что читатель должен это утверждение доказать.

Среди задач встречаются некоторые утверждения из теории. Они имеют метку "(Т)" или "(Теорема...)". Предполагается, что читатель уже знаком с ними по учебникам (хотя некоторые утверждения можно попробовать доказать самостоятельно); цель здесь – напомнить теорему, которая будет применяться при решении следующих за ней задач. Большинство задач относится к теории конечных групп. Автор надеется, что решение предлагаемых задач будет способствовать более глубокому проникновению в теорию.

В конце книги приведён список основных учебников по теории групп (наиболее полными из них являются [16] и [15]), некоторых монографий по отдельным разделам этой теории, затронутым в книге, и сборников задач ([7], [8], [12], [13], [18]).

Автор заранее благодарен всем читателям, которые пришлют советы по совершенствованию книги или сообщат о замеченных недостатках. Сообщения можно послать по электронной почте (e-mail: belonogov@imm.uran.ru) или по адресу: 620219, г. Екатеринбург, ГСП-384, ул. С. Ковалевской, 16, Институт математики и механики УрО РАН, Белоногову В. А.

Предварительные обозначения

Знаки $\in$, $\subseteq$, $\cap$, $\cup$, $\setminus$, $\varnothing$ имеют обычный теоретико-множественный смысл.

$\dot{\cup}$ – знак объединения попарно непересекающихся множеств.

$|A|$ – мощность множества A.

$\{a_1, \ldots, a_n\}$ – множество элементов $a_1, \ldots, a_n$.

$\dot{\{}a_1, \ldots, a_n\}$ – множество $\{a_1, \ldots, a_n\}$ мощности n (т. е. с $a_i \neq a_j$ при $i \neq j$).

$\{\ldots \mid \ldots\}$ – множество всех ... таких, что ... .

$A := B$ – A есть обозначение для B (читается: A по определению равно B).

$A \times B := \{(a, b) \mid a \in A, b \in B\}$ – декартово произведение множеств A и B.

$f : A \to B$ – другая запись для f, если f – функция (отображение) из A в B, т. е. тройка (A, B, Γ), где A и B – множества, $\Gamma \subseteq A \times B$ и для любого $a \in A$ существует точно один элемент $b \in B$ такой, что $(a, b) \in \Gamma$ (A – область отправления, B – область прибытия и Γ – график функции).

Если f – функция из A в B, $a \in A$ и $C \subseteq A$, то

$f(a)$ или a^f – образ a при f,

$f(C) := \{f(c) \mid c \in C\}$,

$C^f := \{c^f \mid c \in C\}$,

$f|_C$ – ограничение f на C.

$(A \to B \mid a \mapsto \ldots)$ – функция из A в B, сопоставляющая каждому a из A элемент ... .

$a \mapsto \ldots$ $(a \in A)$ – функция $(A \to B \mid a \mapsto \ldots)$, когда B ясно из контекста.

$\mathbf{N}$ – множество всех натуральных чисел.

$\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ – множества (начиная с § 6 – кольца) всех целых, всех рациональных, всех вещественных и всех комплексных чисел соответственно.

Для целых чисел m и n:

(m, n) – наибольший общий делитель m и n,

$[m, n]$ – наименьшее общее кратное m и n,

$m \mid n$ означает, что m делит n,

$\pi(n)$ – множество всех простых делителей числа n.

Всюду, где не оговорено противное,

φ есть *функция Эйлера*, т. е. функция из $\mathbf{N}$ в $\mathbf{N}$ с $\varphi(n) = |\{m \in \{1, \ldots, n\} \mid (m, n) = 1\}|$.

δ_{ij} – число, равное 1 при $i = j$ и равное 0 при $i \neq j$ (i и j – любые объекты).

Если $a \in \mathbf{C}$, то

$|a|$ – модуль a,

$\bar{a}$ – число, комплектно сопряжённое с a.

Перечёркнутый знак бинарного отношения обозначает отрицание этого отношения.

Знак $\Leftrightarrow$ заменяет выражение "если и только если".

Ссылка на k-й пункт задачи $m.n$ обозначается через $m.n(k)$.

Обозначения и термины, вводимые в параграфах, собраны (в том порядке, в котором они появляются в тексте) в "Списке обозначений и терминов" в конце книги.

§ 1. Определение группы. Изоморфизм

Закон f, который каждой паре x, y элементов множества M сопоставляет некоторый элемент из M (обозначаемый через xfy), называется *бинарной операцией* на M.

Множество M с бинарной операцией $*$ на M называется *группой*, если:

1) операция $*$ ассоциативна, т. е. $(a * b) * c = a * (b * c)$ для любых элементов a, b, c из M;

2) в M существует по крайней мере один *нейтральный элемент*, т. е. элемент e такой, что $e * a = a$ для любого элемента a из M;

3) для некоторого фиксированного нейтрального элемента e из M и для любого элемента a из M в M существует элемент, *симметричный* элементу a, т. е. элемент x такой, что $x * a = e$.

Таким образом, *группа* – это пара $(M, *)$, где M – некоторое множество, а $*$ – бинарная операция на M со свойствами 1)–3). Эти свойства называют *аксиомами группы*. В группе имеется только один нейтральный элемент и единственный симметричный элемент любому её элементу (см. задачу 1.1).

Мощность $|M|$ множества M группы $G = (M, *)$ называется *порядком группы* G и обозначается через $|G|$. Если эта мощность конечна, то группа называется *конечной*, в противном случае – *бесконечной*.

Группа $(M, *)$ называется *абелевой* или *коммутативной*, если любые два элемента x и y из M перестановочны, т. е. $x * y = y * x$.

Элементы и подмножества множества M называют (допуская вольность речи) элементами и подмножествами группы $G = (M, *)$ и пишут $x \in G$ и $X \subseteq G$ вместо $x \in M$ и $X \subseteq M$ соответственно. Утверждение "$(M, *)$ – группа" выражают также словами: "M есть группа относительно операции $*$".

При изложении теории групп обычно пользуются *мультипликативным обозначением* групповой операции: операцию называют *умножением* и обозначают знаком $\cdot$ (который соглашаются при желании опускать), нейтральный элемент называют *единичным элементом*, или *единицей*, и обозначают обычно цифрой 1, а элемент, симметричный элементу x, называют *обратным к* x и обозначают через x^{-1}. Иногда используют *аддитивное обозначение*: операцию называют *сложением*

и обозначают знаком +, нейтральный элемент называют *нулевым элементом*, или *нулем*, и обозначают цифрой 0, а элемент, симметричный элементу x, называют *противоположным элементу* x и обозначают через $-x$.

В дальнейшем всюду, где не оговорено противное, принята мультипликативная запись групповой операции. Согласно задаче 1.1 $x1 = 1x = x$ и $xx^{-1} = x^{-1}x = 1$ для всех элементов x группы.

Пусть a – элемент группы. Для любого целого числа n определяется n-ая *степень* a^n элемента a : $a^0 = 1$, $a^{i+1} = a^i a$ при $i \geq 0$, $a^n = (a^{-n})^{-1}$ при $n < 0$. Элемент a называется элементом конечного порядка или *периодическим* элементом, если $a^n = 1$ для некоторого натурального n. Наименьшее n с этим свойством называется *порядком* (или *периодом*) элемента a и обозначается через $o(a)$. Если $a^n \neq 1$ при любом натуральном n, то a называют *элементом бесконечного порядка* (или непериодическим элементом) и пишут $o(a) = \infty$. Элемент порядка 2 называется *инволюцией*. Если G состоит из степеней одного своего элемента a, то G называется *циклической группой* (порождённой элементом a).

Изоморфизмом группы $G = (M, \cdot)$ в группу $H = (N, *)$ называется взаимно однозначное отображение φ из M в N такое, что

$$\varphi(ab) = \varphi(a) * \varphi(b) \text{ для любых } a, b \text{ из } M.$$

Любое отображение M в N называют также отображением G в H. Если существует изоморфизм G *на* H, то группы G и H называют *изоморфными* и пишут $G \simeq H$. Если φ – изоморфизм G в H, то, очевидно, φ переводит единицу группы G в единицу группы H и $\varphi(g^{-1}) = \varphi(g)^{-1}$ для всех $g \in G$. Конечные группы G и H могут быть заданы *таблицами умножения* (см. 1.30). Очевидно, взаимно однозначное отображение φ из G на H является изоморфизмом тогда и только тогда, когда при замене в таблице умножения группы G каждого элемента $g \in G$ элементом $\varphi(g)$ получается таблица умножения группы H.

Важную роль в теории групп играют группы перестановок. *Перестановкой* множества X (или перестановкой элементов множества X) называется взаимно однозначное отображение множества X на себя. Операция последовательного выполнения перестановок называется *умножением* перестановок. Группа вида $(H, \cdot)$, где H – некоторое множество перестановок множества X, а $\cdot$ – умножение перестановок из H, называется *группой перестановок* множества X. Если H состоит из всех перестановок множества X, то $(H, \cdot)$ – группа (1.23). Она называется *симметрической группой* множества X и обозначается через S_X, а при $X = \{1, \ldots, n\}$, где $n \in \mathbf{N}$, также через S_n. Перестановка f конечного множества из n элементов $x_1, \ldots, x_n$ обозначается через

$$f = \begin{pmatrix} x_1 & \ldots & x_n \\ f(x_1) & \ldots & f(x_n) \end{pmatrix}.$$

По теореме Кэли (1.28) каждая группа изоморфна некоторой группе перестановок. Использование перестановок позволяет, в частности при проверке того, что некоторая пара $(X, \cdot)$ есть группа, избежать проверки ассоциативности (см. 1.29, 1.30).

В задачах этого параграфа рассматриваются некоторые конкретные абелевы группы $\mathbf{C}^+$, $\mathbf{R}^+$, $\mathbf{Q}^+$, $\mathbf{Z}^+$, $\mathbf{C}^\cdot$, $\mathbf{R}^\cdot$, $\mathbf{Q}^\cdot$, Z_n и одномерный тор (1.13, 1.14, 1.19, 1.17), а также *обобщенно диэдральные группы* $D(A)$ (1.46) и *общие линейные группы* $GL_n(\mathbf{C})$ (1.48). В задаче 1.32 вводится конструкция *внешнего прямого произведения* групп, позволяющая по заданным группам G и H построить новую группу $G \times H$ более сложного строения.

Множество с ассоциативной бинарной операцией называется *полугруппой* (см. 1.52–1.54).

1.1. (Т) Пусть $G = (M, *)$ – группа. Тогда:

1) G имеет точно один нейтральный элемент e, причем $a * e = a$ для всех $a \in M$;

2) для любого $a \in M$ в M существует точно один элемент x, симметричный a, причем $a * x = e$.

1.2. (Т) Пусть a, b, c – элементы группы. Если $ac = bc$ или $ca = cb$, то $a = b$ (т. е. в группе законны сокращения справа и слева).

1.3. В определении группы вместо существования "левой единицы" и "левых обратных" можно потребовать существование "правой единицы" и "правых обратных". Более точно:

множество M с ассоциативной операцией $\cdot$ является группой тогда и только тогда, когда M имеет элемент e такой, что

а) $ae = a$ для всех $a \in M$,

б) для любого $a \in M$ существует элемент $x \in M$ такой, что $ax = e$.

1.4. Для множества M с ассоциативной операцией $\cdot$ равносильны условия:

(1) $(M, \cdot)$ – группа;

(2) для каждой пары a, b элементов из M каждое из уравнений $ax = b$ и $xa = b$ имеет единственное решение в M;

(3) для каждой пары a, b элементов из M каждое из уравнений $ax = b$ и $xa = b$ имеет по крайней мере одно решение в M.

(Пара $(M, \cdot)$, для которой верно условие (2), называется *квазигруппой*. Таким образом, группа – это квазигруппа с ассоциативной операцией.)

1.5. Пусть M – множество и $\cdot$ – ассоциативная операция на нём. Равносильны условия:

(1) $(M, \cdot)$ – группа;

(2) существует отображение φ из M в M такое, что $(a\varphi(a))b = b = b(a\varphi(a))$ для всех $a, b \in M$.

1.6. Пусть $\cdot$ и $*$ – бинарные алгебраические операции, определенные на множествах M и N соответственно. Пусть φ – взаимно однозначное отображение M на N такое, что

$$\varphi(xy) = \varphi(x) * \varphi(y) \text{ для всех } x, y \in M.$$

Тогда если одна из пар $(M, \cdot)$ и $(N, *)$ является группой, то группой является и другая, а φ есть изоморфизм $(M, \cdot)$ на $(N, *)$.

1.7. Пусть $G = (M, \cdot)$ – группа и $a \in M$. Определим на M новую бинарную операцию $*$ по правилу:

$$x * y = xay \quad (x, y \in M).$$

Тогда $(M, *)$ – группа и $(M, *) \simeq (M, \cdot)$.

1.8. Пусть $(M, \cdot)$ – группа, а α и β – отображения из M в M. Определим на M операцию $*$ правилом: $x * y = \alpha(x)\beta(y)$ для всех $x, y \in M$. Равносильны условия:

(1) $(M, *)$ – группа;

(2) существуют $a, b \in M$ такие, что

$$\alpha(g) = ga \text{ и } \beta(g) = bg \text{ для всех } g \in M.$$

1.9. 1) Пусть $G = (M, \cdot)$ – группа и φ: $M \times M \to M$ – функция с разделяющимися переменными (т. е. существуют функции α и β из M в M такие, что $\varphi(x, y) = \alpha(x)\beta(y)$ для всех $x, y \in M$). Если пара (M, φ) является группой, то существует $a \in M$ такой, что $\varphi(x, y) = xay$ для всех $x, y \in M$ и $(M, \varphi) \simeq (M, \cdot)$.

2) Пусть $G = (M, \cdot)$ – группа и Φ – множество всех функций из $M \times M$ в M с разделяющимися переменными. Тогда по множеству Φ можно ("забыв" операцию $\cdot$) восстановить группу G с точностью до изоморфизма (т. е. построить группу, изоморфную G). (В.К. Ионин)

1.10. Пусть на множестве M определены две алгебраические операции $\cdot$ и $*$ такие, что

$$x \cdot y = y * x \text{ для всех } x \text{ и } y \text{ из } M.$$

Тогда если одна из пар $(M, \cdot)$ и $(M, *)$ – группа, то группой является и вторая, причём $(M, \cdot) \simeq (M, *)$.

1.11. Пусть M – множество с ассоциативной операцией $\cdot$ такой, что для любого $a \in M$ в M существуют элементы e и x такие, что $ea = ae = a$ и $xa = ax = e$. Будет ли $(M, \cdot)$ группой?

1.12. Пусть $\cdot$ – ассоциативная бинарная операция на множестве M.

1) Равносильны условия:

(А) $(M, \cdot)$ – группа;

(Б) существует отображение f множества M на себя такое, что

а) f^2 – тождественное отображение M на M ($f^2(m) = f(f(m))$ при $m \in M$),

б) $f(x \cdot y) = f(y) \cdot f(x)$ для всех $x, y \in M$,

в) существует элемент e в M такой, что $f(x)x = e$ для всех $x \in M$ и $eM = M$.

2) Утверждение 1) станет ложным, если из (Б) убрать условие $eM = M$.

1.13. Пусть M – множество всех комплексных, всех вещественных или всех рациональных чисел, а $+$ и $\cdot$ – обычные операции сложения и умножения в M.

1) $(M, +)$ – абелева группа (обозначаемая через $\mathbf{C}^+$, $\mathbf{R}^+$ и $\mathbf{Q}^+$ соответственно).

2) $(M \setminus \{0\}, \cdot)$ – абелева группа (группа $\mathbf{C}^\cdot$, $\mathbf{R}^\cdot$ или $\mathbf{Q}^\cdot$ соответственно).

3) Указать все элементы конечного порядка в группах $\mathbf{C}^+$ и $\mathbf{C}^\cdot$.

1.14. Множество всех целых чисел с операцией сложения является циклической группой. Она обозначается через $\mathbf{Z}^+$.

1.15. Является ли группой:

а) множество всех положительных вещественных чисел с операцией умножения;

б) множество всех положительных рациональных чисел с операцией умножения;

в) множество всех целых чисел с операцией вычитания;

г) множество всех ненулевых рациональных чисел с операцией деления;

д) множество $\mathbf{N}$ всех натуральных чисел с операцией $*$ такой, что $a * b$ есть максимум чисел a и b;

е) множество $M_{m \times n}(\mathbf{C})$ всех комплексных $m \times n$-матриц ($m, n \in \mathbf{N}$) с операцией сложения матриц;

ё) множество всех направленных отрезков трёхмерного пространства, исходящих из одной точки, с операцией сложения по правилу параллелограмма?

1.16. 1) Мультипликативная группа всех положительных вещественных чисел (см. 1.15, а)) изоморфна группе $\mathbf{R}^+$.

2) Мультипликативная группа всех положительных рациональных чисел (см. 1.15, б)) не изоморфна группе $\mathbf{Q}^+$.

1.17. 1) Группами являются:

а) множество всех комплексных чисел, имеющих единичный модуль, с операцией умножения;

б) полуинтервал [0, 1) в $\mathbf{R}$ с операцией $*$ такой, что $a * b$ есть дробная часть числа $a + b$.

2) Группы пунктов а) и б) изоморфны.

(Всякая изоморфная им группа называется *одномерным тором*.)

1.18. Пусть M – множество всех вещественных чисел x с $|x| < 1$. Определим на M операцию $\oplus$ следующим образом:

$$x \oplus y = \begin{cases} x + y, & \text{если } -1 < x + y < 1, \\ x + y - 1, & \text{если } x + y \geq 1, \\ x + y + 1, & \text{если } x + y \leq -1. \end{cases}$$

1) $(M, \oplus)$ – группа.

2) $(M, \oplus)$ не является одномерным тором (1.17).

1.19. Для любого натурального числа n множество всех комплексных корней степени n из единицы (т. е. множество $\{z_n^m \mid m \in \{0, 1, \ldots, n-1\}\}$, где $z_n = e^{\frac{2\pi i}{n}} \left(= \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \right)$) с обычной операцией умножения комплексных чисел есть циклическая группа порядка n. (Эта группа обозначается через Z_n.)

1.20. Произвольная циклическая группа изоморфна либо $\mathbf{Z}^+$, либо Z_n для некоторого $n \in \mathbf{N}$.

1.21. Любая группа порядка, не превосходящего трёх, является циклической.

1.22. Множество $K = \{e, a, b, c\}$ является группой относительно операции $\cdot$, заданной следующей "таблицей умножения":

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Эта группа абелева, но не циклическая. Вычислить порядки всех её элементов.

1.23. (Т) Пусть X – множество и $n \in \mathbf{N}$.

1) Множество всех перестановок множества X с операцией умножения перестановок есть группа (симметрическая группа S_X).

2) Если $|X| = n$, то $S_X \simeq S_n$ (в частности, $|S_X| = n!$).

3) При $|X| \geq 3$ группа S_X неабелева.

1.24. При любом $n \in \mathbb{N}$ указать подмножество в S_n, которое относительно операции умножения перестановок является циклической группой порядка n.

1.25. 1) Для каждой из групп S_2 и S_3 выписать все элементы и определить их порядки.

2) Записать таблицу умножения группы S_3.

1.26. Шесть функций $x \mapsto x$, $x \mapsto \frac{1}{1-x}$, $x \mapsto \frac{x-1}{x}$, $x \mapsto \frac{1}{x}$, $x \mapsto \frac{x}{x-1}$, $x \mapsto 1-x$ из множества M всех вещественных чисел, отличных от 0 и 1, и M образуют группу относительно операции композиции функций ($fg(x) = g(f(x))$). Установить её изоморфизм с группой S_3.

1.27. Конечное множество A перестановок является группой относительно операции умножения перестановок, если произведение любой пары элементов из A принадлежит A.

1.28. (Теорема Кэли) Пусть G – произвольная группа. Для любого элемента $g \in G$ обозначим через φ_g отображение из G в G, определяемое правилом: $\varphi_g(h) = h \cdot g$ $(h \in G)$. Тогда:

1) φ_g – перестановка множества элементов группы G;

2) множество $\{\varphi_g \mid g \in G\}$ с операцией умножения перестановок есть группа (подгруппа в S_G); обозначим её через R_G;

3) отображение $g \mapsto \varphi_g$ $(g \in G)$ есть изоморфизм G на R_G.

1.29. Пусть $\cdot$ – бинарная алгебраическая операция на множестве M. Каждому элементу a из M поставим в соответствие отображение φ_a: $M \to M$, положив $\varphi_a(b) = ba$ для $b \in M$. Равносильны условия:

(1) $(M, \cdot)$ – группа;

(2) а) для любого $a \in M$ φ_a является перестановкой,

б) $\varphi_a \neq \varphi_b$ для любых различных a, b из M,

в) множество $\{\varphi_a \mid a \in M\}$ относительно операции умножения перестановок является группой.

1.30. Пусть на множестве M, состоящем из n элементов $x_1, \ldots, x_n$, определена бинарная операция $\cdot$ с помощью таблицы умножения:

	x_1	x_2	$\ldots$	x_n
x_1	x_{1_1}	x_{1_2}	$\ldots$	x_{1_n}
x_2	x_{2_1}	x_{2_2}	$\ldots$	x_{2_n}
$\vdots$	$\vdots$	$\vdots$		$\vdots$
x_n	x_{n_1}	x_{n_2}	$\ldots$	x_{n_n}

(т. е. $x_i x_j = x_{i_j}$, где i_j – одно из чисел $1, \ldots, n$).

Равносильны условия:

(1) пара $(M, \cdot)$ является группой;

(2) справедливы утверждения:

а) при любом $i \in \{1, \ldots, n\}$ отображение $\alpha_i = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1_i & 2_i & \ldots & n_i \end{pmatrix}$ есть перестановка (другими словами, каждый элемент из M встречается в каждом столбце таблицы),

б) множество $A = \{\alpha_1, \ldots, \alpha_n\}$ состоит из n элементов (т. е. в таблице нет равных столбцов),

в) произведение любой пары элементов из A лежит в A.

1.31. Если элементы $x_1, \ldots, x_n$, образуют группу, таблица умножения которой дана в задаче 1.30, то $2n$ элементов $x_1, \ldots, x_n, y_1, \ldots, y_n$ образуют группу относительно операции, заданной следующей таблицей:

	x_1	$\cdots$	x_n	y_1	$\cdots$	y_n
x_1	x_{1_1}	$\cdots$	x_{1_n}	y_{1_1}	$\cdots$	y_{1_n}
$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
$\cdot$		$\cdots$		$\cdot$	$\cdots$	$\cdot$
$\cdot$	$\cdot$	$\cdots$			$\cdots$	$\cdot$
x_n	x_{n_1}	$\cdots$	x_{n_n}	y_{n_1}	$\cdots$	y_{n_n}
y_1	y_{1_1}	$\cdots$	y_{1_n}	x_{1_1}	$\cdots$	x_{1_n}
$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$	$\cdots$	$\cdot$
$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$	$\cdots$	
$\cdot$	$\cdot$	$\cdots$	$\cdot$	$\cdot$	$\cdots$	
y_n	y_{n_1}	$\cdots$	y_{n_n}	x_{n_1}	$\cdots$	x_{n_n}

1.32. (Т) Пусть A и B – произвольные группы (с мультипликативным обозначением групповой операции).

1) Множество всех пар (a, b), где $a \in A$ и $b \in B$, с умножением

$$(a, b)(a', b') = (aa', bb')$$

является группой. (Она обозначается через $A \times B$ и называется *(внешним) прямым произведением* групп A и B.)

2) $A \times B \simeq B \times A$.

3) $A \times B \simeq A_1 \times B_1$, если $A \simeq A_1$ и $B \simeq B_1$ (A_1 и B_1 – группы).

1.33. Группа $(M, \cdot)$ задачи 1.22 изоморфна группе $Z_2 \times Z_2$. (Всякая группа, изоморфная $Z_2 \times Z_2$, называется *четверной группой*.)

1.34. $Z_2 \times Z_3 \simeq Z_6$.

1.35. Всякая группа порядка 4 изоморфна либо Z_4, либо $Z_2 \times Z_2$.

1.36. В любой неабелевой группе имеется по крайней мере 6 элементов.

1.37. Существует неабелева группа любого порядка, делящегося на 6.

1.38. Если $G = (M, \cdot)$ – группа, заданная таблицей умножения из 1.30, то группа задачи 1.31 изоморфна группе $G \times Z_2$.

1.39. Пусть $m, n \in \mathbf{N}$. Построить группу перестановок $m + n$ элементов, изоморфную группе $S_m \times S_n$.

1.40. Пусть $M = \{2^a 3^b \mid a, b \in \mathbf{Z}\}$ и $\cdot$ – обычная операция умножения на M.

1) $(M, \cdot)$ – группа.

2) $(M, \cdot) \simeq \mathbf{Z}^+ \times \mathbf{Z}^+$.

1.41. $\dot{\mathbf{C}} \simeq A \times T$, где A – мультипликативная группа всех положительных вещественных чисел (1.15, a)), а T – одномерный тор (1.17).

1.42. Обобщить понятие внешнего прямого произведения групп (1.32) на случай любого конечного числа множителей.

1.43. Пусть $G = (M, +)$, где M – множество всех бесконечных последовательностей $(a_1, a_2, \ldots)$ целых чисел, а $+$ – операция на M, определяемая равенством

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots).$$

Тогда G – группа.

1.44. Пусть M – некоторое множество и $B(M)$ – множество всех его подмножеств. Введем на $B(M)$ операцию Δ по правилу:

$$A \Delta B = (A \cup B) \setminus (A \cap B) \quad (A, B \in B(M)).$$

($A \Delta B$ называется *симметрической разностью* множеств A и B.)

1) $(B(M), \Delta)$ – абелева группа.

2) Решить уравнения $A \Delta X = B$ и $X \Delta A = B$ в группе $(B(M), \Delta)$ (X – неизвестное).

3) Порядок любого неединичного элемента в $(B(M), \Delta)$ равен 2.

1.45. Являются ли группами пары $(B(M), \cup)$, $(B(M), \cap)$ и $(B(M), \setminus)$?

1.46. Пусть A – группа. Положим $D(A) := (M, \cdot)$, где

$$M = \{(a, \varepsilon) \mid a \in A, \ \varepsilon = \pm 1\},$$

а операция · определяется правилом:

$$(a_1, \varepsilon_1)(a_2, \varepsilon_2) = (a_1 a_2^{\varepsilon_1}, \varepsilon_1 \varepsilon_2).$$

1) $D(A)$ является группой тогда и только тогда, когда A абелева. (Группа, изоморфная группе $D(A)$ для некоторой абелевой группы A, называется *обобщённо диэдральной группой*.)

2) Если A – абелева группа, то $D(A) = A_+ \cup A_-$, где $A_+ = \{(a, 1) \mid a \in A\}$, $A_- = \{(a, -1) \mid a \in A\}$, причём A_+ относительно ограничения на нём операции · есть группа, изоморфная A, а A_- состоит из инволюций.

3) Каждый элемент обобщённо диэдральной группы есть либо инволюция, либо произведение двух инволюций.

4) Группа $D(A)$ абелева тогда и только тогда, когда каждый неединичный элемент группы A является инволюцией.

5) Если A и B – абелевы группы и $A \simeq B$, то $D(A) \simeq D(B)$.

1.47. 1) Множество всех пар (a, b) таких, что $a \in \mathbf{R}$ и $b \in \mathbf{R}\backslash\{0\}$, с операцией

$$(a_1, b_1)(a_2, b_2) = (a_1 + b_1 a_2, b_1 b_2)$$

является группой. Обозначим её через G.

2) Найти в G два подмножества, каждое из которых относительно ограничения на нём операции · есть группа, причём одна из них изоморфна группе $\mathbf{R}^+$, а другая – группе $\mathbf{R}^\cdot$.

3) Указать в G все инволюции. Имеет ли G элементы конечного порядка, большего двух?

1.48. 1) Пусть $n \in \mathbf{N}$ и M – множество всех $(n \times n)$-матриц с элементами из множества $\mathbf{R}$ всех вещественных чисел, имеющих ненулевой (соответственно, единичный) определитель. Тогда M с обычной операцией умножения матриц является группой (группы $GL_n(\mathbf{R})$ и $SL_n(\mathbf{R})$ соответственно).

2) Утверждение 1) останется верным, если в нём заменить $\mathbf{R}$ множеством $\mathbf{C}$ всех комплексных чисел (группы $GL_n(\mathbf{C})$ и $SL_n(\mathbf{C})$ соответственно).

1.49. При любом $n \geq 2$ группы $GL_n(\mathbf{R})$, $SL_n(\mathbf{R})$, $GL_n(\mathbf{C})$ и $SL_n(\mathbf{C})$ неабелевы.

1.50. Пусть $a \in \mathbf{R}$ и M_a – множество всех ненулевых матриц вида

$$\begin{pmatrix} x & y \\ ay & x \end{pmatrix},$$

где $x, y \in \mathbf{R}$. При каких a M_a является группой относительно операции умножения матриц?

1.51. Является ли группой множество всех симметрических матриц из $GL_n(\mathbf{C})$ ($n \geq 2$) относительно операции умножения матриц?

1.52. Множество с ассоциативной бинарной операцией называется *полугруппой*. Так же, как и для групп, вводится понятие изоморфизма полугрупп.

1) Если M – произвольное множество и $*$ – операция на M, заданная правилом $x * y = y$, то $(M, *)$ – полугруппа.

2) Для любого множества M пары $(B(M), \cup)$ и $(B(M), \cap)$, где $B(M)$ определено в 1.44, являются полугруппами. Будут ли они изоморфными?

1.53. Каждая конечная полугруппа содержит *идемпотент*, т. е. элемент a такой, что $a^2 = a$.

1.54. Каково максимальное число попарно неизоморфных полугрупп порядка 2?

§ 2. Подгруппы и смежные классы

Если $H = (X, *)$ и $G = (M, \cdot)$ – группы такие, что 1) $X \subseteq M$ и 2) $x * y = x \cdot y$ для любых элементов x и y из X, то говорят, что H есть *подгруппа* группы G, и пишут $H \leq G$. Говорят также, что X *образует подгруппу* в G, или, допуская вольность речи, что X *есть подгруппа* группы G, и пишут $X \leq G$ (что, обычно, не вызывает недоразумений, так как операция на X ясна из указания группы G). Подгруппу $\{1\}$, состоящую из одного лишь единичного элемента, называют *единичной* и обозначают цифрой 1, или, полагаясь на контекст, через 1. Множество всех степеней любого элемента a группы G также является подгруппой в G (2.5), которая обозначается через $\langle a \rangle$. Если $H \leq G$ и $H \neq G$, то говорят, что H – *истинная* подгруппа в G и пишут $H < G$. Если $1 < H < G$, то H называется *собственной* (или *нетривиальной*) подгруппой в G. Подгруппа H группы G называется *максимальной* в G, если H есть истинная подгруппа в G и не является истинной подгруппой никакой истинной подгруппы группы G. Говорят, что подгруппы A и B *взаимно просты*, если $A \cap B = 1$.

Если H – подгруппа группы G и $g \in G$, то подмножество $Hg := \{hg \mid h \in H\}$ называется *правым смежным классом* G *по* H. Множество всех правых смежных классов группы G по подгруппе H обозначается через $G : H$, а его мощность $|G : H|$ называется *индексом* подгруппы H в группе G. Подмножество группы G, содержащее точно один элемент из каждого правого смежного класса по H, называется *правой системой вычетов* G *по* H. Аналогично определяются левые смежные классы gH и левая система вычетов по H. Отметим, что правый смежный класс Hg есть в то же время левый смежный класс $g(g^{-1}Hg)$ по подгруппе $g^{-1}Hg$ (см. 2.18). Подгруппы вида $g^{-1}Hg$ называются *сопряжёнными с* H *в* G и будут специально рассматриваться в § 5.

Множества вида HgK, где H и K – подгруппы группы G и $g \in G$, называются *двойными смежными классами* G по (H, K).

Под произведением $|A||B|$ мощностей множеств A и B понимается мощность их декартова произведения $A \times B$, а неравенство $|A| \leq |B|$ означает, что существует взаимно однозначное отображение A в B. Говорят, что $|A|$ *делит* $|B|$, если $|B| = |A||C|$ для некоторого множества C.

Для любых подмножеств A и B группы G определяются подмножества:

$$AB := \{ab \mid a \in A, b \in B\} - \textit{произведение } A \text{ и } B,$$

$$A^{-1} := \{a^{-1} \mid a \in A\},\ A^n := \underbrace{A \cdots A}_{n \text{ раз}} \text{ при } n \in \mathbf{N}.$$

Понятие *подполугруппы* полугруппы определяется подобно понятию подгруппы.

В задачах этого параграфа вводятся: *группа кватернионов* Q_8 (2.29) и *квазициклическая группа* Z_{p^∞} (2.56).

2.1. Если $H \leq G$, то

1) единица группы H является единицей группы G;

2) элемент, обратный к элементу $h \in H$ в H, является обратным к h в G.

2.2. Пусть X – подмножество группы G. Равносильны условия:

(1) $X \leq G$;

(2) $XX \cup X^{-1} \subseteq X$ (т. е. $xy \in X$ для любых $x, y \in X$ и $x^{-1} \in X$ для каждого $x \in X$);

(3) $XX^{-1} \subseteq X$;

(4) $X^{-1}X \subseteq X$;

(5) $Xx = X$ для любого $x \in X$;

(6) $xX = X$ для любого $x \in X$.

2.3. Пусть X – подмножество группы G такое, что $XX \subseteq X$ (т. е. X – подполугруппа в G).

1) Если X конечно или состоит из периодических элементов, то $X \leq G$.

2) В общем случае X может не быть подгруппой в G.

2.4. Пересечение любого множества подгрупп группы G является подгруппой в G.

2.5. Пусть g – элемент группы G и $\langle g \rangle := \{g^m \mid m \in \mathbf{Z}\}$.

1) $\langle g \rangle$ – (циклическая) подгруппа в G.

2) Если $H \leq \langle g \rangle$ и m – наименьшее натуральное число такое, что $g^m \in H$, то $H = \langle g^m \rangle$.

3) Если $o(g) = n \in \mathbf{N}$, то $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$.

2.6. Может ли бесконечная группа иметь лишь конечное число подгрупп?

2.7. Пусть G – группа, $g \in G$ и $o(g) = n \neq \infty$.

1) Если $g^m = 1$, то $m \mid n$.

2) Если k – целое число, то $o(g^k) = \dfrac{n}{(n,k)}$.

2.8. Пусть $G = \langle a \rangle$ – конечная циклическая группа порядка n и k, $m \in \mathbf{Z}$.

1) $\langle a^m \rangle = \langle a^{(m,n)} \rangle$.

2) $a^k \in \langle a^m \rangle \Leftrightarrow (m, n) \mid k$.

3) Описать множество всех подгрупп группы G. Заметить, что:

а) для любого делителя m числа n группа G имеет точно одну подгруппу порядка m;

б) число всех подгрупп группы G совпадает с числом всех делителей числа n.

4) Указать все максимальные подгруппы группы G и их число.

2.9. (Теорема Лагранжа) Пусть $H \leq G$ и $\{Hg_i \mid i \in J\}$ – множество всех правых смежных классов G по H ($Hg_i \neq Hg_j$ при $i \neq j$). Тогда:

1) $G = \dot{\bigcup}_{i \in J} Hg_i$,

2) $|G| = |H|\,|G : H|$, в частности, если G – конечная группа, то $|H|$ делит $|G|$.

2.10. Получить аналог утверждения 2.9, рассмотрев левые смежные классы вместо правых.

2.11. Порядок элемента конечной группы делит порядок этой группы.

2.12. Группа простого порядка является циклической.

2.13. Определить все подгруппы каждой из групп: Z_4, $Z_2 \times Z_2$, Z_6, S_3.

2.14. Останется ли верным утверждение 1) из 2.3 (хотя бы в случае конечной группы G), если условие $XX \subseteq X$ заменить условием "произведение любой пары *различных* элементов из X принадлежит X"?

2.15. Определить все подгруппы группы $\mathbf{Z}^+$ и их индексы. Указать её максимальные подгруппы. Заметить, что для любого $k \in \mathbf{N}$ группа $\mathbf{Z}^+$ имеет точно одну подгруппу индекса k.

2.16. Группа $\mathbf{Z}^+$ имеет собственные подгруппы и изоморфна каждой из них.

Имеются ли другие группы с этим свойством?

2.17. 1) В циклической группе нет двух подгрупп с равными индексами.

2) Указать систему вычетов $\langle g \rangle$ по $\langle g^m \rangle$ $(m \in \mathbf{Z})$.

2.18. 1) Если $H \leq G$ и $g \in G$, то $g^{-1}Hg := \{g^{-1}hg \mid h \in H\} \leq G$. (Подгруппы вида $g^{-1}Hg$ называются *сопряжёнными* с H в G.)

2) Сопряжённые подгруппы изоморфны и имеют равные индексы в G.

3) Привести пример группы G и её подгруппы H в случаях, когда

а) H имеет несовпадающие с ней сопряжённые подгруппы,

б) H не имеет несовпадающих с ней сопряжённых подгрупп.

2.19. Пусть A и B – подгруппы группы G. Равносильны условия:

(1) $AB \subseteq BA$;

(2) $AB = BA$;

(3) $AB \leq G$.

2.20. (Закон Дедекинда) Пусть A, B, H – подгруппы группы G такие, что $G = AB$ и $A \leq H \leq G$. Тогда $H = A(B \cap H)$.

2.21. Пусть A и B – множества периодических элементов группы G и $ABA \subseteq A$. Тогда AB и BA – подгруппы в G, а A есть левый смежный класс по BA и правый смежный класс по AB.

2.22. Пусть A и B – конечные подмножества группы G. Равносильны условия:

(1) $ABA \subseteq A$;

(2) $A \leq G$ и $B \subseteq A$.

2.23. Может ли какая-либо группа быть теоретико-множественным объединением двух своих истинных подгрупп?

2.24. Пусть A, B, C, D – подгруппы группы G такие, что

$$A \cup B = C \cup D.$$

Тогда

либо $\{A, B\} = \{C, D\}$,

либо левая и правая части равенства – подгруппы в G (и тогда левая часть совпадает с A или B, а правая – с C или D).

2.25. Пусть группа G имеет подгруппы A и B такие, что разность $G \setminus A \cup B$ состоит из конечного числа k-элементов.

1) Группа G конечна.

2) $|A \cap B|$ делит k и $k \geq |(A \setminus A \cap B)(B \setminus A \cap B)|$.

3) Какова группа G при $k \in \{1, 2\}$?

2.26. Определить все группы, которые

а) не имеют собственных подгрупп,

б) имеют точно одну собственную подгруппу,

в) имеют точно две собственные подгруппы,

г) имеют точно три собственные подгруппы.

2.27. Определить конечные группы, имеющие

а) точно одну максимальную подгруппу,

б) точно две максимальные подгруппы.

2.28. Пусть n – натуральное число и M – множество всех $n\times n$-матриц, составленных из чисел 0 и 1, в любой строке и любом столбце которых имеется точно одна единица. Тогда M – подгруппа в $GL_n(\mathbf{C})$, изоморфная симметрической группе S_n.

2.29. Восемь матриц

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

где $i^2 = -1$, образуют подгруппу группы $GL_2(\mathbf{C})$. (Эта группа обозначается через Q_8, а всякая изоморфная ей группа называется *группой кватернионов*.)

2.30. Пусть $M = \{1, -1, i, j, k, -i, -j, -k\}$ (здесь знак "–" служит лишь различительным знаком при задании некоторых элементов) и $\cdot$ – бинарная операция на M, заданная таблицей:

$\cdot$	1	-1	i	j	k	$-i$	$-j$	$-k$
1	1	-1	i	j	k	$-i$	$-j$	$-k$
-1	-1	1	$-i$	$-j$	$-k$	i	j	k
i	i	$-i$	-1	k	$-j$	1	$-k$	j
j	j	$-j$	$-k$	-1	i	k	1	$-i$
k	k	$-k$	j	$-i$	-1	$-j$	i	1
$-i$	$-i$	i	1	$-k$	j	-1	k	$-j$
$-j$	$-j$	j	k	1	$-i$	$-k$	-1	i
$-k$	$-k$	k	$-j$	i	1	j	$-i$	-1

1) $(M, \cdot)$ – группа, изоморфная Q_8.

2) Определить порядки всех элементов этой группы и все её подгруппы.

2.31. Пусть A и B – подгруппы группы G.

1) Если $Ag \subseteq Bh$ для некоторых $g, h \in G$, то $A \le B$.

2) Если A_1 и B_1 – объединения некоторых множеств правых смежных классов по подгруппам A и B соответственно, то $A_1 \cap B_1$ есть объединение некоторого множества правых смежных классов по $A \cap B$.

2.32. Пусть M – подмножество группы G. Равносильны условия:

(1) для любого $g \in G$ либо $gM = M$, либо $gM \cap M = \varnothing$;

(2) $MM^{-1}M = M$;

(3) M есть смежный класс по некоторой подгруппе из G.

2.33. Если множество M периодических элементов группы G таково, что $M^n = M$ для некоторого $n \ge 2$, то $M^{n-1} \le G$ и M – смежный класс по M^{n-1}.

2.34. Пусть M – подмножество группы G. Тогда множество $H := \{g \in G \mid Mg = M\}$ является подгруппой в G, причём $MH = M$ и если $|M|$ конечен, то $|H|$ делит $|M|$.

2.35. Если подмножество M группы G является объединением некоторого множества левых смежных классов по подгруппе H_1 и одновременно является объединением некоторого множества левых смежных классов по подгруппе H_2, то G является объединением некоторого множества левых смежных классов по подгруппе $\langle H_1, H_2\rangle$.

2.36. Для конечных подмножеств A и B группы G равносильны условия:

(1) $|AB| = |A|$;

(2) A является объединением нескольких левых смежных классов по подгруппе $\langle BB^{-1}\rangle$.

2.37. Если M – конечное подмножество группы G, то

$$\bigcap_{m\in M} Mm^{-1} \text{ и } \bigcap_{m\in M} m^{-1}M - \text{ подгруппы в } G.$$

2.38. Пусть $H \le G$ и $g \in G$. Равносильны условия:

(1) $gHg \subseteq H$;

(2) $H \cup gH \le G$.

2.39. Если группа G является объединением конечного числа смежных классов по подгруппам $H_1, \dots, H_n$ ($n \in \mathbf{N}$), то по крайней мере одна из этих подгрупп H_i имеет конечный индекс в G.

2.40. Произведение $A_1 \dots A_n$ подмножеств $A_1, \dots, A_n$ группы G называется *точным произведением* и обозначается через $A_1 \circ \dots \circ A_n$, если каждый элемент x из $A_1 \dots A_n$ имеет единственную запись вида $x = a_1 \dots a_n$, где $a_i \in A_i$ $(1 \le i \le n)$.

1) Если $A \le G$, то равенство $G = A \circ S$ (соответственно, $G = S \circ A$) равносильно утверждению, что S есть некоторая правая (соответственно, левая) система вычетов G по A.

2) Произведение подгрупп A и B является точным тогда и только тогда, когда $A \cap B = 1$.

3) Произведение конечных подмножество $A_1, \dots, A_n$ группы G является точным тогда и только тогда, когда $|A_1 \dots A_n| = |A_1| \dots |A_n|$.

4) $(A \circ B) \circ C = A \circ (B \circ C)$, т.е. если $ABC = (A \circ B) \circ C$, то $ABC = A \circ (B \circ C)$, и обратно; при этом $ABC = A \circ B \circ C$.

5) Если $A = A_1 \circ \cdots \circ A_n$, $B = B_1 \circ \cdots \circ B_m$ и $AB = A \circ B$, то $AB = A_1 \circ \cdots \circ A_n \circ B_1 \circ \cdots \circ B_m$.

6) $x(A \circ B)y = (xA) \circ (By)$ при любых $x, y \in G$.

2.41. Пусть φ – изоморфизм группы G в группу H и $A \leq B \leq G$. Тогда $A^{\varphi} \leq B^{\varphi} \leq H$ и $|B^{\varphi} : A^{\varphi}| = |B : A|$.

2.42. $\mathbf{Z}^+ \times \mathbf{Z}^+ \not\cong \mathbf{Z}^+$.

2.43. Пусть $A \leq B \leq G$. Показать, что из $G = S_1 \circ B$ и $B = S_2 \circ A$ ($S_1 \subseteq G$, $S_2 \subseteq G$) следует $G = (S_1 \circ S_2) \circ A$. В частности, $|G : A| = |G : B| \cdot |B : A|$.

2.44. Пусть A и B – подгруппы группы G.

1) Если $A = S \circ (A \cap B)$, то $AB = S \circ B$.

2) Если $AB = S \circ B$ и $S \subseteq A$, то $A = S \circ (A \cap B)$.

3) Если A и B конечны, то

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

2.45. Если A и B – подгруппы G, то из $A = (A \cap B) \circ S_1$ и $B = (A \cap B) \circ S_2$ следует, что $AB = (A \cap B) \circ (S_1 \circ S_2)$.

Получить аналог этого утверждения для левых систем вычетов.

2.46. 1) Пусть H – подгруппа конечного индекса n группы G. Тогда для любой подгруппы A из G индекс $|A : A \cap H|$ также конечен и не превосходит n. При этом $|A: A \cap H| = n$ тогда и только тогда, когда $AH = G$.

2) Если A, B, C – подгруппы группы G и $A \leq B$, то $|B \cap C : A \cap C| \leq |B : A|$.

2.47. Если подгруппы A и B имеют конечные индексы в группе G, то их пересечение $A \cap B$ также имеет конечный индекс в G, причём

$$|G : A \cap B| \leq |G : A| \cdot |G : B|.$$

Равенство здесь имеет место тогда и только тогда, когда $G = AB$.

2.48. Если $A_1 \leq A \leq G$ и $B_1 \leq B \leq G$, то

$$|A \cap B : A_1 \cap B_1| \leq |A : A_1|\,|B : B_1|$$

2.49. Пусть H – подгруппа группы G и $G = H \circ T$, где $T \subseteq G$. Если $TT \subseteq T$, то T – подгруппа в G.

2.50. Пусть G – группа и T – левый смежный класс группы G по некоторой ее неединичной подгруппе. Предположим, что T при замене любого его элемента любым элементом из $G \backslash T$ снова будет смежным классом группы G. Найти строение G.

2.51. Пусть A и B – подгруппы группы G. Тогда различные двойные смежные классы AgB ($g \in G$) попарно не пересекаются.

2.52. Пусть $A_1 g B_1 \subseteq AhB$, где A_1, B_1, A, B – подгруппы и g, h – элементы группы G. Верно ли, что $A_1 \leq A$ и $B_1 \leq B$?

2.53. Пусть A и B – подгруппы группы G и $g \in G$.

1) $AgB = A \circ S$, где $S \subseteq G$ и $|S| = |B : B \cap g^{-1}Ag|$.

2) $AgB = T \circ B$, где $T \subseteq G$ и $|T| = |A : gBg^{-1} \cap A|$.

3) Если $Ag_1B, \ldots, Ag_nB$ – все двойные смежные классы G по (A, B), то

$$|G : A| = \sum_{i=1}^{n} |B : B \cap g_i^{-1}Ag_i|.$$

2.54. Пусть H и K – подгруппы конечных и равных между собой порядков в группе G (в частности, может быть $H = K$). Тогда G имеет подмножество S такое, что

$$G = H \circ S = S \circ K,$$

т. е. существует общая система представителей левого разложения G по H и правого разложения G по K.

2.55. Не всегда из $G = H \circ S$, где $H \leq G$ и $S \subseteq G$, следует, что $G = S \circ H$ (даже для конечной группы G).

2.56. 1) Множество всех элементов группы $\mathbf{C}^*$, порядки которых есть степени данного простого числа p, является в ней подгруппой. (Эта группа обозначается через Z_{p^∞}, а всякая изоморфная ей группа называется *квазициклической p-группой* (или *группой типа* p^∞).)

2) $Z_{p^\infty} = \bigcup_{n=1}^{\infty} Z_{p^n}$.

3) Z_{p^∞} есть бесконечная группа, все истинные подгруппы которой конечны.

4) Имеет ли группа Z_{p^∞} максимальные подгруппы?

2.57. Пусть в группе G даны подгруппы $H_1, H_2, \ldots, H_n, \ldots$, составляющие возрастающую последовательность, т. е. такие, что $H_n \subset H_{n+1}$ для любого $n = 1, 2, \ldots$. Тогда $\bigcup_{n=1}^{\infty} H_n$ также является подгруппой в G.

2.58. Какие из следующих групп являются объединением возрастающей последовательности своих истинных подгрупп: $\mathbf{Z}^+$, $\mathbf{Q}^+$, Z_{p^∞}, группа с конечным порождающим множеством, подгруппа группы $\mathbf{C}^*$, состоящая из всех её периодических элементов?

2.59. В группе $\mathbf{Q}^+$ каждая подгруппа является либо бесконечной циклической группой, либо объединением возрастающей последовательности бесконечных циклических групп.

2.60. Группа $\mathbf{Q}^+$ не имеет истинных подгрупп конечного индекса. Имеются ли в $\mathbf{Q}^+$ максимальные подгруппы?

§ 3. Элементы и порождающие множества группы

Пусть X – подмножество группы G. Пересечение всех подгрупп группы G, содержащих X, есть подгруппа в G (3.1), которая называется *подгруппой, порождённой множеством* X, и обозначается через $\langle X \rangle$. Очевидно, $\langle \varnothing \rangle = \{1\}$ и $\langle X \rangle = \langle X^{-1} \rangle$, где $X^{-1} = \{x^{-1} \mid x \in X\}$. Если $G = \langle X \rangle$, то говорят, что X есть *порождающее множество* группы G, или, что G *порождается множеством* X, или, что G *порождается элементами множества* X. Если $X = \{a, b, \ldots\}$ или $X = X_1 \cup X_2 \cup \ldots$, то вместо $\langle X \rangle$ пишут $\langle a, b, \ldots \rangle$ или $\langle X_1, X_2, \ldots \rangle$ соответственно. (Это не противоречит введенному в § 1 обозначению $\langle g \rangle$ ввиду 3.1).

При изучении группы важным является выявление перестановочности определённых её элементов. В связи с этим рассматриваются следующие подгруппы (3.18):

$C_G(g) := \{x \in G \mid xg = gx\}$ – *централизатор элемента* g в G ($g \in G$), и

$Z(G) := \bigcap\limits_{g \in G} C_G(g)$ – *центр группы* G.

Пусть π – множество простых чисел. Элемент группы называется *π-элементом*, если он имеет конечный порядок, все простые делители которого лежат в π. Группа, состоящая из π-элементов, называется *π-группой*. При $\pi = \{p\}$ в этих терминах вместо π пишется p. p-элементы при любом простом p называются *примарными* элементами. Важными подгруппами конечной группы G являются её силовские подгруппы. Если p^a – наивысшая степень простого числа p, делящая $|G|$, и $a \in \mathbf{N}$, то любая подгруппа из G порядка p^a называется её *силовской p-подгруппой*. В 3.8 утверждается, что конечная абелева группа имеет силовскую p-подгруппу для любого простого p, делящего её порядок. (Такие подгруппы существуют в любой конечной группе; см. 5.17 и 10.1.) Неединичная абелева группа, все неединичные элементы которой имеют простой порядок p, называется *элементарной абелевой p-группой*. Положим

$$E_{p^n} := \underbrace{Z_p \times \ldots \times Z_p}_{n \text{ раз}} \quad (p \text{ – простое число}, n \in \mathbf{N}).$$

Напомним, что $o(g)$ обозначает порядок элемента g группы.

В задачах этого параграфа вводятся *диэдральные группы* D_{2n} и D_∞ (3.42, 3.43) и группа p-ичных дробей $\mathbf{Q}(p)$ (3.61). Появляются здесь

также элементы вида $x^{-1}gx$, где $g, x \in G$, называемые *сопряжёнными с g в G*. (Систематическому рассмотрению сопряжённых элементов посвящен § 5.)

3.1. Если X – подмножество группы G, то

$$\langle X \rangle = \{1, x_1 \dots x_s \mid x_i \in X \cup X^{-1}, s = 1, 2, \dots\}.$$

3.2. Группа имеет порождающее множество мощности 1 если и только если она – циклическая.

3.3. 1) Пусть $n \in \mathbf{N}$, $g \in G$ и $o(g) = n$. Если $m \in \mathbf{N}$ и $(m, n) = 1$, то существует $t \in \mathbf{N}$ такое, что $g^{mt} = g$ и, следовательно, $mt \equiv 1 (mod\ n)$.

2) Пусть $m, n \in \mathbf{N}$. Тогда существуют целые числа x и y такие, что $(m, n) = xm + yn$.

3.4. Пусть $G = \langle a \rangle$ – циклическая группа ($a \in G$) и $H \leq G$.

1) Если $H = \langle a^{m_1}, a^{m_2}, \dots \rangle$, где $\{m_1, m_2, \dots\} \subseteq \mathbf{Z}$, то $H = \langle a^d \rangle$, где d есть наибольший общий делитель чисел $m_1, m_2, \dots$.

2) $\langle a^k \rangle \cap \langle a^l \rangle = \langle a^{[k,l]} \rangle$ при любых $k, l \in \mathbf{Z}$, где $[k, l] = |kl|/(k, l)$ (наименьшее общее кратное k и l).

3) Указать все элементы, каждый из которых порождает G. Заметить, что если $|G| = n$, то число таких элементов равно $\varphi(n)$, где φ – функция Эйлера (т.е. $\varphi(n) = |\{m \in \mathbf{N} \mid m \leq n, (m, n) = 1\}|$).

4) Если $|G : H| = m$, то всякий порождающий элемент группы H является m-ой степенью некоторого порождающего элемента группы G.

5) Выписать все элементы группы G, не являющиеся квадратами никаких элементов из G.

3.5. Если группа имеет периодическую подгруппу конечного индекса, то она сама периодическая.

3.6. Пусть π – множество простых чисел и G – абелева группа, порождённая некоторым множеством π-элементов.

1) G есть π-группа.

2) Если G конечна, то все простые делители её порядка лежат в π.

3) Показать, что для неабелевой группы G утверждение 1) может быть неверным.

3.7. Пусть a – элемент некоторой группы G, порядок которого равен mn, где $(m, n) = 1$. Тогда в G существует точно одна пара элементов g, h такая, что

$$a = gh = hg, \quad o(g) = m, \quad o(h) = n,$$

причём g и h являются степенями элемента a и $\langle a \rangle = \langle g \rangle \langle h \rangle$.

3.8. Пусть G – конечная абелева группа.

1) Если $|G| = mn$, где $(m, n) = 1$, то G имеет точно одну подгруппу M порядка m и точно одну подгруппу N порядка n. При этом $G = MN$.

2) Если $|G| = p_1^{a_1} \dots p_s^{a_s}$, где $p_1, \dots, p_s$ – различные простые числа и $a_i \in \mathbf{N}$, то $G = P_1 \dots P_s$, где P_i – (единственная) подгруппа порядка $p_i^{a_i}$ (силовская p_i-подгруппа) в G $(i = 1, \dots, s)$.

3) Записать разложение группы G в произведение её силовских подгрупп P_i (как в 2)) для $G \in \{Z_{30}, Z_{61}, Z_{10} \times Z_{60}\}$.

4) G имеет элемент, порядок которого делится на порядок любого элемента из G.

3.9. 1) Привести пример конечной группы G и её истинной подгруппы H таких, что $G \setminus H$ не содержит элементов простого порядка.

2) Существует ли конечная группа G с истинной подгруппой H такой, что $G \setminus H$ не содержит примарных элементов (т. е. элементов, порядок которых есть степень простого числа)?

3.10. Группа S_3 порождается двумя элементами a и b, удовлетворяющими соотношениям (равенствам)

$$a^2 = 1, \quad b^3 = 1, \quad (ab)^2 = 1.$$

3.11. В группе S_4 рассмотрим элементы

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

1) $\langle a \rangle \langle b \rangle$ – силовская 2-подгруппа в S_4.

2) Указать некоторую силовскую 3-подгруппу в S_4.

3) Группа S_4 порождается двумя элементами x и y, удовлетворяющими соотношениям

$$x^4 = 1, \quad y^3 = 1, \quad (xy)^2 = 1.$$

3.12. Какие из следующих отображений являются взаимно однозначными отображениями из G на G для любой группы G?

1) $g \mapsto g^{-1}$ $(g \in G)$.

2) $g \mapsto g^2$ $(g \in G)$.

3) $g \mapsto ag$ $(g \in G)$ при фиксированном $a \in G$.

4) $g \mapsto a^{-1}ga$ $(g \in G)$ при фиксированном $a \in G$.

Какие из этих отображений являются изоморфизмами: а) любой группы G, б) любой абелевой группы G?

3.13. 1) В конечной группе чётного порядка всегда есть инволюция. Более того, число её инволюций нечётно.

2) В любой конечной группе число элементов порядка n при каждом $n > 2$ чётно.

3.14. Если все неединичные элементы группы G имеют порядок 2, то эта группа абелева.

3.15. Конечная элементарная абелева p-группа, где p – простое число, изоморфна E_{p^n} для некоторого $n \in \mathbf{N}$.

3.16. Найти число подгрупп порядка p^m в группе E_{p^n} $(m \le n)$.

3.17. Пусть G – группа нечётного порядка.

1) Каждый её элемент является квадратом некоторого элемента.

2) Пусть a – некоторый фиксированный элемент из G. Тогда каждый элемент g из G единственным образом представляется в виде:

$$g = xax, \text{ где } x \in G.$$

3.18. Пусть $a \in G$ и $X \subseteq G$. Тогда множество

$C_G(X) := \{g \in G \mid xg = gx \text{ для всех } x \in X\}$

есть подгруппа в G. В частности, $C_G(a)$ и $Z(G)$ – подгруппы в G.

3.19. Может ли $Z(G)$ быть максимальной подгруппой в G?

3.20. Если $H \le G$, то $C_G(C_G(C_G(H))) = C_G(H)$.

3.21. Найти централизаторы элементов:

а) $x = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ и $y = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ в группе $GL_2(\mathbf{C})$,

б) $z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ в группе $GL_3(\mathbf{C})$.

3.22. Пусть A и B – конечные подмножества группы G. Тогда

$$\sum_{a \in A} |B \cap C_G(a)| = \sum_{b \in B} |A \cap C_G(b)|.$$

3.23. Пусть φ – изоморфизм группы G на группу H.

1) $Z(G)^\varphi = Z(H)$.

2) $C_G(X)^\varphi = C_H(X^\varphi)$ для любого подмножества X из G.

3.24. 1) Группа $SL_2(\mathbf{C})$ имеет точно одну инволюцию.

2) Найти все инволюции группы $GL_2(\mathbf{C})$.

3.25. Пусть a и b – элементы группы G.

1) $o(a) = o(a^{-1})$.

2) Если $b = g^{-1}ag$ для некоторого $g \in G$ (т. е. b сопряжён с a в G), то $o(a) = o(b)$.

3) $o(ab) = o(ba)$.

4) Если группа G имеет только одну инволюцию t, то $t \in Z(G)$.

3.26. 1) Пусть a, b, c – инволюции некоторой группы. Тогда все элементы группы, получающиеся из произведения abc перестановкой множителей, имеют равные порядки.

2) Для произвольных элементов a, b, c группы может быть $o(abc) \neq o(cba)$. (Рассмотреть группу S_4.)

3.27. Пусть $G = \langle a, b \rangle$, где $a^{-1}ba = b^{-1}$ и $b^{-1}ab = a^{-1}$. Тогда $a^4 = b^4 = 1$. Если при этом $a \neq 1 \neq b$, то G изоморфна $Z_2 \times Z_2$ или Q_8.

3.28. Если x, y – неединичные периодические элементы группы G такие, что $x^{-1}yx = y^{-1}$, то хотя бы один из элементов x и y имеет чётный порядок.

3.29. Пусть $G = \langle a, b \rangle$ и $bab = a$, то $a^2 \in Z(G)$.

3.30. Если $a, b \in G$, $a^4 = b^4 = 1$ и $ba = a^2b^2$, то $ab = (ba)^2$ и $(ba)^5 = 1$.

3.31. Если $a, b \in G$ и $ba = a^2b^2$, то

1) $ba^2 = a^{2n}(ba^2)b^{2n}$ при любом целом n,

2) a^2 и b^2 имеют равные порядки,

3) ab^4 и a^4b имеют равные порядки.

3.32. Если a и b – элементы группы такие, что $ba = a^4b^3$, то $o(a^4b) = o(a^2b^3)$.

3.33. Если $a, b \in G$ и $ba = a^mb^n$ ($m, n \in \mathbb{Z}$), то элементы a^mb^{n-2}, $a^{m-2}b^n$ и ab^{-1} имеют равные порядки.

3.34. Если $a, b \in G$, $a^6 = 1$ и $ba = a^4b$, то $a^3 = 1$ и $ab = ba$.

3.35. Пусть a и b – периодические элементы группы и $n \in \mathbb{N}$.

1) Если $a^n = b^n$, то $[n, o(a)] = [n, o(b)]$.

2) Если $o(a) = p^\alpha$ и $o(b) = p^\beta$, где p – простое число и $\alpha, \beta \in \mathbb{N}$, и если $a^n = b^n \neq 1$, то $o(a) = o(b)$.

3.36. Если A и B – подгруппы группы G и $B \not\subseteq A$, то $\langle B \setminus A \rangle = B$.

3.37. Пусть G – группа, в которой среди любых трёх элеменов найдутся два перестановочных между собой. Тогда G абелева.

3.38. Пусть A и B – истинные подгруппы (циклической) группы G такие, что любой элемент из G, не порождающий G, лежит в $A \cup B$. Какова G?

3.39. Каждая группа имеет порождающее множество, порядки элементов которого либо все конечны, либо все бесконечны.

3.40. Пусть $H \leq G$, $t \in G \setminus H$ и $t^{-1}ht = h^{-1}$ для всех $h \in H$.
1) H абелева и $\langle H, t\rangle = H\langle t\rangle$.
2) Если t – инволюция, то $\langle H, t\rangle \simeq D(H)$.
($D(H)$ – обобщённо диэдральная группа, определённая в 1.46.)

3.41. Пусть $H < G$ и $G \setminus H$ состоит из инволюций. Тогда H абелева и либо G – элементарная абелева 2-группа,
либо $|G : H| = 2$ и $G \simeq D(H)$.

3.42. Пусть $G := D(Z_n)$, где $n \in \mathbf{N}$ и $n \geq 2$.
1) G есть группа порядка $2n$. (Эта группа обозначается через D_{2n}, а всякая изоморфная ей группа называется *диэдральной группой* порядка $2n$.)
2) G имеет циклическую подгруппу $\langle a\rangle$ порядка n и $G \setminus \langle a\rangle$ состоит из инволюций.
3) $D_4 \simeq Z_2 \times Z_2$.
4) При $n > 2$ группа D_{2n} неабелева.
5) $D_8 \neq Q_8$.

3.43. Положим, $D_\infty := D(\mathbf{Z}^+)$. (Всякая группа, изоморфная группе D_∞, называется *бесконечной диэдральной группой*.)
Тогда G имеет бесконечную циклическую подгруппу $\langle a\rangle$ индекса 2 и $G \setminus \langle a\rangle$ состоит из инволюций.

3.44. Для группы G и натурального числа $n \geq 2$ следующие условия равносильны ($a, b, x, y \in G$):
(1) $G = \langle a, b\rangle$, где $o(a) = o(b) = 2$ и $o(ab) = n$;
(2) $G = \langle x, y\rangle$, где $o(x) = 2$, $o(y) = n$, $x \neq y$ и $x^{-1}yx = y^{-1}$;
(3) $G \simeq D_{2n}$.

3.45. Следующие условия группы G равносильны:
(1) $G = \langle a, b\rangle$, где $o(a) = o(b) = 2$ и $o(ab) = \infty$;
(2) $G = \langle x, y\rangle$, где $o(x) = 2$, $o(y) = \infty$ и $x^{-1}yx = y^{-1}$;
(3) $G \simeq D_\infty$.

3.46. Найти центры групп D_{2n} и D_∞.

3.47. Следующие подгруппы группы S_4 является диэдральными:

1) $\left\langle \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix} \right\rangle$;

2) $\left\langle \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}, \begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix} \right\rangle$.

Указать их порядки.

3.48. Следующие условия группы G равносильны:

(1) G порождается двумя инволюциями;

(2) G – диэдральная группа (конечная или бесконечная).

3.49. Если G – группа порядка $2p$, где p – простое число, то G изоморфна Z_{2p} или D_{2p}.

3.50. Существуют ли группы, содержащие точно две инволюции?

3.51. Группа кватернионов Q_8 (2.29) порождается двумя элементами i и j, которые связаны соотношениями:

$$i^4 = 1,\ j^4 = 1,\ i^2 = j^2,\ ij = j^{-1}i.$$

3.52. Пусть $G = \langle x, y\rangle$, где элементы x и y удовлетворяют соотношениям:

$$x^4 = 1,\ y^4 = 1,\ x^2 = y^2,\ xy = y^{-1}x.$$

Тогда справедливо одно из следующих утверждений о строении G:

1) $x = y = 1$ и $G = 1$;

2) $x = 1$, $o(y) = 2$ и $G = \langle y\rangle \simeq Z_2$;

3) $o(x) = 2$, $y = 1$ и $G = \langle x\rangle \simeq Z_2$;

4) $o(x) = o(y) = 2$ и $G \simeq D_4$;

5) $o(x) = o(y) = 4$ и $G \simeq Q_8$.

3.53. Какова группа G, которая порождается любыми двумя своими неединичными элементами?

3.54. Пусть любые два неединичных элемента конечной группы G порождают циклическую подгруппу. Какова G?

3.55. Пусть любые два неединичных элемента конечной группы G порождают циклическую или диэдральную подгруппу. Какова G?

3.56. Если G – конечно порождённая (т. е. порождённая конечным подмножеством) группа, то каждое её порождающее множество содержит конечное подмножество, порождающее G.

3.57. На примере группы $D_\infty \times Z_2$, показать, что

а) произведение двух неединичных периодических элементов группы может быть как периодическим, так и непериодическим элементом;

б) произведение двух непериодических элементов может быть как периодическим, так и непериодическим элементом;

в) произведение неединичного периодического и непериодического элементов (в любом порядке) может быть как периодическим, так и непериодическим элементом.

Имеется ли такая "свобода" быть периодическим или непериодическим элементом для произведения элементов в абелевых группах?

3.58. В одномерном торе (см. 1.17)

а) любое конечное множество периодических элементов порождает конечную подгруппу,

б) каждая конечная подгруппа – циклическая,

в) для каждого натурального числа n существует одна и только одна подгруппа порядка n.

3.59. Пусть $a, b \in \mathbf{C}^+$. Тогда либо $\langle a\rangle \cap \langle b\rangle = \{0\}$, либо $\langle a, b\rangle$ – циклическая группа.

3.60. 1) Любое конечное множество элементов группы $\mathbf{Q}^+$ порождает циклическую подгруппу.

2) Пересечение любых двух неединичных подгрупп группы $\mathbf{Q}^+$ есть также неединичная подгруппа.

3) Группа $\mathbf{Q}^+$ порождается элементами вида $\frac{1}{p^n}$, где p – простое число и $n \in \mathbf{N}$.

4) $\mathbf{Q}^+ = \left\langle \frac{1}{2!}, \frac{1}{3!}, \ldots, \frac{1}{n!}, \ldots \right\rangle$.

3.61. Для любого простого числа p обозначим через $\mathbf{Q}(p)$ множество всех p-ичных дробей, т. е. чисел вида $\frac{m}{p^n}$, где m и n – целые числа.

1) $\mathbf{Z}^+ < \mathbf{Q}(p) < \mathbf{Q}^+$.

2) $\mathbf{Q}(p) = \left\langle \frac{1}{p}, \frac{1}{p^2}, \ldots, \frac{1}{p^n}, \ldots \right\rangle$.

3) Если подгруппа H из $\mathbf{Q}(p)$ содержит несократимые дроби $\frac{a}{p^i}$ и $\frac{b}{p^{i+j}}$, где $a, b, i, j \in \mathbf{N}$, то H содержит также дробь $\frac{d}{p^{i+j}}$, где $d = (a, b)$.

4) Определить все подгруппы группы $\mathbf{Q}(p)$. Показать, что каждая её истинная нециклическая подгруппа имеет вид $k\mathbf{Q}(p)$ $\left(= \left\langle \frac{k}{p}, \frac{k}{p^2}, \ldots, \frac{k}{p^n}, \ldots \right\rangle\right)$, где $k \in \mathbf{N}$ и $(k, p) = 1$, и изоморфна всей группе $\mathbf{Q}(p)$. Каков индекс $|\mathbf{Q}(p) : k\mathbf{Q}(p)|$?

5) Указать максимальные подгруппы группы $\mathbf{Q}(p)$.

6) $\mathbf{Q}(p) \neq \mathbf{Q}(q)$ при $p \neq q$ (q – простое число).

3.62. Пусть a и b – элементы абелевой группы без кручения (т. е. без элементов конечного порядка).

1) Если $a^n = b^n$, где $n \in \mathbf{N}$, то $a = b$.

2) Если $a^n = b^m$, где $\{m, n\} \subseteq \mathbf{N}$, то $\langle a, b\rangle$ – циклическая группа.

3.63. Пусть G – бесконечная абелева группа, каждая собственная подгруппа которой имеет в ней конечный индекс. Тогда G – циклическая группа.

3.64. Пусть группа G имеет элементы a и b конечных порядков m и n такие, что $ab = ba$.

1) Если $(m, n) = 1$, то $o(ab) = mn$ и $\langle a, b\rangle = \langle ab\rangle$.

2) Если $(m, n) = d > 1$, то $o(ab)$ делит $\frac{mn}{d}$ и делится на $\frac{mn}{d^2}$.

3) Показать на примерах, что в случае 2) $o(ab)$ может быть равен $\frac{mn}{d^2}$, может быть равен $\frac{mn}{d}$ и может отличаться и от $\frac{mn}{d^2}$, и от $\frac{mn}{d}$.

4) Если $\langle a\rangle \cap \langle b\rangle = 1$, то $o(ab) = \frac{mn}{d}$.

5) В группе $\langle a, b\rangle$ всегда есть элемент порядка $\frac{mn}{d}$.

6) Если $m = p^{\alpha}$ и $n = p^{\beta}$, где p – простое число и $\alpha < \beta$, то $o(ab) = p^{\beta}$.

3.65. Пусть a – элемент, а H – подгруппа некоторой группы. *Порядок элемента a относительно подгруппы H*, обозначаемый символом $o(a; H)$, определяется следующим образом: если среди степеней a^n $(n \geq 1)$ элемента a есть содержащиеся в H и a^r – наименьшая среди них, то $o(a; H) = r$; если же ни одна степень a^n $(n \geq 1)$ не содержится в H, то $o(a; H) = \infty$.

Доказать следующие утверждения:

1) если $o(a; H) = r \in \mathbf{N}$, то

а) $\langle a^r\rangle = \langle a\rangle \cap H$,

б) $r = |\langle a\rangle : \langle a\rangle \cap H|$,

в) $o(a^n; H) = \frac{r}{(r, n)}$ для всех $n \in \mathbf{Z}$;

2) если $o(a)$ конечен, то $o(a; H) \mid o(a)$;

3) $o(a; H) = \infty$ тогда и только тогда, когда $o(a) = \infty$ и $\langle a\rangle \cap H = 1$;

4) из $H \leq K \leq G$ следует, что $o(a; K) \mid o(a; H)$ (если $o(a; H)$ конечен);

5) если $a^m \in H$ $(m \in \mathbf{N})$, то m делится на $o(a; H)$.

3.66. Если $a, b \in G$, $o(a) = \alpha$, $o(b) = \beta$, $o(a;\langle b\rangle) = \alpha_1$, $o(b; \langle a\rangle) = \beta_1$, то

1) $\frac{\alpha}{\alpha_1} = \frac{\beta}{\beta_1}$;

2) если $b^{\beta_1} = a^r$, то $\alpha_1 = (\alpha, r)$;

3) если $b^{\beta_1} = a^r$ и $ab = ba$, то

$$o(ab) = \frac{\alpha\beta_1}{(\alpha, \beta_1 + r)}.$$

3.67. Пусть $a, b \in G$. Определить $o(b)$, $o(ab)$ и $|\langle a, b\rangle|$, если
1) $o(a) = 12$, $b^7 = a^9$, $ab = ba$;
2) $o(a) = 20$, $b^4 = a^6$, $ab = ba$.

3.68. Пусть $m, n \in \mathbf{N}$.
1) Определить порядки всех элементов группы $Z_m \times Z_n$.
2) $Z_m \times Z_n \simeq Z_{mn}$ если и только если $(m, n) = 1$.

§ 4. Нормальные подгруппы и гомоморфизмы

Если H – подгруппа группы G и $Hg = gH$ для всех $g \in G$, то говорят, что H – *нормальная подгруппа* группы G и пишут $H \trianglelefteq G$. Другими словами, H нормальна в G, если она совпадает с любой сопряжённой с ней подгруппой $g^{-1}Hg$. Запись $H \triangleleft G$ означает, что $H \trianglelefteq G$ и $H \neq G$. Группа называется *простой*, если она не единична и не имеет собственных нормальных подгрупп. *Минимальной нормальной подгруппой* группы G называется неединичная нормальная подгруппа из G, не содержащая других неединичных нормальных подгрупп группы G.

Если A и B – подгруппы группы G такие, что 1) $G = AB$, 2) $A \cap B = 1$, 3) $A \trianglelefteq G$ и 4) $B \trianglelefteq G$, то пишут

$G = A \times B$ и говорят, что группа G есть *(внутреннее) прямое произведение подгрупп* A и B. Хотя знак $\times$ употребляют также и при обозначении внешнего прямого произведения (см. 1.32), из контекста обычно бывает ясно, какое прямое произведение подразумевается. Если для подгрупп A и B выполнены условия 1)–3), то пишут

$G = A \lambda B$ и говорят, что группа G есть *полупрямое произведение* A и B с нормальным множителем A. Для подмножества M группы G подмножество

$N_G(M) := \{g \in G \mid Mg = gM\}$ есть подгруппа в G, называемая *нормализатором* M в G, причём для любой подгруппы H из G $N_G(H)$ есть наибольшая среди подгрупп N группы G таких, что $H \trianglelefteq N$ (4.10).

Важнейшим свойством нормальной подгруппы H группы G является то, что множество всех смежных классов gH ($g \in G$) относительно операции умножения подмножеств является группой (4.19). Эта группа обозначается через G/H и называется *фактор-группой* группы G по H. Понятие фактор-группы тесно связано (см. 4.33) с понятием гомоморфизма.

Отображение φ группы G в группу H называется *гомоморфизмом*, если

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ для всех } a, b \in G$$

(и в G, и в H групповая операция обозначена точкой). Наряду с обозначением $\varphi(g)$ для образа элемента g часто используется обозначение g^{φ}. С гомоморфизмом φ группы G в группу H связаны:

$\varphi(G) := \{\varphi(g) \mid g \in G\}$ – *образ гомоморфизма* φ (подгруппа в H),

$Ker(\varphi) := \{g \in G \mid \varphi(g) = 1\}$ – *ядро* φ (нормальная подгруппа в G). Вместо $\varphi(G)$ пишут также G^{φ}.

Говорят, что H есть *собственный гомоморфный образ* группы G, если существует гомоморфизм φ G на H такой, что $1 < Ker(\varphi) < G$. Гомоморфизм φ группы G в группу H называется *эпиморфизмом*, если $\varphi(G) = H$, *мономорфизмом*, если φ – изоморфизм, и *тривиальным гомоморфизмом*, если $\varphi(G) = 1$. Фактор-группа подгруппы группы G называется её *секцией*.

Наличие в группе собственных нормальных подгрупп часто позволяет применить индукцию при доказательстве утверждений о конечной группе.

Если H – абелева группа с операцией +, то множество M всех гомоморфизмов из G в H с операцией

$$(\alpha + \beta)(g) = \alpha(g) + \beta(g) \quad (\alpha, \beta \in M, g \in G)$$

является группой (4.62), которая обозначается через $Hom(G, H)$.

Далее будет использоваться знак $\simeq \leq$ (единственное произведение бинарных отношений, встречающееся в этой книге), а именно, запись $A \simeq \leq B$ означает, что A изоморфна подгруппе группы B.

4.1. Если $N \trianglelefteq G$, то для любой подгруппы A из G

$$\langle A, N\rangle = AN = NA \text{ и } N \cap A \trianglelefteq A.$$

4.2. Если G – конечная группа, $N \trianglelefteq G$, $g \in G$ и $(o(g), |G : N|) = 1$, то $g \in N$.

4.3. Подгруппа индекса 2 любой группы нормальна в ней.

4.4. Пусть $H \leq G$ и S – некоторая правая система вычетов G по H (т.е. $G = H \circ S$). Равносильны условия:

(1) $H \trianglelefteq G$,

(2) $g^{-1}hg \in H$ для любых $g \in G$ и $h \in H$,

(3) $s^{-1}hs \in H$ для любых $s \in S$ и $h \in H$.

4.5. Если $A_1 \trianglelefteq A \leq G$ и $B_1 \trianglelefteq B \leq G$, то $A_1 \cap B_1 \trianglelefteq A \cap B$.

4.6. Пусть $N := \langle a, b\rangle$, где $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ – элементы группы S_4.

1) $N = \langle a\rangle \times \langle b\rangle \simeq E_4$.

2) S_4 имеет подгруппу S, изоморфную S_3, такую что $S_4 = NS$.

3) $N \trianglelefteq S_4$ и, следовательно, $S_4 = N\lambda S$.

4) S_4 имеет точно одну (нормальную) подгруппу индекса 2 (это – знакопеременная группа A_4 в терминах §7).

4.7. Пусть $N \trianglelefteq G$ и N содержит произведение ab некоторых элементов a и b из G. Тогда N содержит элементы $a^m b^m$ и $b^m a^m$ при любом целом m.

4.8. Для группы G и её подгруппы H следующие условия равносильны:

1) $H \trianglelefteq G$;

2) всякий раз, когда H содержит произведение ab каких-либо элементов a и b группы G, H содержит также произведение $a^2 b^2$ квадратов этих элементов.

4.9. Пусть G – конечная группа и $G = AB$, где A и B – подгруппы взаимно простых порядков. Тогда для любой нормальной подгруппы N из G справедливо равенство $N = (A \cap N)(B \cap N)$.

4.10. Пусть M – подмножество группы G.

1) $N_G(M) := \{g \in G \mid Mg = gM\}$) есть подгруппа группы G (нормализатор M в G).

2) Если $H \leq G$, то $N_G(H)$ есть единственный максимальный элемент во множестве всех подгрупп N группы G таких, что $H \trianglelefteq N$.

3) $C_G(M) \trianglelefteq N_G(M)$. В частности, если $H \trianglelefteq G$, то $C_G(H) \trianglelefteq G$.

4.11. Пусть M – максимальная подгруппа группы G. Тогда для любой подгруппы A из G либо $Z(A) \subseteq M$, либо $Z(M) \cap A \lhd G$.

4.12. Если $A < B \leq G$, то $N_G(B \setminus A) = N_G(A) \cap N_G(B)$.

4.13. Привести пример группы G и её подмножества M таких, что $N_G(M) = 1$.

4.14. Если $G = A \times B$ – прямое произведение подгрупп A и B, то каждый элемент из A перестановочен с каждым элементом из B.

4.15. 1) Если $G = A \times B$ – прямое произведение подгрупп A и B, то G изоморфна внешнему прямому произведению групп A и B.

2) Если $H = A \times B$ – внешнее прямое произведение групп A и B, то H – прямое произведение своих подгрупп $\tilde{A}$ и $\tilde{B}$ таких, что $\tilde{A} \simeq A$ и $\tilde{B} \simeq B$.

4.16. Пусть a и b – перестановочные элементы конечных взаимно простых порядков группы G. Тогда

1) $\langle ab \rangle = \langle a \rangle \times \langle b \rangle$,

2) $C_G(ab) = C_G(a) \cap C_G(b)$,

3) $N_G(\langle ab \rangle) = N_G(\langle a \rangle) \bigcap N_G(\langle b \rangle)$.

4.17. Пусть $G = \langle a \rangle \times \langle b \rangle$, где $o(a) = o(b) = n \in \mathbf{N}$, и $H = \langle ab, a^{-1}b \rangle$. Тогда $H = G$, если n нечётно, и $|G : H| = 2$, если n чётно.

4.18. Для подгруппы H группы G равносильны условия:

(1) множество всех левых смежных классов по H совпадает с множеством всех правых смежных классов по H;

(2) каждая левая система вычетов G по H является правой системой вычетов G по H;

(3) $H \trianglelefteq G$.

4.19. (Т) Пусть $H \leq G$ и $\mathcal{H}$ – множество всех левых смежных классов G по H. Равносильны условия:

(1) $\mathcal{H}$ является группой относительно операции умножения подмножеств,

(2) $H \trianglelefteq G$.

4.20. Утверждение 4.19 останется вериым, если в нём слово "левых" заменить словóм "правых".

4.21. Пусть E – единичная подгруппа группы G. Верно ли, что $G/E = G$?

4.22. Пусть $\mathcal{H}$ – некоторое множество непустых подмножеств группы G, являющееся группой относительно операции умножения подмножеств группы G.

1) Если $\mathcal{H}$ содержит конечное подмножество из G или же группа G периодическая, то $\mathcal{H}$ является фактор-группой некоторой подгруппы из G.

2) Заключение пункта 1), вообще говоря, неверно, если все подмножества группы G, содержащиеся в $\mathcal{H}$, бесконечны, и группа G не периодическая (рассмотреть группу $\mathbf{Z}^+$).

4.23. Пусть H – подгруппа группы $\mathbf{R}^+$. Для любого $h \in H$ определим подмножество $K_h = \{x \in \mathbf{R}^+ \mid x > h\}$. Тогда множество $\{K_h \mid h \in H\}$ с операцией сложения подмножеств есть группа, изоморфная H. При этом ни одно из подмножеств K_h ($h \in H$) не является подгруппой в $\mathbf{R}^+$.

4.24. Пусть H и K – подгруппы группы G.

1) Если множество $\mathfrak{D}$ всех двойных смежных классов HgK группы G по (H, K) является группой относительно операции умножения подмножеств, то $HK \trianglelefteq G$ и $\mathfrak{D} = G/HK$ (в частности, $HgK = gHK$ для всех $g \in G$).

2) Из $HK \trianglelefteq G$ не следует, что $HgK = gHK$ для всех $g \in G$. (Рассмотреть подгруппу A_4 из S_4, см. 4.6.)

4.25. (Т) Пусть $N \trianglelefteq G$ и $A \leq G$. Тогда $AN \leq G$, $A \cap N \trianglelefteq A$ и

$$AN/N \simeq A/A \cap N.$$

Более того, если $S \subseteq A$, то: $AN = S \circ N \Leftrightarrow A = S \circ (A \cap N)$.

4.26. Пусть G_1 и G_2 – группы и $N_i \trianglelefteq G_i$ при $i \in \{1, 2\}$. Тогда $N_1 \times N_2 \trianglelefteq G_1 \times G_2$ и

$$(G_1 \times G_2)/(N_1 \times N_2) \simeq (G/N_1) \times (G/N_2).$$

4.27. Пусть N и K – нормальные подгруппы группы G. Тогда

$$N \cap K \trianglelefteq G \text{ и } G/N \cap K \simeq\leq (G/N) \times (G/K).$$

4.28. Пусть N *и* K – нормальные подгруппы группы G такие, что $N \cap K = 1$.

1) Если G/N и G/K абелевы, то и G абелева.

2) Если G/N и G/K – π-группы, где π – множество простых чисел, то и G – π-группа.

4.29. Пусть $\cdot$ и $*$ – бинарные операции на множествах X и Y соответственно и φ – отображение X на Y такое, что

$$\varphi(x_1x_2) = \varphi(x_1)*\varphi(x_2) \text{ для всех } x_1, x_2 \in G.$$

Если $(X, \cdot)$ – группа, то $(Y, *)$ – группа.

Верно ли обратное утверждение?

4.30. Отображение φ группы G в группу H есть гомоморфизм если и только если $\{(g, \varphi(g)) \mid g \in G\}$ есть подгруппа в группе $G \times H$.

4.31. Пусть φ – гомоморфизм группы G в абелеву группу H. Тогда отображение

$$\theta: = (G \times G \to H \mid (g_1,g_2) \mapsto \varphi(g_1)\varphi(g_2)^{-1})$$

есть гомоморфизм.

4.32. Пусть φ – гомоморфизм группы G, а A и B – её подмножества. Тогда

1) $(A \cup B)^\varphi = A^\varphi \cup B^\varphi$,

2) $(AB)^\varphi = A^\varphi B^\varphi$,

3) $\langle A, B\rangle^\varphi = \langle A^\varphi, B^\varphi\rangle$.

4.33. (Теорема о гомоморфизмах)

1) Пусть $N \trianglelefteq G$. Тогда отображение α с $g^\alpha = gN$ $(g \in G)$ является гомоморфизмом G на G/N. (α называется *естественным гомоморфизмом* из G на G/N.)

2) Пусть φ – гомоморфизм группы G в группу H. Тогда

$$Ker(\varphi) \trianglelefteq G \text{ и } G/Ker(\varphi) \simeq G^{\varphi}.$$

Более того, $\varphi = \alpha\mu$, где α – естественный гомоморфизм G на $G/Ker(\varphi)$, а μ – некоторый изоморфизм $G/Ker(\varphi)$ на G^{φ}.

4.34. (Т) Пусть $N \trianglelefteq G$, $\mathfrak{L} = \{H \mid N \le H \le G\}$ и $A, B \in \mathfrak{L}$.

1) Отображение $\pi : A \mapsto A/N$ $(A \in \mathfrak{L})$ есть взаимно однозначаное отображение $\mathfrak{L}$ на множество всех подгрупп из G/N.

2) $A^{\pi} \cap B^{\pi} = (A \cap B)^{\pi}$.

3) $\langle A^{\pi}, B^{\pi}\rangle = \langle A, B\rangle^{\pi}$.

4) $|G^{\pi} : A^{\pi}| = |G : A|$.

5) $A \trianglelefteq G \Leftrightarrow A^{\pi} \trianglelefteq G^{\pi}$, и при $A \trianglelefteq G$ $G^{\pi}/A^{\pi} \simeq G/A$.

4.35. Пусть φ – гомоморфизм группы G с ядром N, а A и B – её подмножества.

1) $(A \cap B)^{\varphi} \le A^{\varphi} \cap B^{\varphi} = (AN \cap BN)^{\varphi}$.

2) $N_G(A)^{\varphi} \le N_{G^{\varphi}}(A^{\varphi}) = N_G(AN)^{\varphi}$.

3) $C_G(A)^{\varphi} \le C_{G^{\varphi}}(A^{\varphi}) = \bigcap\limits_{a \in A} N_G(aN)^{\varphi}$.

Привести примеры строгих включений в пунктах 1)–3).

4.36. Пусть φ – гомоморфизм группы G и $g \in G$. Если $o(g) < \infty$, то $o(g^{\varphi})$ делит $o(g)$.

4.37. Усилить утверждение 4.2 следующим образом. Пусть g периодический элемент и N – нормальная подгруппа конечного индекса группы G. Если $(o(g), |G : N|) = 1$, то $g \in N$.

4.38. Пусть φ – гомоморфизм группы G и $A \le B \le G$.

1) $A^{\varphi} \le B^{\varphi}$, и $|B^{\varphi} : A^{\varphi}|$ делит $|B : A|$.

2) Если $A \trianglelefteq B$, то $B^{\varphi}/A^{\varphi} \simeq BKer(\varphi)/AKer(\varphi) \simeq\le B/A$.

4.39. Пусть $G = \langle a\rangle \lambda \langle b\rangle \simeq D_{2n}$, т. е. $o(a) = n$, $o(b) = 2$ и $bab = a^{-1}$.

1) Определить все нормальные подгруппы в G, доказав, что

а) все подгруппы из $\langle a\rangle$ нормальны в G;

б) если G имеет собственные нормальные подгруппы, не содержащиеся в $\langle a\rangle$, то n чётно, таких подгрупп – точно две, и обе они содержат $\langle a^2\rangle$.

2) Определить все (с точностью до изоморфизма) гомоморфные образы группы D_{2n}.

4.40. Определить все нормальные подгруппы и все (с точностью до изоморфизма) гомоморфные образы группы D_{∞}.

4.41. В группах Q_8 и $Z_2 \times Q_8$ каждая подгруппа нормальна. Определить все их гомоморфные образы.

4.42. Группа $Z_4 \times Q_8$ имеет ненормальную подгруппу.

4.43. 1) Указать две неизоморфные группы G с $G/Z(G) \simeq D_8$.
2) Не существует группы G с $G/Z(G) \simeq Q_8$.

4.44. Группа Z_{p^∞} изоморфна любой своей собственной факторгруппе.

4.45. Указать неединичную группу G такую, что $G/Z(G) \simeq G$.

4.46. Пусть $N_1 \trianglelefteq G_1$ и $N_2 \trianglelefteq G_2$.
1) Если $N_1 \simeq N_2$ и $G_1/N_1 \simeq G_2/N_2$, то будет ли $G_1 \simeq G_2$?
2) Если $G_1 \simeq G_2$ и $N_1 \simeq N_2$, то будет ли $G_1/N_1 \simeq G_2/N_2$?
3) Если $G_1 \simeq G_2$ и $G_1/N_1 \simeq G_2/N_2$, то будет ли $N_1 \simeq N_2$?

4.47. Группа G является объединением (теоретико-множественным) трёх своих истинных подгрупп A, B, C тогда и только тогда, когда она имеет нормальную подгруппу N такую, что фактор-группа G/N является четверной группой (т. е. изоморфна E_4). Более того, если две из этих трёх подгрупп абелевы, то и третья подгруппа абелева. Привести пример такой группы G в случае, когда $A \cap B \cap C \neq 1$.

4.48. Пусть группа G такова, что в каждом её четырёхэлементном подмножестве имеются два подмножества, состоящие из двух перестановочных элементов. Тогда G абелева.

4.49. Следующие условия группы G равносильны:
(1) среди любых четырёх элементов группы G имеются два перестановочных;
(2) либо G – абелева группа, либо $G/Z(G) \simeq E_4$.

4.50. Пусть в группе G централизатор любого элемента либо равен G, либо является её максимальной подгруппой. Тогда группа $G/Z(G)$ есть объединение некоторого множества попарно взаимно простых абелевых подгрупп (в таком случае говорят, что группа $G/Z(G)$ обладает абелевым расщеплением).

4.51. Пусть M – максимальная подгруппа группы G и $M \trianglelefteq G$. Тогда $|G : M|$ – простое число.

4.52. Пусть M – максимальная подгруппа группы G, не содержащая неединичных нормальных подгрупп из G.

1) Если $1 < N \trianglelefteq G$, то $C_G(N)$ есть либо единичная, либо минимальная нормальная подгруппа в G.

2) Существует не более одной неединичной абелевой нормальной подгруппы в G.

3) Существует не более двух различных минимальных нормальных подгрупп в G.

4) Если A и B – различные минимальные нормальные подгруппы G, то

а) $G = A \lambda M = B \lambda M$,

б) $A = C_G(B)$ и $B = C_G(A)$,

в) A, B и $AB \cap M$ – изоморфные неабелевы группы.

4.53. Пусть H/K и L/M – две секции группы G. Говорят, что H/K *покрывает* L/M, если $(H \cap L)M = L$ и $K \cap L \subseteq M$. Равносильны условия:

(1) H/K покрывает L/M;

(2) существует система представителей смежных классов L по M, содержащаяся в H, и всякая система представителей смежных классов L по M, содержащаяся в H, содержится в некоторой системе представителей смежных классов H по K.

4.54. Пусть H/K покрывает L/M. Тогда отображение $xK \mapsto xM$ $(x \in H \cap L)$ является гомоморфизмом группы $(H \cap L)K/K$ на L/M с ядром $(H \cap M)K/K$ ("естественный гомоморфизм покрытия").

4.55. Отображение $x \mapsto det(x)$ является гомоморфизмом группы $GL_n(C)$ на группу $\mathbf{C}^*$. Каково ядро этого гомоморфизма?

4.56. 1) $\mathbf{C}^+/\mathbf{R}^+ \simeq \mathbf{R}^+$.

2) $\mathbf{Q}(p)/\mathbf{Z}^+ \simeq Z_{p^\infty}$.

3) $\mathbf{Q}^+ / N_p \simeq \mathbf{Z}_{p^\infty}$, где N_p – подгруппа группы $\mathbf{Q}^+$, состоящая из всех чисел, знаменатели которых взаимно просты с p.

4.57. Пусть U обозначает мультипликативную группу всех комплексных чисел с модулем, равным 1 (одномерный тор).

1) $\mathbf{R}^+/\mathbf{Z}^+ \simeq U$.

2) $U/Z_n \simeq U$.

3) $\mathbf{C}^* / Z_n \simeq \mathbf{C}^*$.

4) $\mathbf{C}^* / \mathbf{R}^* \simeq U$.

4.58. Пусть $n \in \mathbf{N}$ и H_n – подмножество из $\mathbf{C}^*$, состоящее из всех чисел, лежащих на n лучах, исходящих от нуля под равными углами,

причём один из этих лучей совпадает с положительной действительной полуосью. Тогда $H_n < \mathbf{C}^{\cdot}$ и $\mathbf{C}^{\cdot}/H_n \simeq U$.

4.59. Отображение группы $\mathbf{Q}^{\cdot}$, сопоставляющее числу $2^l\frac{m}{n}$, где $\{l, m, n\} \subseteq \mathbf{Z}$ и m, n нечётны, есть гомоморфизм группы $\mathbf{Q}^{\cdot}$ на группу $\mathbf{Z}^{+}$.

4.60. Указать все пары (m, n) целых чисел, при которых отображение

$$x \mapsto mx^n \ (x \in \mathbf{Q}^{\cdot})$$

является гомоморфизмом группы $\mathbf{Q}^{\cdot}$.

4.61. Для каждой из групп $\mathbf{Q}^{+}$, $\mathbf{Z}^{+}$, $\mathbf{R}^{\cdot}$ и $\mathbf{Q}^{\cdot}$ проверить, может ли она быть гомоморфно отображена на конечную неединичную группу.

4.62. Пусть G и H – группы. Если группа H абелева с операцией $+$, то множество M всех гомоморфизмов из G в H является абелевой группой относительно операции $+$:

$$(\alpha + \beta)(g) = \alpha(g) + \beta(g) \ \ (\alpha, \beta \in M, g \in G)$$

(группа $Hom(G,H)$).

4.63. Пусть $A = \langle a \rangle$ и $B = \langle b \rangle$ – циклические группы. Тогда $Hom(A. B) = \langle c \rangle$, где

$$o(c) = \begin{cases} o(b), & \text{если } o(a) = \infty, \\ 1, & \text{если } o(a) < \infty, \ o(b) = \infty, \\ (o(a), o(b)), & \text{если } o(a) < \infty, o(b) < \infty. \end{cases}$$

4.64. Найти группы $Hom(G, H)$ в случаях, когда $(G. H)$ есть одна из пар

а) $(\mathbf{Z}^{+}, \mathbf{Q}^{+})$,

б) $(Z_n, \mathbf{Q}^{+})$,

в) $(\mathbf{Q}^{+}, Z_n)$ $(n \in \mathbf{N})$.

4.65. 1) Если φ – гомоморфизм $\mathbf{Q}^{+}$ в $\mathbf{C}^{+}$, то $\varphi(q) = q\varphi(1)$ для всех $q \in \in \mathbf{Q}^{+}$.

2) Найти $Hom(\mathbf{Q}^{+}, \mathbf{Z}^{+})$ и $Hom(\mathbf{Q}^{+}, \mathbf{Q}^{+})$.

§ 5. Сопряжённость

Элементы a и b группы G называются *сопряжёнными в* G, если имеется элемент g в G такой, что $g^{-1}ag = b$. Элемент $g^{-1}ag$ обозначается также через a^g. Множество

$$a^G := \{a^g \mid g \in G\}$$

называется *классом сопряжённых элементов* группы G (содержащим элемент a). Любой элемент группы содержится, очевидно, точно в одном её классе сопряжённых элементов. В частности, для конечной группы G справедливо так называемое *классовое равенство*:

$$|G| = |C_1| + \ldots + |C_k|,$$

где $C_1, \ldots, C_k$ – все классы сопряжённых элементов группы G. С его помощью может быть доказана очень важная

первая теорема Силова: в любой конечной группе G для любого простого числа p существует силовская p-подгруппа (т. е. подгруппа, порядок которой есть наивысшая степень p, делящая $|G|$). Путь доказательства этой теоремы предложен в задаче 5.17.

Объединение любого множества классов сопряжённых элементов группы G называется *нормальным подмножеством* в G. Очевидно, нормальность подмножества X в G равносильна каждому из условий: а) $Xg = gX$ для всех $g \in G$ и б) $N_G(X) = G$. Следовательно, если $H \leq G$ и H – нормальное подмножество в G, то $H \trianglelefteq G$.

Если $H \leq G$, то (нормальная) подгруппа

$H_G := \bigcap\limits_{g \in G} H^g$ называется *сердцевиной* подгруппы H в G.

Для подмножества X и Y и элемента a группы G определяют:

$X^a := \{x^a \mid x \in X\}$ – множество, *сопряжённое* с X в G;

$\{X\}^G := \{X^g \mid g \in G\}$ – *класс сопряжённых подмножеств* группы G (содержащий X);

$X^Y := \{x^y \mid x \in X, y \in Y\}$.

5.1. Для любого $g \in G$ отображение $x \mapsto x^g$ $(x \in G)$ есть изоморфизм G на G.

5.2. Пусть A и B – подмножества группы G и $g \in G$.

1) $(A \cup B)^g = A^g \cup B^g$.

2) $(A \cap B)^g = A^g \cap B^g$.

3) $(A \setminus B)^g = A^g \setminus B^g$.

4) $(AB)^g = A^g B^g$.

5) $(A^{-1})^g = (A^g)^{-1}$.

6) $\langle A \rangle^g = \langle A^g \rangle$.

7) $N_B(A)^g = N_{B^g}(A^g)$.

8) $C_B(A)^g = C_{B^g}(A^g)$.

9) Если $A \leq B \leq G$, то $|B^g : A^g| = |B : A|$.

5.3. Если A и B – нормальные подмножества группы G, то таковы же и $A \cup B$, $A \cap B$, $A \setminus B$, AB, A^{-1}, $\langle A \rangle$, $N_B(A)$, $C_B(A)$.

5.4. Объединение всех конечных классов сопряжённых элементов группы является её (нормальной) подгруппой.

5.5. (Т) Пусть G – группа, $a \in G$ и $X \subseteq G$. Тогда

1) $|a^G| = |G : C_G(a)|$,

2) $|\{X\}^G| = |G : N_G(X)|$.

5.6. Определить все классы сопряжённых элементов каждой из групп D_6, D_8, Q_8.

5.7. Пусть a_1, b_1, a_1, b_2 – элементы группы G такие, что a_1 сопряжён с b_1 и a_2 сопряжён с b_2. Будет ли $a_1 a_2$ сопряжён с $b_1 b_2$?

5.8. Каковы конечные группы, имеющие точно два класса сопряжённых элементов? (См. также 5.46.)

5.9. Пусть G – конечная группа, в которой объединение любого множества классов сопряжённых элементов, содержащее 1, является (нормальной) подгруппой. Какова G?

5.10. Пусть G – конечная группа и d – наибольший общий делитель порядков классов сопряженных элементов группы G, состоящих более чем из одного элемента. Тогда d делит $|Z(G)|$.

5.11. Если G – конечная неабелева группа, то по крайней мере два её класса сопряжённых элементов содержатся в $G \setminus Z(G)$.

5.12. Пусть G – группа порядка p^n, где p – простое число и $n \in \mathbf{N}$.

1) $Z(G) > 1$.

2) Если M – максимальная подгруппа группы G, то $M \trianglelefteq G$ и $|M| = p^{n-1}$.

3) Если $H < G$, то $H < N_G(H)$.

5.13. Группа порядка p^2, где p – любое простое число, есть либо циклическая группа, либо прямое произведение двух циклических подгрупп порядка p.

5.14. Пусть G – неабелева группа порядка p^3, где p – простое число. Найти

1) $|Z(G)|$,

2) число классов сопряжённых элементов в G.

5.15. Предположим, что известны порядок конечной группы G и число r решений (x, y) уравнения $xy = yx$ в группе G. Можно ли найти число классов сопряжённых элементов группы G?

5.16. Если $N \trianglelefteq G$ и $|N| < \infty$, то $|G : C_G(N)| < \infty$.

5.17. Доказать первую теорему Силова, проделав следующее. Пусть G – группа наименьшего порядка без силовских p-подгрупп. Показать, что

1) если $H < G$, то p делит $|G : H|$;

2) G не имеет неединичных нормальных p-подгрупп;

3) p делит $|Z(G)|$;

4) пункты 2) и 3) противоречат друг другу ввиду 3.8.

5.18. Пусть G – конечная группа и p – простое число. Если некоторая силовская p-подгруппа P группы G нормальная в G, то P совпадает с множеством всех p-элементов из G, и, в частности, P есть единственная силовская p-подгруппа в G.

5.19. Пусть G – конечная группа, имеющая точно 3 класса сопряжённых элементов. Тогда либо $G \simeq Z_3$, либо $G \simeq S_3$.

5.20. Пусть G – конечная группа такая, что для любых двух её подгрупп A и B из "$|A|$ делит $|B|$" следует "$A \leq B$". Какова G?

5.21. Пусть G – конечная группа порядка n. Равносильны условия:

1) для любого делителя m числа n уравнение $x^m = 1$ имеет не более m решений в группе G;

2) для любого делителя m числа n группа G имеет точно одну подгруппу порядка m;

3) G циклическая.

5.22. Если $H \le G$, то $H_G \left(= \bigcap_{g \in G} H^g\right) \trianglelefteq G$. Если $|G : H| < \infty$, то $|G : H_G| < \infty$.

5.23. Если A и B – подгруппы в G, то $A_G \cap B_G = (A \cap B)_G$.

5.24. Пусть H – π-подгруппа конечного индекса группы G. Тогда G является π-группой если и только если $|G : H|$ – π-число (т. е. натуральное число, все простые делители которого лежат в π).

5.25. Утверждение 2.54 останется верным, если в нём слово "порядков" заменить словом "индексов". А именно, если H и K – подгруппы конечных и равных между собой индексов в группе G, то G имеет подмножество S такое, что $G = H \circ S = S \circ K$.

5.26. Конечная группа не может быть теоретико-множественным объединением своих истинных подгрупп, сопряжённых между собой в этой группе.

5.27. Конечная группа, в которой все максимальные подгруппы сопряжены между собой, является циклической группой порядка p^α, где p – простое число и $\alpha \in \mathbf{N} \cup \{0\}$.

5.28. Если G – конечная группа и $G = a_1^G \cup a_2^G \cup \ldots \cup a_n^G$, то $G = \langle a_1, a_2, \ldots, a_n \rangle$ ($a_1, \ldots, a_n$ – элементы группы G).

5.29. Пусть G – конечная группа, порядок любой собственной подгруппы которой есть простое число. Какова G? (Дать необходимое и достаточное условие.)

5.30. Описать конечные группы, имеющие не более четырёх классов сопряжённых подгрупп.

5.31. Пусть конечная группа G имеет точно три максимальные подгруппы, причём их пересечение равно 1. Какова G?

5.32. Пусть G – конечная группа и $H < G$.

1) Если $G \setminus H$ есть класс сопряжённых элементов в G, то H – абелева группа нечётного порядка и $G \simeq D(H)$.

2) Пусть $G \setminus H$ содержится в некотором классе сопряжённых элементов группы G. Какова G?

5.33. Пусть $H \le G$ и $|G : H| = n < \infty$.

1) Для любого $g \in G$ $g^G \cap H$ есть объединение не более чем n классов сопряжённых элементов подгруппы H.

2) Если группа G имеет конечное число k классов сопряжённых элементов, то подгруппа H также имеет конечное число классов сопряжённых элементов и это число не превосходит $k\,|\,G:H\,|$.

5.34. Пусть A – подгруппа индекса 2 группы G (нормальная в G по 4.3). Тогда для любого $a \in A$ либо $a^G = a^A$, либо $a^G = a^A \cup b^A$, где $b \in A$, $a^A \neq b^A$ и $|\,a^A\,| = |\,b^A\,|$.

5.35. Пусть φ – гомоморфизм группы G, $g \in G$, а A и B – подгруппы G.

1) $(g^G)^\varphi = (g^\varphi)^{G^\varphi}$.

2) Если A и B сопряжены в G, то A^φ и B^φ сопряжены в G^φ.

3) В случае, когда A и B содержат ядро φ, верно утверждение, обратное к 2).

5.36. Пусть G – конечная группа и $H \subseteq G$.

1) При любом гомоморфизме φ группы G.

$$|\,\{H^\varphi\}^{G^\varphi}\,| \text{ делит } |\,\{H\}^G\,|.$$

2) Если $H \leq G$ и $H \trianglelefteq G$, то

$$|\,\{H \cap N\,|^N|\ \text{ делит } |\,\{H\}^G\,|.$$

5.37. Пусть G – конечная группа $N \trianglelefteq G$, $g \in G$, $\overline{G} = G/N$ и $\overline{g} = gN$.

1) $|\,\overline{g}^{\overline{G}}\,| = |\,g^G\,| / |\,g^G \cap gN\,|$.

2) $C_{\overline{G}}(\overline{g}) = \dfrac{|\,C_G(g)\,|\,g^G \cap gN\,|}{|\,N\,|}$.

3) $\dfrac{|\,C_G(g)\,|}{|\,C_N(g)\,|} \leq |\,C_{\overline{G}}(\overline{g})\,| \leq |\,C_G(g)\,|$.

5.38. Пусть G – конечная группа, φ – её гомоморфизм с ядром N и $g \in G$.

1) Если $g \in N \setminus \{1\}$, то $|\,C_{G^\varphi}(g^\varphi)\,| < |\,C_G(g)\,|$.

2) Если $C_N(g) = 1$, то $C_{G^\varphi}(g^\varphi) = C_G(g)^\varphi \simeq C_G(g)$.

5.39. Пусть $H \trianglelefteq G$ и φ – естественный гомоморфизм G на $G/C_G(H)$.

1) Если $Z(H) = 1$, то $C_{G^\varphi}(H^\varphi) = 1$ и $H^\varphi \simeq H$.

2) Если группа G конечна, то из $H^\varphi \simeq H$ следует, что $Z(H) = 1$.

5.40. Пусть A, B – подмножества группы G и $A \subseteq B$.

1) $A^G \subseteq B^G$ и $B^G \setminus A^G \subseteq (B \setminus A)^G$.

Привести пример строгого включения в последнем соотношении.

2) Равносильны условия:

(а) $(B \setminus A)^G = B^G \setminus A^G$;

(б) $A^G \cap B \subseteq A$ (в этом случае говорят, что A *сильно замкнуто в* B *относительно* G).

5.41. Пусть A и B – подгруппы группы G, ни одна из которых не содержится в другой, и пусть $g \in N_G(A \cup B)$. Тогда

либо $g \in N_G(A) \cap N_G(B)$,

либо $A^g = B$ и $B^g = A$.

Каков индекс $|N_G(A \cup B) : N_G(A) \cap N_G(B)|$?

5.42. Пусть $G = \langle a, b \rangle$ $(a, b \in G)$.

1) Если $\langle a \rangle \trianglelefteq G$, то $b^{-1}ab = a^s$ для некоторого целого числа s.

2) Если хотя бы один из элементов a и b периодический, то верно утверждение, обратное к 1).

5.43. Пусть a и b – периодические элементы группы, $b^{-1}ab = a^2$ и $o(b) = 5$. Каков $o(a)$?

5.44. Пусть $b^{-1}ab = a^s$, где a и b – периодические элементы группы порядка α и β соответственно и s – целое число.

1) $s^{(\beta, \varphi(\alpha))} \equiv 1 \pmod{\alpha}$.

2) $(\beta, \varphi(\alpha)) \neq 1$ при $ab \neq ba$.

(φ – функция Эйлера.)

5.45. Пусть G – периодическая группа и p – наименьший из порядков её неединичных элементов.

1) Элемент порядка p группы G не может быть сопряжён в G со своей степенью, отличной от него.

2) Каждая нормальная подгруппа порядка p группы G содержится в $Z(G)$.

5.46. Циклические группы порядка 2 – единственные периодические группы, имеющие точно два класса сопряжённых элементов.

5.47. Пусть a – периодический элемент группы G. Тогда

1) $a^G \cap \langle a \rangle = a^{N_G(\langle a \rangle)}$,

2) $|a^G \cap \langle a \rangle|$ делит $|a^G|$,

3) $|a^G \cap \langle a \rangle|$ делит $\varphi(o(a))$.

5.48. Пусть $a \in G$, $o(a) = n$ и $|a^G| = j$ $(n, j \in \mathbf{N})$. Если $(j, \varphi(n)) = 1$, то никакие две степени элемента a не сопряжены в G.

5.49. Пусть t – инволюция группы G, $C_G(t) = \langle t \rangle \times H$, где $H \simeq S_3$, и $Q := \langle t \rangle \times \langle a \rangle$, где a – инволюция из H. Тогда $|N_G(Q)| = 4m$, где $m \in \{1, 2, 3\}$.

5.50. Пусть $A \leq B \leq G$ и B конечна. Предположим, что B содержит подгруппу, сопряжённую с A в G, но не в B. Пусть $\mathcal{H}$ – множество всех таких подгрупп в B и j – наибольший общий делитель индексов $|A : A \cap A_1|$, где $A_1 \in \mathcal{H}$. Тогда $|B : A|$ делится на j.

5.51. Пусть A и B – подгруппы конечной группы G, α – число подгрупп, сопряжённых с A и содержащихся в B, а β – число подгрупп, сопряжённых с B и содержащих A. Тогда

$$\alpha |N_G(A)| = \beta |N_G(B)|.$$

5.52. Если $H \leq G$, $g \in G$ и gH – нормальное подмножество в G, то $H \trianglelefteq G$.

5.53. Если M – нормальное подмножество в G, то $\{g \in G \mid gM \subseteq M\}$ – нормальное подмножество в G и $\{g \in G \mid gM = M\} \trianglelefteq G$.

5.54. Если объединение нескольких левых смежных классов группы G по некоторой её неединичной подгруппе есть истинное нормальное подмножество в G, то группа G непроста.

5.55. Пусть H – собственная подгруппа G. Если квадрат $M^2 := MM$ некоторого смежного класса M группы G по H содержит нормальное подмножество J из G, то

$$H\langle JJ^{-1} \rangle < G.$$

В частности, если $J \not\subseteq \{1\}$, то группа G непроста.

5.56. Пусть M – любое подмножество группы G и $H \leq N_G(M)$. Тогда

$$\langle M \setminus H \rangle \trianglelefteq \langle M, H \rangle = \langle M \rangle H.$$

5.57. Пусть $G = \langle M \rangle$, где M – нормальное подмножество из G, и H – произвольная подгруппа в G. Тогда $\langle M \setminus H \rangle \trianglelefteq G$.

5.58. Пусть M – подмножество группы G.

1) $\langle M \setminus N_M(M) \rangle \trianglelefteq \langle M \rangle$.

2) Не всегда $\langle N_M(M) \rangle \trianglelefteq \langle M \rangle$.

5.59. Пусть M – класс сопряжённых элементов группы G и $G = \langle M \rangle$.
1) $G = \langle M \setminus H \rangle$ для любой истинной подгруппы H из G.
2) Если $M = M_1 \cup M_2$, то либо $G = \langle M_1 \rangle$, либо $G = \langle M_2 \rangle$.

5.60. Пусть G – простая неабелева группа и M – её минимальное порождающее подмножество (т. е. $G = \langle M \rangle$, но $G \neq \langle M_1 \rangle$ при $M_1 \subset M$). Тогда $N_M(M) = \varnothing$.

5.61. Пусть M – нормальное подмножество группы G и $n \in \mathbf{N}$. Тогда $|\langle M \rangle : \langle M^n \rangle|$ делит n. ($M^n := \underbrace{M \ldots M}_{n \text{ раз}}$.)

5.62. Пусть a и b – элементы группы G. Описать все пары (a_1, b_1) элементов из G такие, что

$$a_1 b_1 = ab \text{ и } b_1 a_1 = ba.$$

Верно ли, что число всех таких пар (a_1, b_1) равно $|C_G(ab)|$?

5.63. Для элементов a, b, a_1, b_1 группы G равносильны условия:
(1) $a_1 b_1$ сопряжён в G с ab, а $b_1 a_1$ сопряжён в G с ba;
(2) существуют элементы x и y в G такие, что $a_1 = x^{-1}ay$ и $b_1 = y^{-1}bx$.

5.64. Пусть $\{a, b\} \subseteq G$. Равносильны условия:
(1) $a^2 = b^2$;
(2) $b = ca$, где $c \in C_G(a^2)$ и $c^a = c^{-1}$.

5.65. Пусть $G = \langle a, b \rangle$, где $a, b \in G$ и $b^a = b^{-1} \neq b$. Тогда $\langle a^2 \rangle \subseteq Z(G)$ и $G/\langle a^2 \rangle$ – диэдральная группа.

5.66. 1) В группе G $L_2(\mathbf{Q})$ множество G всех матриц вида $\begin{pmatrix} \alpha & \beta \\ 0 & 1 \end{pmatrix}$ $(\alpha, \beta \in \mathbf{Q},\ \alpha \neq 0)$ является подгруппой.
2) В группе G найти элемент a, который сопряжён в G с любой своей степенью a^m при $m \neq 0$.
3) В группе G найти подгруппу, которая сопряжена в G с любой своей собственной подгруппой.

5.67. В периодической группе никакая подгруппа не может быть сопряжена со своей собственной подгруппой.

5.68. Пусть $A \leq B \leq G$, $g \in G$ и $A^g \subseteq B$. Будет ли $|B : A^g| = |B : A|$?

5.69. В группе $GL(2, \mathbb{Q})$ найти подгруппу G и элемент a такие, что

1) G – группа без кручения (т. е. порядки всех её неединичных элементов бесконечны),

2) $\langle a \rangle \lhd G$,

3) $\langle a \rangle \not\subseteq Z(G)$ (следовательно, a сопряжён в G с a^{-1}).

(Таким образом, утверждение 5.45 не переносится на "случай $p = \infty$".)

5.70. Пусть A – абелева группа и $G = D(A)$ – обобщённо диэдральная группа. Тогда G имеет нормальную подгруппу A_1 индекса 2 такую, что

1) $A_1 \simeq A$;

2) $G \setminus A_1$ (смежный класс по A_1) состоит из инволюций;

3) $G = A_1 \lambda \langle t \rangle$, где t – любой элемент из $G \setminus A_1$;

4) если $H \leq D(A)$, то

либо $H \leq A_1$ и тогда $H \trianglelefteq G$,

либо $|H : H \cap A_1| = 2$ и $H \simeq D(H \cap A_1)$.

Найти $Z(G)$ и $C_G(t)$ для $t \in G \setminus A_1$.

5.71. Пусть $G = D_{2n}$ – группа диэдра порядка $2n$, т. е. $G = \langle a \rangle \langle b \rangle$, где $o(a) = n$, $o(b) = 2$, и $b^{-1}ab = a^{-1}$. Определить

а) $C_G(a)$, $C_G(b)$ и $Z(G)$,

б) все классы сопряжённых элементов в G,

в) все классы сопряжённых подгрупп в G (указать представители классов) и отметить нормальные подгруппы.

5.72. Пусть r – число классов сопряжённых элементов группы D_{2n}. Тогда

$$r = \begin{cases} \frac{1}{2}(n+3), & \text{если } n \text{ нечётно,} \\ \frac{1}{2}n + 3, & \text{если } n \text{ чётно.} \end{cases}$$

5.73. 1) Для любого натурального $n \geq 3$ существует конечная неабелева группа, содержащая точно n классов сопряжённых элементов.

2) Для любого $n \in \mathbb{N}$ существует конечная неабелева группа, содержащая точно n классов сопряжённых ненормальных подгрупп.

5.74. При каких значениях n

а) группа D_{2n} является прямым произведением двух собственных подгрупп,

б) в группе D_{2n} все инволюции сопряжены между собой,

в) $Z(D_{2n}) = 1$?

5.75. В группе D_∞ найти все классы сопряжённых элементов и все нормальные подгруппы.

5.76. Следующие условия группы G равносильны:
(1) G порождается двумя сопряжёнными инволюциями;
(2) $G \simeq D_{2n}$ для некоторого нечётного n.

5.77. Следующие условия группы G равносильны:
(1) G порождается двумя несопряжёнными инволюциями;
(2) либо $G \simeq D_{2n}$ для некоторого чётного n, либо $G \simeq D_\infty$.

5.78. Пусть $A \leq G$. Равносильны условия:
(1) $G = A \lambda \langle b \rangle$, где $o(b) = 2$ и $a^b = a^{-1}$ для каждого $a \in A$;
(2) A абелева и $G \simeq D(A)$.

5.79. Пусть G – конечная группа, имеющая подгруппу A такую, что все элементы в $G \setminus A$ – инволюции. Тогда либо G – абелева группа, все неединичные элементы которой – инволюции, либо подгруппа A абелева и $G \simeq D(A)$.

§ 6. Кольца, и группы матриц

При изучении групп оказываются полезными и другие алгебраические системы, в частности кольца. *Кольцо* – это тройка $K = (M, +, \cdot)$, где $(M, +)$ – абелева группа, $\cdot$ – ассоциативная операция на M и пара $(+, \cdot)$ дистрибутивна, т. е. $a(b + c) = ab + ac$ и $(b + c)a = ba + ca$ для любых элементов, a, b, c из M. Первая операция называется *сложением*, а вторая – *умножением*, хотя вместо + и $\cdot$ используются и другие знаки. При этом группа $(M, +)$ обозначается через K^+ и называется *аддитивной группой кольца* K. Если кольцо K имеет *единицу* (т. е. элемент 1 такой, что $1 \cdot x = x \cdot 1 = x$ для всех x из M), то множество всех *обратимых элементов* из M (т. е. элементов a, для которых уравнения $xa = ax = 1$ разрешимы в M) с операцией умножения есть группа, которая называется *мультипликативной группой кольца* K и обозначается через K^* (см. 6.1). В частности, каждый обратимый элемент a из K имеет точно один обратный элемент, который обозначается через a^{-1}. Если $a, b \in K \setminus \{0\}$ и $ab = 0$, то каждый из элементов a и b называется *делителем нуля* в K.

Кольцо $K = (M, +, \ )$ называется *полем*, если $(M \setminus \{0\}, \ )$ группа. *Характеристикой поля* K называется число $char(K)$, равное нулю, если $n \cdot 1 \neq 0$ для всех $n \in \mathbf{N}$ (1 – единица поля), и равное наименьшему из чисел $n \in \mathbf{N}$ с $n \cdot 1 = 0$ в противном случае.

Гомоморфизмом кольца R в кольцо K называется отображение $f : R \to K$ такое, что

$$f(x + y) = f(x) + f(y) \text{ и } f(xy) = f(x)f(y) \text{ для всех } x, y \in R.$$

Множество $Ker(f) = \{r \in R \mid f(r) = 0\}$ называется *ядром гомоморфизма* f. *Идеалом* кольца R называется его подкольцо I такое, что $rI \cup Ir \subseteq I$ для каждого $r \in R$. Подобно понятию фактор-группы вводится понятие *фактор-кольца* R/I кольца R по идеалу I (см. 6.55).

Определение *подкольца* подобно определению подгруппы.

Перечислим обозначения некоторых групп и колец, которые вводятся в задачах этого параграфа:

C – поле всех комплексных чисел,

R – поле всех вещественных чисел,

Q – поле всех рациональных чисел,

Z – кольцо всех целых чисел,

$\mathbf{Z}_n$ – кольцо вычетов по модулю n ($n \in \mathbf{N}$),

$\mathbf{H}$ – кольцо кватернионов,

$M_n(K)$ – кольцо всех $(n \times n)$-матриц над кольцом K,

$GL_n(K) := M_n(K)^*$ – *общая линейная группа степени n над K*,

$SL_n(K)$ – *специальная линейная группа степени n над K*;

$Diag_n(K)$, $T_n(K)$, $UT_n(K)$, $O_n(K)$ – диагональная, треугольная, унитреугольная, ортогональная подгруппа в $GL_n(K)$. Последние шесть обозначений предполагают, что K – коммутативное кольцо с единицей и $n \in N$ (см. 6.21, 6.31). (Имеются и другие обозначения этих групп: $GL(n, K)$, $SL(n, K)$ и т. п.)

Матрица $x \in M_n(K)$ называется *скалярной*, если $x = ke$, где $k \in K$ и e – единичная матрица. Важными элементами группы $GL_n(K)$ являются матрицы

$t_{ij}(\alpha)$ (*элементарные трансвекции*) (см. 6.47). Для любой матрицы x положим:

x_{ij} – элемент, лежащий в i-й строке и j-м столбце в x, и

x^T – матрица, траспонированная к x.

Мы предполагаем, что читатель знаком с основами линейной алгебры. Напомним некоторые определения. *Векторное пространство* над полем F – это множество V с операциями сложения ($u + v \in V$ для $u, v \in V$) и умножения на скаляр ($fv \in V$ для $f \in F$ и $v \in V$) такими, что: 1) V – абелева группа по сложению; 2) $f(u + v) = fu + fv$. $(f_1 + f_2)v = f_1v + f_2v$; 3) $(f_1f_2)v = f_1(f_2v)$, $1v = v$ для любых $u, v \in V$; $f, f_1, f_2 \in F$; 1 – единица поля F. Размерность пространства V (т. е. мощность его базы (или базиса)) обозначается через $dim(V)$, а отображение α: $V \to V$ называется *линейным оператором* на V (или *эндоморфизмом* V), если $(u+v)^\alpha = u^\alpha + v^\alpha$ и $(fv)^\alpha = fv^\alpha$ при $u, v \in V$ и $f \in F$. Множество всех линейных операторов V относительно операций сложения и умножения ($v^{\alpha+\beta} = v^\alpha + v^\beta$ и $v^{\alpha\beta} = (v^\alpha)^\beta$) есть кольцо, которое обозначается через $End(V)$. Положим, $GL(V) := End(V)^*$ (другое обозначение: $Aut(V)$). Пусть $B = (v_1, \ldots, v_n)$ – упорядоченная база V. *Матрицей оператора* α относительно B называется матрица α_B, составленная из коэффициентов разложения векторов $v_1^\alpha, \ldots, v_n^\alpha$ по базе B, а именно, если

$$v_i^\alpha = f_{i1}v_1 + \ldots + f_{in}v_n, \quad \text{где } f_{ij} \in F, \ (i = 1, \ldots, n),$$

то

$$a_B = \begin{pmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & & \vdots \\ f_{n1} & \cdots & f_{nn} \end{pmatrix}.$$

Каждое векторное пространство размерности n над полем F, очевидно, изоморфно векторному пространству $V(n, F)$, состоящему из всех последовательностей длины n с элементами из F и с операциями, определяемыми покомпонентно.

Алгеброй над полем F называется множество M с бинарными операциями умножения и сложения и с операцией умножения на элементы из F, которое относительно первых двух операций является кольцом, а относительно двух последних – векторным пространством, причём $f(ab) = (fa)b = a(fb)$ для всех $f \in F$ и $a, b \in M$.

В задачах этого параграфа вводятся понятия группового кольца (6.70), групповой алгебры (6.71) и прямой суммы колец (6.64).

6.1. (Т) Пусть K – кольцо с единицей.

1) K имеет точно одну единицу.

2) Множество всех обратимых элементов кольца K есть группа относительно операции умножения (группа K^*).

3) Если a, x, y – элементы из K такие, что $xa = 1 = ay$, то элемент a обратим и $x = y = a^{-1}$ (обратный элемент к a в группе K^*).

6.2. Пусть M – множество всех комплексных, всех вещественных или всех рациональных чисел. Тогда M с обычными операциями сложения и умножения чисел есть поле (поля **C**, **R** и **Q**).

6.3. 1) Множество всех целых чисел с обычными операциями сложения и умножения есть кольцо (кольцо **Z**).

2) Указать все подкольца в **Z**. Заметить, что существуют кольца без единицы.

3) Найти все подмножества в **Z**, которые относительно операции умножения являются группами.

6.4. Подмножество L кольца K является подкольцом в K тогда и только тогда, когда $(L, +) \leq K^+$ и L замкнуто относительно операции умножения.

6.5. Пусть p – простое число и $M = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbf{Z} \text{ и } p \text{ не делит } b \right\}$. Тогда M есть подкольцо в **Q** (*кольцо p-целых рациональных чисел*).

6.6. Пусть $\{a_1, \ldots, a_n\}$ – подгруппа порядка $n > 1$ мультипликативной группы некоторого поля. Тогда $a_1 + \ldots + a_n = 0$.

6.7. Пусть $m, n \in \mathbf{N}$, ε – первообразный корень степени n из 1 в кольце **C** (например, $\varepsilon = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$), $m \mid n$ и $m < n$. Тогда $1 + \varepsilon^m + \varepsilon^{2m} + \ldots + \varepsilon^{\left(\frac{n}{m}-1\right)m} = 0$.

6.8. При любом кольце K множество $K[x]$ всех многочленов $f(x)$ над K (т. е. с коэффициентами из K) с обычными операциями сложения и умножения многочленов есть кольцо.

6.9. Многочлен $x^n - 1$ делится на многочлен $x^m - 1$ в кольце $K[x]$ тогда и только тогда, когда $m \mid n$.

6.10. Если F – поле, то любой многочлен степени n ($n \in \mathbf{N}$) над F имеет в поле F не более n корней.

6.11. Пусть n – натуральное число.

1) Множество всех классов вычетов по модулю n с операциями сложения и умножения классов есть кольцо. (Классы вычетов по модулю n можно записать в виде $[0], [1], \ldots, [n-1]$, где $[i]$ – множество всех целых чисел, имеющих при делении на n остаток i; тогда $[i] + [j] = [k]$, где k – остаток от деления на n числа $i + j$, и $[i][j] = [s]$, s – остаток от деления на n числа ij.)

(Это кольцо обозначается через $\mathbf{Z}_n$ и называется *кольцом вычетов по модулю n*.)

2) $\mathbf{Z}_n^+ \simeq Z_n$.

6.12. 1) Записать таблицы сложения и умножения элементов кольца $\mathbf{Z}_n$ для каждого $n \leq 8$. В каждом случае указать делители нуля и обратимые элементы. Показать, что $\mathbf{Z}_8^{\cdot} \simeq Z_2 \times Z_2$.

2) $\mathbf{Z}_{16}^{\cdot} \simeq Z_4 \times Z_2$.

6.13. При подходящем $n \in \mathbf{N}$ найти многочлен $f(x)$ степени 2 над $\mathbf{Z}_n$ такой, что

1) $f(x)$ имеет более двух корней в $\mathbf{Z}_n$,

2) $f(x) = (x - a)(x - b) = (x - c)(x - d) \neq (x - a)(x - c)$, где $\{a, b\} \cap \{c, d\} = \varnothing$ $(a, b, c, d \in \mathbf{Z}_n)$.

6.14. Обратимый элемент кольца не является в нём делителем нуля.

6.15. В конечном кольце с единицей каждый ненулевой элемент либо обратим, либо является делителем нуля.

6.16. Пусть $[a] \in \mathbf{Z}_n$ $(a \in \mathbf{Z})$.

1) $[a] \in \mathbf{Z}_n^{\cdot} \Leftrightarrow (a, n) = 1$.

2) Порядок группы $\mathbf{Z}_n^{\cdot}$ равен $\varphi(n)$, где φ – функция Эйлера.

6.17. Пусть $k, m, n \in \mathbf{N}$ и $a \in \mathbf{Z}$. Рассмотрев мультипликативную группу $\mathbf{Z}_n^{\cdot}$ кольца $\mathbf{Z}_n$, доказать следующие утверждения:

1) Если $a^k \equiv 1 \pmod{n}$ и $a^m \equiv 1 \pmod{n}$, то $a^{(k,m)} \equiv 1 \pmod{n}$,

2) (Теорема Эйлера) Если $(a, n) = 1$, то $a^{\varphi(n)} \equiv 1 \pmod{n}$.

6.18. Кольцо $\mathbf{Z}_n$ является полем тогда и только тогда, когда n – простое число.

6.19. Через $\mathbf{F}_4$ обозначим тройку $(M, +, \cdot)$, где $M = \{0, 1, x, y\}$, а $+$ и $\cdot$ – операции на M, задаиные с помощью таблиц:

$+$	0	1	x	y
0	0	1	x	y
1	1	0	y	x
x	x	y	0	1
y	y	x	1	0

$\cdot$	0	1	x	y
0	0	0	0	0
1	0	1	x	y
x	0	x	y	1
y	0	y	1	x

1) $\mathbf{F}_4$ – поле.

2) Любое поле из четырёх элементов изоморфно полю $\mathbf{F}_4$.

6.20. Конечная подгруппа мультипликативной группы поля – циклическая. В частности, мультипликативная группа конечиого поля – циклическая.

6.21. (Т) Пусть $n \in \mathbf{N}$ и K – кольцо.

1) Множество всех $(n \times n)$-матриц над K с обычными операциями сложения и умножения матриц есть кольцо (кольцо $M_n(K)$).

2) Пусть K коммутивно и имеет единицу. Тогда

а) $GL_n(K) := M_n(K)^{\cdot} = \{x \in M_n(K) \mid det(x) \in K^{\cdot}\}$,

б) множество $\{x \in M_n(K) \mid det(x) = 1\}$ есть подгруппа в $GL_n(K)$ (группа $SL_n(K)$);

в) при любом $n \geq 2$ группы $GL_n(K)$ и $SL_n(K)$ неабелевы.

6.22. Пусть K – коммутативное кольцо с единицей и G – множество всех матриц вида $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ над K с $a^2 \neq b^2$. Будет ли G подгруппой в $GL_2(K)$?

6.23. Пусть K – коммутативное кольцо с единицей и $a \in K$. Тогда множество G_a всех невырожденных (т. е. с ненулевым определителем) матриц вида

$$\begin{pmatrix} x & y \\ ay & x \end{pmatrix},$$

где $x, y \in K$, является группой относительно операции умножения матриц.

6.24. Пусть g – нескалярная матрица из $GL_2(K)$, где K – коммутативное кольцо с единицей, и $x \in M_2(K)$. Равносильны условия:

(1) $xg = gx$;

(2) $x = k_1 g + k_2 e$, где $k_1, k_2 \in K$ и e – единичная матрица

6.25. 1) Выписать все элементы кольца $M_2(\mathbf{Z}_2)$.

2) В кольце $M_2(\mathbf{Z}_2)$ найти подкольцо из четырёх элементов, являющееся полем.

3) $GL_2(\mathbf{Z}_2) = SL_2(\mathbf{Z}_2) \simeq S_3$.

6.26. 1) Определить порядки групп $GL_2(\mathbf{Z}_2)$ и $SL_2(\mathbf{Z}_2)$.

2) В группе $G = SL_2(\mathbf{Z}_2)$ найти подгруппу Q, изоморфную группе Q_8 (2.29), и показать, что $G \simeq Q \lambda A$, где $A \simeq Z_3$.

6.27. Подгруппа группы $GL_2(\mathbf{C})$, порождённая матрицами

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

где $i^2 = -1$, изоморфна Q_8.

6.28. 1) Пусть n – натуральное число, $n \geq 2$. Тогда подгруппа группы $GL_2(\mathbf{C})$, порождённая матрицами

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix},$$

где α – примитивный корень степени n из единицы, изоморфна группе D_{2n}.

2) В группе $GL_2(\mathbf{C})$ найти подгруппу, изоморфную группе D_∞.

6.29. В группе $GL_n(K)$ при $n > 1$ существует по крайней мере n подгрупп, изоморфных $GL_{n-1}(K)$. Аналогичное утверждение справедливо и для группы $SL_n(K)$.

6.30. В группе $GL_n(K)$ для любой пары натуральных чиссл (s, t) таких, что $s + t \leq n$, существует подгруппа, изоморфная $GL_s(K) \times GL_t(K)$.

6.31. Пусть K – коммутативное кольцо с единицей 1. Подгруппами группы $GL_n(K)$ являются следующие её подмножества:

а) множество всех диагональных матриц (*диагональная подгруппа* $Diag_n(K)$);

б) множество всех матриц с нулевым углом над главной диагональю (*треугольная подгруппа* $T_n(K)$);

в) множество всех матриц из $T_n(K)$ с единицами на главной диагонали (*унитреугольная подгруппа* $UT_n(K)$);

г) множество всех ортогональных матриц, т. е. матриц a таких, что $aa^{\mathrm{T}} = e$, где a^{T} – матрица, транспонированная к a, а e – единичная матрица (*ортогональная подгруппа* $O_n(K)$);

д) множество всех матриц, у которых в каждой строке и в каждом столбце на одном месте стоит единица, а на остальных – нули (группа, изоморфная симметрической группе S_n).

6.32. $GL_n(K) = SL_n(K) \lambda A$, где $A \simeq K^*$.

6.33. $T_n(K) = UT_n(K) \lambda Diag_n(K)$.

6.34. Если A – подгруппа группы $GL_n(K)$, то множество всех матриц, транспонированных к матрицам из A, образует подгруппу в $GL_n(K)$, изоморфную подгруппе A.

6.35. Пусть M – множество всех матриц вида $\begin{pmatrix} a & 0 \\ b & 1 \end{pmatrix}$, где $a, b \in \mathbf{Z}_n$, $n > 2$, и $a \in \{1, -1\}$. Тогда M является подгруппой в $GL_2(\mathbf{Z}_n)$, изоморфной группе D_{2n}.

6.36. Пусть T – множество всех выражений вида

$$(*) \qquad x_1 + x_2 i + x_3 j + x_4 k,$$

где $\{x_1, x_2, x_3, x_4\} \subseteq \mathbf{R}$, а i, j, k – некоторые три элемента, не входящие в $\mathbf{R}$. Введём в T операции + и · следующим образом:

$$(x_1 + x_2 i + x_3 j + x_4 k) + (y_1 + y_2 i + y_3 j + y_4 k) =$$

$$= (x_1 + y_1) + (x_2 + y_2) i + (x_3 + y_3) j + (x_4 + y_4) k,$$

а умножение получается распространением по дистрибутивности на T следующих соотношений:

$$1x = x1 = x \text{ для всех } x \in T, \quad i^2 = j^2 = k^2 = -1,$$

$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j.$$

Для каждого элемента x вида (*) определим сопряжённый элемент $\bar{x} = x_1 - ix_2 - jx_3 - kx_4$ и модуль $|x| = \sqrt{x\bar{x}} = \sqrt{x_1^2 + x_2^2 + x_3^2 + x_4^2}$.

1) $\mathbf{H} := (T, +, \cdot)$ – кольцо (называемое *кольцом кватернионов*).

2) Каждый ненулевой элемент из T обратим.

3) $\overline{xy} = \bar{y}\,\bar{x}$ для всех $x, y \in T$.

4) Множество всех $x \in T$ с $|x| = 1$ есть подгруппа в $\mathbf{H}^*$ (группа единичных кватернионов). Определить порядка всех её элементов и все её подгруппы.

6.37. Множество $\{1, -1, i, -i, j, -j, k, -k\}$ есть подгруппа в $\mathbf{H}^*$, изоморфная группе кватернионов Q_8 (2.29).

6.38. 1) Группа $\mathbf{H}^*$ имеет точно один элемент порядка 2.

2) Множество всех элементов порядка 4 из $\mathbf{H}^*$ совпадает с множеством всех чисто мнимых кватернионов (т. е. элементов вида $xi + yi + zk$) с единичным модулем.

6.39 В кольце $M_2(\mathbf{H})$ найти матрицу x такую, что $det(x) \neq 0$, но x не обратима. Таким образом, в случае некоммутативного кольца K утверждение 2а) в 6.21 неверно.

6.40. Пусть K – кольцо и $a \in M_n(K)$. Тогда $C_{M_n(K)}(a) := \{x \in M_n(K) \mid xa = ax\}$ – подкольцо в $M_n(K)$ (называемое *централизатором a в $M_n(K)$*).

6.41. Пусть K – кольцо с единицей 1. Найти централизатор:

а) матрицы $x = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, в $M_2(K)$,

б) матрицы $y = \begin{pmatrix} x & o \\ o & x \end{pmatrix}$, в $M_4(K)$.

6.42. Пусть K – кольцо.

1) Множество всех матриц вида

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

с $a, b \in K$ есть подкольцо в $M_2(K)$. Обозначим его через S.

2) S коммутативно если и только если K коммутативно.

3) Если $K \subseteq \mathbf{R}$ и $1 \in K$, то S – поле.

4) Если $K = \mathbf{R}$, то $S \simeq \mathbf{C}$.

5) Если $K = \mathbf{Z}_2$, то S – кольцо из четырёх элементов, которое не изоморфно $\mathbf{Z}_4$ и не является полем.

6) Если $K = \mathbf{Z}_3$, то S – поле из 9 элементов.

6.43. Пусть S – кольцо из предыдущей задачи при $K = \mathbf{C}$.

1) S состоит из всех линейных комбинаций с вещественными коэффициентами матриц

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad c = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}.$$

2) S – коммутативное кольцо (и, в частности, не изоморфно $\mathbf{H}$).

3) Определить подгруппу в S^*, порождённую матрицами a, b, c. Показать, что она изоморфна группе $Z_4 \times Z_2$.

6.44. Множество всех матриц вида $\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$, где $\{a, b\} \subseteq \mathbf{C}$, есть подкольцо в $M_2(\mathbf{C})$, изоморфное кольцу $\mathbf{H}$.

6.45. Пусть a – диагональная матрица из $GL_n(\mathbf{C})$ и все элементы её главной диагонали различны между собой. Найти централизатор a в группе $GL_n(\mathbf{C})$.

6.46. Найти централизатор матрицы $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ в $GL_3(\mathbf{C})$.

6.47. Пусть $G = GL_n(K)$, где K – коммутативное кольцо с единицей и $n > 1$. Пусть e – единичная $n \times n$-матрица и $e(i, j)$ – $n \times n$-матрица,

содержащая на (i, j)-ом месте единицу, а на остальных местах нули ($\{i, j\} \subseteq \{1, \ldots, n\}$). Положим

$$t_{ij}(\alpha) := e + \alpha e(i, j) \quad \text{и} \quad d_i(\alpha) := e + (\alpha - 1)e(i, i) \ (\alpha \in K, i \neq j)$$

(матрицы $t_{ij}(\alpha)$ при $\alpha \neq 0$ называются *элементарными трансвекциями*.)

1) Найти централизаторы в $GL_n(K)$ матрица $t_{ij}(1)$ и $d_i(\alpha)$ при $\alpha \neq 1$.

2) Центр группы G состоит из всех её скалярных матриц (т. е. матриц вида αe, где $\alpha \in K$ и e – единичная матрица).

3) Центр группы $SL_n(K)$ состоит из всех её скалярных матриц.

6.48. Найти централизатор подгруппы $Diag_n(K)$ группе $GL_n(K)$.

6.49. (Т) Пусть K – поле и $n > 1$. Примем обозначения из 6.47.

1) $GL_n(K) = \langle t_{ij}(\alpha),\ d_1(\beta) \mid \alpha,\ \beta \in K,\ i \neq j \rangle$,

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

6.50. Пусть $F = (M, +, \cdot)$ – поле. Определим в M новую операцию $*$ по правилу: $a * b = a + b + ab$. Тогда $(M \setminus \{-1\}, *)$ – группа, изоморфная группе F^*.

6.51. Пусть $K = (M, +, \cdot)$ – произвольное кольцо. Введём в M операцию $\circ$ по правилу:

$$a \circ b = a + b - ab \ \text{ для всех } \ a, b \in M$$

($\circ$ называется *присоединённым умножением* в кольце K).

1) (Единственным) нейтральным элементом относительно $\circ$ в M является нуль кольца K.

2) Множество всех элементов из M, обратимых относительно операции $\circ$, является группой относительно $\circ$. Она называется *присоединённой группой кольца* K.

3) Найти присоединённые группы колец $\mathbf{Z}$ и $\mathbf{Q}$.

6.52. 1) В кольце $M_2(\mathbf{C})$ указать бесконечное множество вырожденных матриц, которое относительно операции умножения матриц является группой.

2) Существует ли в $M_2(\mathbf{C})$ подмножество M такое, что $(M, \cdot)$ – группа и M содержит как вырожденные, так и невырожденные матрицы?

6.53. Множество всех матриц вида

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

с $a \in \mathbf{C}$ является подполем кольца $M_2(\mathbf{C})$. Установить его изоморфизм с полем $\mathbf{C}$.

6.54. Идеал кольца R, отличный от R, не содержит обратимых элементов из R.

6.55. (Т) Пусть I – идеал кольца R. Множество всех подмножеств из R вида $r + I$, где $r \in R$, является кольцом относительно операций сложения и умножения, определяемых правилами:

$$(x + I) + (y + I) = (x + y) + I \quad \text{и} \quad (x + I)(y + I) = xy + I.$$

(Это кольцо обозначается через R/I и называется *фактор-кольцом* R по I).

6.56. Пусть φ – гомоморфизм кольца K в кольцо K'.

1) $\varphi(0) = 0'$, где 0 и $0'$ – нули колец K и K' соответственно.

2) Если K имеет единицу, то $\varphi(1) = 1'$, где 1 и $1'$ – единицы в K и K' соответственно.

6.57. Пусть R – кольцо с единицей 1 и φ – гомоморфизм кольца R в кольцо K такой, что $\varphi(1)$ есть единица в K.

1) Ограничение $\tilde{\varphi}$ гомоморфизма φ на $R^{\cdot}$ есть гомоморфизм группы $R^{\cdot}$ в $K^{\cdot}$.

2) Как связаны $Ker(\varphi)$ и $Ker(\tilde{\varphi})$?

6.58. Определить все идеалы и все фактор-кольца кольца $\mathbf{Z}$. Верно ли, что при любом $n \in \mathbf{N}$ $\mathbf{Z}_n$ есть фактор-кольцо кольца $\mathbf{Z}$?

6.59. Пусть $m, n \in \mathbf{N}$ и $m \mid n$. Тогда отображение

$$\varphi : [a]_n \mapsto [a]_m \quad ([a]_n \in \mathbf{Z}_n,\ a \in \mathbf{Z})$$

есть (корректно определённый) гомоморфизм кольца $\mathbf{Z}_n$ на кольцо $\mathbf{Z}_m$. ($[a]_m$ – класс вычетов по модулю m, содержащий a.)

Указать $Ker(\varphi)$.

6.60. Кольцо $\mathbf{Z}_n$ $(n > 1)$ для любого делителя k числа n имеет точно один идеал мощности k.

6.61. Пусть I – идеал кольца R с единицей и $I \neq R$. Показать, что существует гомоморфизм группы $GL_n(R)$ на группу $GL_n(R/I)$, и найти его ядро.

6.62. В группе $G = GL_2(\mathbf{Z}_{p^2})$ указать p-подгруппу N такую, что $G / N \simeq GL_2(\mathbf{Z}_p)$.

6.63. Пусть p – простое число и R – кольцо p-целых рациональных чисел (см. 6.5). Тогда pR – идеал в R и $R/pR \simeq \mathbf{Z}_p$.

6.64. 1) Пусть A и B – кольца. Тогда множество всех пар (a, b), где $a \in A$ и $b \in B$, с операциями $(a_1, b_1) + (a_2, b_2) + (a_1 + a_2, b_1 + b_2)$ и $(a_1, b_1)(a_2, b_2) = (a_1a_2), (b_1\, b_2)$ есть кольцо (которое называется (внешней) *прямой суммой колец* A и B и обозначается через $A \oplus B$).

2) Кольцо $K = A \oplus B$ имеет подкольца $\tilde{A}$ и $\tilde{B}$ такие, что $\tilde{A} \simeq \tilde{A}$, $\tilde{B} \simeq B$, $K = \tilde{A} + \tilde{B}$, $\tilde{A} \cap \tilde{B} = \{0\}$ и $\tilde{a}\tilde{b} = 0$ для всех $\tilde{a} \in \tilde{A}$ и $\tilde{b} \in \tilde{B}$ (тогда $\tilde{A}$ и $\tilde{B}$ – идеалы в K).

6.65. Описать кольцо $\mathbf{Z}_2 \oplus \mathbf{Z}_2$. Определить его мультипликативную группу и все его подкольца и идеалы.

6.66. Если V – векторное пространство размериости n над полем F и B – его упорядоченная база, то отображение $a \mapsto a_B$ $(a \in End(V))$ (см. введение к § 6) есть изоморфизм кольца $End(V)$ на кольцо $M(n, F)$, а его ограничение

$$i_B: a \mapsto a_B \quad (a \in Aut(V))$$

– изоморфизм группы $GL(V)$ на группу $GL_n(F)$ (*естественный изоморфизм* $GL(V)$ на $GL(n, F)$).

6.67. Пусть A и B – упорядоченные базы векторного пространства V, записанные в виде столбцов, и $\alpha \in GL(V)$. Тогда $\alpha_B = T\alpha_A T^{-1}$, где T – матрица перехода от A к B.

6.68. Пусть V и W – векторные пространства над полем F с упорядоченными базами A и B соответственно. Тогда для $\alpha \in GL(V)$ и $\beta \in GL(W)$ равносильны условия:

(1) $\alpha_A = \alpha_B$;

(2) $\beta = \gamma^{-1}\alpha\gamma$, где γ – (единственный) изоморфизм из V на W, переводящий A в B.

6.69. (Теорема Машке) Пусть G – конечная группа, F – поле и $char(F)$ не делит $|G|$.

1) Пусть G – подгруппа группы $GL_n(F)$, состоящая из матриц вида

$$g_i = \begin{pmatrix} a_i & o \\ b_i & c_i \end{pmatrix} \quad (i = 1, \ldots, |G|),$$

где a_i, b_i, c_i – матрицы размеров $m \times m$, $(n - m) \times m$, $(n - m) \times (n - m)$ и o – нулевая $m \times (n - m)$-матрица $(1 \le m < n)$. Тогда отображение

$$\varphi: g_i \mapsto \begin{pmatrix} a_i & o \\ o & b_i \end{pmatrix} \quad (i = 1, \ldots, |G|)$$

сеть гомоморфизм из G в $GL_n(F)$, матрица $s := \sum_{g \in G} g^{-1}g^{\varphi}$ невырождена и

$s^{-1}Gs = G^{\varphi}$.

2) Пусть $G \leq GL(V)$, где $V \simeq V(n, F)$. Если V имеет G-инвариантное подпространство U ($U^g = U$ для всех $g \in G$), то V имеет также G-инвариантное подпространство W такое, что $V = U + W$ и $U \cap W = \{0\}$ (т. е. V есть *прямая сумма подпространств* U и V).

6.70. Пусть F – кольцо и G – группа. Множество всех формальных сумм вида $\sum_{g \in G} f_g g$, где $f_g \in F$, с операциями

$$\sum_{g \in G} f_g g + \sum_{g \in G} h_g g = \sum_{g \in G} (f_g + h_g) g,$$

$$\left(\sum_{g \in G} f_g g \right) \left(\sum_{g \in G} h_g g \right) = \sum_{g, x \in G} f_g h_x g x = \sum_{g \in G} \left(\sum_{y \in G} f_{gy^{-1}} h_y \right) g$$

($f_g, h_g, f \in F$) является кольцом. (Оно обозначается через FG и называется *групповым кольцом* группы G над F.)

6.71. Пусть F – поле. Тогда групповое кольцо FG вместе с операцией умножения на скаляр, заданной правилом

$$f \left(\sum_{g \in G} f_g g \right) = \sum_{g \in G} (f f_g) g$$

($f_g, h_g, f \in F$), является алгеброй над F (и называется *групповой алгеброй* группы G над полем F).

6.72. Пусть G – группа и K – кольцо с единицей. Если G – имеет неединичный элемент конечного порядка, то кольцо KG имеет делители нуля.

§ 7. Симметрические и знакопеременные группы

Симметрическая группа S_X произвольного множества X определена в § 1. Наряду с обозначением $f(x)$ для образа элемента x при перестановке f мы будем использовать также запись x^f.

Пусть X – конечное множество мощности n. *Циклом* длины m $(2 \leq m \leq n)$ в группе S_X называется перестановка вида

$$\begin{pmatrix} x_1 & x_2 & \dots & x_{m-1} & x_m & y_1 & \dots & y_{n-m} \\ x_2 & x_3 & \dots & x_m & x_1 & y_1 & \dots & y_{n-m} \end{pmatrix}.$$

Краткая её запись – $(x_1 \dots x_m)(y_1) \dots (y_{n-m})$ или, когда множество X ясно из контекста, просто $(x_1 \dots x_m)$ (вместо пробелов между символами здесь допускается ставить запятые). Цикл длины 2 называется *транспозицией*. Циклы $(x_1 \dots x_m)$ и $(z_1 \dots z_s)$ называются *независимыми*, если $\{x_1, \dots, x_m\} \cap \{z_1, \dots, z_s\} = \varnothing$. Единичную перестановку часто называют *циклом длины 1* и обозначают через $(x_1)(x_2) \dots (x_n)$, а также через (x_i) при любом $i \in \{1, \dots, n\}$. Если $x^g = x$, где $x \in X$ и $g \in S_X$, то говорят, что x есть *неподвижная точка перестановки* g.

Пусть $g \in S_X$ и $g = g_1 \dots g_m$ – разложение g в произведение попарно независимых циклов. Циклы $g_1 \dots g_m$ называются *циклическими компонентами* перестановки g. Пусть $l_1, \dots, l_m$ – длины этих циклов, записанные в неубывающем порядке, и r – число неподвижных точек перестановки g $(r \geq 0)$. Последовательность $(\underbrace{1, \dots, 1}_{r \text{ раз}}, l_1, \dots, l_m)$ называется *(циклическим) типом* перестановки g.

Пусть $X = \dot{}\{x_1, \dots, x_n\}$, $n \geq 2$. Рассмотрим многочлен

$$\Delta(x_1, \dots, x_n) = \prod_{i<j} (x_i - x_j)$$

(произведение по всем парам (i, j) чисел из $\{1, \dots, n\}$ таких, что $i < j$). Множество всех линейных множителей этого многочлена находится во взаимно однозначном соответствии с миожеством $\mathcal{P}$ всех двуэлементных подмножеств множества X. Пусть $g \in S_X$. Отображение g индуцирует перестановку элементов множества $\mathcal{P}$. Поэтому

$$\Delta(x_1^g, \dots, x_n^g) = \varepsilon \Delta(x_1, \dots, x_n),$$

где $\varepsilon = \pm 1$. Перестановка g называется *чётной*, если $\varepsilon = 1$, и *нечётной*, если $\varepsilon = -1$. ε называют *знаком* перестановки g и обозначают через $sign(g)$. Множество всех чётных перестановок из S_X является подгруппой в S_X (7.20), которая обозначается через A_X и называется *знакопеременной группой множества* X. Таким образом, A_X есть группа симметрий многочлена $\Delta(x_1, \ldots, x_n)$ в смысле определения из 7.53. При $X = \{1, \ldots, n\}$ она обозначается через A_n. При $n = 1$ единственная перестановка из S_n считается чётной, т.е. $A_1 = S_1$.

В задаче 7.30 вводятся *подгруппы Юнга* группы S_X.

7.1. (Т) Пусть X – конечное множество.

1) Любые два независимых цикла из S_X перестановочны.

2) Каждая неединичная перестановка из S_X одиозначно с точностью до порядка множителей представляется в виде произведения попарно независимых циклов.

3) Если g – перестановка типа $(m_1, \ldots, m_s)$ из S_X, то $o(g) = H.O.K.(m_1, \ldots, m_s)$ – наименьшее общее кратное чисел $m_1, \ldots, m_s$.

7.2. 1) Выписать все элементы группы S_4 (в циклических обозначениях) и определить их порядки.

2) Подсчитать число циклических подгрупп каждого порядка в S_4.

7.3. Определить наибольший из порядков элементов группы S_n для каждого $n \leq 10$.

7.4. 1) Группа S_n имеет не менее $(n-1)!$ элементов порядка n.

2) Если $a \in S_n$ и $o(a)$ есть степень простого числа, то $o(a) \leq n$.

7.5. Пусть $n \in \mathbb{N}$ и $m = p_1^{a_1} \ldots p_s^{a_s}$, где p_i – различные простые числа и $a_i \in \mathbb{N}$. Равносильны условия:

(1) группа S_n имеет элемент порядка m,

(2) $p_1^{a_1} + \ldots + p_s^{a_s} \leq n$.

7.6. Сколько элементов порядка n имеет группа S_n, когда $n = 2p \neq 4$ или $n = p^m$, где p – простое число и $m \in \mathbb{N}$.

7.7. Пусть a – цикл длины m из S_n и k – натуральное число. Каков циклический тип перестановки a^k?

7.8. Если все циклические компоненты перестановки g имеют одну и ту же длину, то g является степенью некоторого цикла.

7.9. Число всех подгрупп группы S_n, которые порождены циклом длины n, равно $\dfrac{(n-1)!}{\varphi(n)}$ (следовательно, $\varphi(n)$ делит $(n-1)!$ при любом $n \in \mathbf{N}$).

7.10. Пусть $a \in S_n$, и любая его степень a^k, отличная от единицы, не имеет неподвижных точек. Тогда порядок a делит n.

7.11. Справедливы следующие соотношения для перестановок из S_n:

1) $(i_1 i_2 \dots i_m) = (i_1 i_2)(i_1 i_3)\dots(i_1 i_m)$,

2) $(ij) = (ki)(kj)(ki)$ при $k \notin \{i, j\}$,

3) $(ij)(ik) = (ijk)$ при $k \neq j$,

4) $(ij)(kl) = (ijk)(ilk)$ при $\{i, j\} \cap \{k, l\} = \varnothing$,

5) $(ijk)^{-1} = (kji)$,

6) $(ijk)^{-1}(ijl)(ijk) = (jkl)$,

7) если $z = (12 \dots n)$, то $z^{-1}(ij)z = (i+1 \;\; j+1)$ при $i < n$, $j < n$ и $z^{-1}(in)z = (i+11)$.

7.12. При любом $n \geq 2$:

1) $S_n = \langle (12), (13), \dots, (1n) \rangle$,

2) $S_n = \langle (12), (23), \dots, (n-1n) \rangle$,

3) $S_n = \langle (12), (12 \dots n) \rangle = \langle (12), (23 \dots n) \rangle$.

7.13. Если a и b – транспозиции группы S_n, то $o(ab) \leq 3$.

7.14. Пусть $a = (a_1, \dots, a_k)$ и $b = (b_1, \dots, b_l)$ независимые циклы $(k, l \in \mathbf{N})$. Вычислить $ab(a_1, b_1)$.

7.15. Пусть $z = (a_1 \dots a_k)$ и $1 \leq i < j \leq k$. Вычислить произведения: $z(a_i a_j)$, $(a_i a_j)z$ и $(a_i a_j)z(a_i a_j)$.

7.16. Вычислить следующие произведения циклов $(k, l, m \in \mathbf{N})$:

1) $(a_1, \dots, a_k, b_1, \dots, b_l, c_1, \dots, c_m)(a_1, b_1, c_1)$.

2) $(a_1, \dots, a_k, b_1, \dots, b_l, c_1, \dots, c_m)(a_1, b_1, c_1)^{-1}$.

7.17. 1) Каждая перестановка симметрической группы S_n есть произведение двух циклов.

2) Для любой перестановки x, имеющей t неподвижных точек, и любого целого s с $0 \leq s \leq t$ существует цикл z такой, что xz есть цикл длины $n - s$.

7.18. Пусть $g, h \in S_n$.

1) $sign(gh) = sign(g)\;\; sign(h)$.

2) Если h – транспозиция, то знаки перестановок g и gh противоположны.

3) Если $(z_1, \dots, z_s)$ – циклический тип g, то $sign(g) = (-1)^t$, где $t = \sum_{i=1}^{s} (z_i - 1)$.

4) $sign(g) = \prod_{i<j} (j-i) / \prod_{i<j} (g(j) - g(i))$.

7.19. Пусть $2 \le |X| < \infty$.

1) Каждая перестановка из S_X является произведением нескольких транспозиций из S_X.

2) Чётная перестановка из S_X не может быть произведением нечётиого числа транспозиций.

3) Нечётиая перестаиовка не может быть произведением чётного числа транспозиций.

7.20. (Т) Пусть $|X| = n \in \mathbb{N}$.

1) Множество всех чётных перестановок множества X есть подгруппа группы S_X (знакопеременная группа A_X).

2) $A_X \simeq A_n$.

3) Если $n \ge 2$, то $|A_n| = n!/2$ (т. е. $|S_n : A_n| = 2$).

7.21. 1) Выписать все элементы группы A_4 и определить их порядки.

2) Определить все подгруппы группы A_4. Заметить, что группа A_4 не имеет подгрупп порядка 6. Следовательно, теорема, обратная теореме Лагранжа, не верна.

3) Группа A_4 порождается двумя элементами a и b, удовлетворяющими соотношениям

$$a^3 = 1, \ b^3 = 1, \ (ab)^2 = 1.$$

7.22. Каков наибольший из порядков элементов группы A_n при каждом $n \le 10$?

7.23. При $n \ge 3$ группа A_n порождается всеми тройными циклами из S_n.

7.24. Пусть $k \in \mathbb{N}$, k нечетно и $3 \le k \le n$. Тогда A_n порождается всеми циклами длины k из S_n.

7.25. При любом $n \ge 3$:

1) $A_n = \langle (123), (124), \dots, (12n) \rangle$,

2) $A_n = \langle (123), (123 \dots n) \rangle$ при нечётном n,

3) $A_n = \langle (123), (23 \dots n) \rangle$ при чётном n.

7.26. При любом $n > 2$ группа A_n содержит подгруппу, изоморфную группе S_{n-2}.

7.27. *Инверсией перестановки* $f \in S_n$ называется пара (i, j) такая, что $1 \le i < j \le n$ и $f(i) > f(j)$. Пусть $I(f)$ – число инверсий f. Тогда

$$f \text{ чётна} \Leftrightarrow I(f) \text{ чётно}.$$

7.28. Определить число инверсий перестановки $(1k)$ группы S_n $(1 < k < n)$.

7.29. Пусть $Y \subseteq X$, $S_X(Y) := \{g \in S_X \mid y^g \in Y$ для всех $y \in Y\}$ (*глобальный стабилизатор* Y в S_X) и $N := \{g \in S_X \mid y^g = y$ для всех $y \in Y\}$ (*поточечный стабилизатор* Y в S_X). Тогда $N \trianglelefteq S_X(Y) \le S_X$ и $S_X(Y)/N \simeq S_Y$.

7.30. Пусть $\{X_1, \ldots, X_k\}$ – разбиение множества X, т. е. $X = X_1 \dot\cup \ldots \dot\cup X_k$ $(k \in \mathbf{N})$. Подгруппа $S(X_1, \ldots, X_k) := \bigcap_{i=1}^{k} S_X(X_i)$, где $S_X(X_i)$ – глобальный стабилизатор X_i в S_X (7.29), называется *подгруппой Юнга* группы S_X, соответствующей данному разбиению.

1) $S(X_1, \ldots, X_k) \simeq S_{X_1} \times \ldots \times S_{X_k}$.

2) Подгруппа в S_X, сопряжённая с подгруппой Юнга группы S_X, является подгруппой Юнга в S_X.

3) Пусть $n = n_1 + \ldots + n_k$, где $n_1, \ldots, n_k \in \mathbf{N}$. Каково число подгрупп Юнга группы S_n, изоморфных $S_{n_1} \times \ldots \times S_{n_k}$?

7.31. Две перестановки из группы S_X, где $|X| < \infty$, сопряжены в S_X тогда и только тогда, когда они имеют одинаковый (циклический) тип. Именно, если a и g – элементы из S_X и

$$a = (x_{11} \ldots x_{1m_1})(x_{21} \ldots x_{2m_2}) \ldots (x_{k1} \ldots x_{km_k}),$$

то

$$a^g = (x_{11}^g \ldots x_{1m_1}^g)(x_{21}^g \ldots x_{2m_2}^g) \ldots (x_{k1}^g \ldots x_{km_k}^g).$$

7.32. Пусть $g \in S_n$ и $m \in \mathbf{Z}$. Тогда элементы g и g^m сопряжены в S_n если и только если $(o(g), m) = 1$.

7.33. При $n \ge 4$ в централизаторе любой инволюции группы S_n имеется более одной инволюции.

7.34. 1) В группе S_n каждый элемент сопряжён со своим обратным элементом. Для цикла $a = (1 \ldots m)$ указать элемент g такой, что $a^g = a^{-1}$.

2) При $n \geq 4$ каждый неединичный элемент g группы S_n

а) содержится в диэдральной подгруппе порядка $2o(g)$,

б) является произведением двух инволюций.

7.35. Централизатор инволюции (12) в группе $S_n (n \geq 2)$ совпадает с подгруппой Юнга $S(\{1, 2\}, \{3, \ldots, n\}) = S_n(\{1, 2\})$ (см. 7.29).

7.36. При $n \geq 3$ $Z(S_n) = 1$.

7.37. Если a – цикл длины n в группе S_n, то

$$C_{S_n}(a) = \langle a \rangle \text{ и } |a^{S_n}| = (n-1)!.$$

7.38. Пусть a и b – циклы в S_n такие, что $ab = ba$. Тогда либо a и b независимы, либо $\langle a \rangle = \langle b \rangle$.

7.39. 1) В группе S_4 найти централизатор инволюции (12)(34).

2) Найти $|C_{S_n}(a)|$, где $a = (12)(34) \ldots (n-1, n)$, при любом чётном n.

7.40. Пусть g – перестановка типа $(z_1, \ldots, z_s)$ из S_n. Для любого $i = 1, 2, \ldots, n$ обозначим через $c(i)$ кратность числа i в последовательности $(z_1, \ldots, z_s)$. Тогда

$$|C_{S_n}(g)| = \prod_{i=1}^{n} c(i)! i^{c(i)}$$

и, следовательно, $|g^G| = n! / \prod_{i=1}^{n} c(i)! i^{c(i)}$.

7.41. Найти все классы сопряжённых элементов групп S_4 и S_5 (для каждого класса указать одного представителя, порядок элементов класса и порядок класса).

7.42. Пусть a – перестановка циклического типа $(z_1, \ldots, z_m)$ из A_n.

1) $a^{S_n} \subseteq A_n$, причём либо $a^{S_n} = a^{A_n}$, либо a^{S_n} – объединение двух равномощных классов сопряжённых элементов группы A_n.

2) $a^{S_n} \neq a^{A_n}$ тогда и только тогда, когда все z_i нечётны и попарно различны.

7.43. Пусть x и y – два цикла длины k в A_n, где $k \leq n-2$ и $n \geq 5$. Тогда x и y сопряжены в A_n.

7.44. Найти все классы сопряжённых элементов групп A_4 и A_5.

7.45. 1) Группа A_5 простая.

2) Группа S_5 имеет точно одну собственную нормальную подгруппу, а именно – A_5.

7.46. (Т) Пусть $n \in \mathbf{N}$ и $n \geq 5$.

1) Группа A_n простая.

2) A_n – единственная собственная нормальная подгруппа в S_n.

7.47. В группе A_5

1) все инволюции сопряжены;

2) централизатор инволюции изоморфен $Z_2 \times Z_2$;

3) имеется подгруппа порядка 4, совпадающая со своим централизатором.

7.48. Группа A_5 порождается двумя элементами a и b, удовлетворяющими соотношениям

$$a^5 = 1,\ b^3 = 1,\ (ab)^2 = 1.$$

7.49. В группе A_5

1) найти все классы сопряжённых элементов,

2) определить строение максимальных подгрупп.

7.50. В группе A_6

1) все инволюции сопряжены;

2) централизатор инволюции изоморфен D_8;

3) имеется циклическая подгруппа порядка 4, совпадающая со своим централизатором.

7.51. При каких значениях n в группе A_n все инволюции сопряжены?

7.52. В группе A_7 найти подгруппу вида $B\lambda A$, где $A \simeq S_4$ и $B \simeq Z_3$, причем A не нормальна в AB.

7.53. Пусть $f(x_1, \ldots, x_n)$ – многочлен от переменных из множества $X = \{x_1, \ldots, x_n\}$ с комплексными коэффициентами и S – множество всех перестановок $\gamma \in S_X$ таких, что $f(\gamma(x_1), \ldots, \gamma(x_n)) = f(x_1, \ldots, x_n)$. Тогда S – подгруппа в S_X (называемая *группа симметрий многочлена* $f(x_1, \ldots, x_n)$). Найти группу симметрий каждого из следующих многочленов (n – наибольший из встречающихся индексов):

$x_1^2 + 2x_2 + x_3^2$,

$(x_1 + x_2)(x_1 + x_3)(x_2 + x_3)$,

$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$,

$x_1x_2 + x_3x_4$,

$x_1x_2 - x_3x_4$,

$(x_1 + x_2)(x_3 + x_4)$,

$(x_1 + x_2 - x_3 - x_4)^2$,

$(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4)$,

$(x_1x_2 - x_3x_4)^2 + (x_1x_3 - x_2x_4)^2$,

$(x_1x_2 - x_3x_4)^2 + (x_1x_3 - x_2x_4)^2$,

$x_1^2x_2 + x_3x_4^2 + x_1^2x_3 + x_2x_4^2$,

$x_1^2 + 2x_2 + x_3^2 + 2x_4$,

$(x_1 - x_2)(x_2 - x_3)(x_3 - x_4)(x_4 - x_1)$,

$x_1x_3 + x_2x_4x_5$.

7.54. При любом натуральном n группа симметрий многочлена $x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + \ldots + x_nx_1^2$ есть циклическая группа порядка n.

§ 8. Группы перестановок. Представления перестановками

Группа перестановок множества X – это подгруппа симметрической группы S_X (равносильное определение дано в § 1). $|X|$ называется *степенью* этой группы. При рассмотрении групп S_X элементы из X часто называют точками.

Пусть $G \leq S_X$, $x \in X$ и $Y \subseteq X$. Положим:

$G_x := \{g \in G \mid x^g = x\}$ – *стабилизатор* x в G;

$G_Y := \{g \in G \mid y^g = y$ для всех $y \in Y\}$ – *поточечный стабилизатор* Y в G;

$G(Y) := \{g \in G \mid y^g \in Y$ для всех $y \in Y\}$ – *глобальный стабилизатор* Y в G (все эти стабилизаторы – подгруппы в G (см. 8.1));

$x^G := \{x^g \mid g \in G\}$ – *орбита* группы G, содержащая x (очевидно, что орбиты группы G попарно не пересекаются и объединение всех её орбит есть X);

$Fix(g) := \{x \in X \mid x^g = x\}$ – *множество неподвижных точек перестановки* g;

$Fix(H) := \{x \in X \mid x^h = x$ для всех $h \in H\}$ при $H \subseteq S_X$.

Стабилизатором двух точек x и y в G называется пересечение $G_x \cap G_y$. Группа G называется *транзитивной*, если она имеет точно одну орбиту (т. е. для любых x, y из X существует $g \in G$ такой, что $x^g = y$). Нетранзитивную группу называют *интранзитивной*. Пусть Y – подмножество из X. Говорят, что группа G *действует* на Y, если Y есть объединение нескольких орбит группы G.

Пусть $G \leq S_X$. Группа G называется *регулярной* (на X), если она транзитивна и $G_x = 1$ для любого $x \in X$. Для любого $k \in \mathbf{N}$ группа G называется *k-транзитивной* (или *k-кратно транзитивной*), если для любых последовательностей $(x_1, \ldots, x_k)$ и $(y_1, \ldots, y_k)$, составленных из k элементов множества X, существует элемент $g \in G$ такой, что $x_i^g = y_i$ при $i = 1, \ldots, k$.

Пусть $\mathcal{S} := \{X_1, \ldots, X_m\}$ – *разбиение* множества X, т.е. $X = X_1 \dot\cup \ldots \dot\cup X_m$. Говорят, что $\mathcal{S}$ есть *система импримитивности* группы G на X, если $Y^g \in \mathcal{S}$ для всех $Y \in \mathcal{S}$ и $g \in G$. Системы импримитивности $\{\{x\} \mid x \in X\}$ и $\{X\}$ называются *тривиальными*. Группа перестано-

вок называется *imprимитивной*, если она транзитивна и обладает нетривиальной системой импримитивности. Транзитивная, но не импримитивная, группа называется *примитивной*.

Пусть G – произвольная группа и $\mathcal{P}$ – гомоморфизм группы G в симметрическую группу S_X. В этом случае говорят, что $\mathcal{P}$ есть *представление группы G перестановками множества X* или что G *действует на X посредством $\mathcal{P}$*. Слова "посредством $\mathcal{P}$" опускают, если из контекста ясно, о каком $\mathcal{P}$ идёт речь; при этом орбиты группы $\mathcal{P}(G)$ называют орбитами группы G. $|X|$ называется *степенью* представления $\mathcal{P}$. Представление $\mathcal{P}$ называется *точным*, если $Ker(\mathcal{P}) = 1$, и *транзитивным*, если $\mathcal{P}(G)$ транзитивна. (Иногда *действием* группы G на множестве X называется отображение из $X \times G$ в X с $(x, g) \mapsto x^{\mathcal{P}(g)}$, где $\mathcal{P}$ – некоторое представление $G \to S_X$.) Следующие два вида представлений применяются особенно часто.

Пусть X – некоторое множество элементов или подмножеств группы G и $H \leq G$.

1) Если для любого $h \in H$ отображение $\mathcal{P}(h) : x \mapsto xh (x \in X)$ есть перестановка множества X (т.е. $Xh = X$), то отображение $\mathcal{P}: h \mapsto \mathcal{P}(h)$ $(h \in H)$ является гомоморфизмом H в S_X (см. 8.25). В этом случае говорят, что $\mathcal{P}$ есть *представление H на X сдвигами* или что H *действует на X сдвигами*.

2) Если для любого $h \in H$ отображение $\mathcal{Q}(h) : x \mapsto x^h$ $(x \in X)$ есть перестановка множества X (т. е. $X^h = X$), то отображение $\mathcal{Q} : h \mapsto \mathcal{Q}(h)$ $(h \in H)$ является гомоморфизмом из H в S_X (см. 8.25). В этом случае говорят, что $\mathcal{Q}$ есть *представление H на X сопряжениями или* что H *действует на X сопряжениями*.

Пусть $G \leq S_X$ и $H \leq S_Y$. Говорят, что G и H *подобны* (или *изоморфны как группы перестановок*), если существуют взаимно однозначное отображение f из X на Y и изоморфизм φ из G на H такие, что

$$f(x^g) = f(x)^{\varphi(g)} \text{ для всех } x \in X \text{ и } g \in G$$

(т. е. G и H изоморфны и действуют "одинаково" на своих множествах точек).

Представления перестановками $\mathcal{A} : G \to S_X$ и $\mathcal{B} : G \to S_Y$ называются *эквивалентными*, если существует взаимно однозначное отображение f из X на Y такое, что $f^{-1}\mathcal{A}(g)f = \mathcal{B}(g)$ для всех $g \in G$.

Пусть W – обычное 1-мерное (прямая), 2-мерное (плоскость) или 3-мерное эвклидово пространство. Перестановка множества W, которая не изменяет расстояние между точками, называется *движением* (или *изометрией*) пространства W. Множество всех движений W с операцией умножения движений (как перестановок) является группой (8.44). Она называется *эвклидовой группой* размерности n, где n – размерность W, и обозначается через $\mathbf{E}(n)$. Пусть F – некоторая фигура (т. е. любое множество точек) из W. Множество всех движений W,

совмещающих фигуру F с собой, образует подгруппу в $\mathbf{E}(n)$ (8.44). Она называется *группой симметрий фигуры* F в W.

8.1. Пусть G – группа перестановок множества X, $x \in X$ и $Y \subseteq X$.

1) G_x (стабилизатор x в G), G_Y (поточечный стабилизатор Y в G) и $G(Y)$ (глобальный стабилизатор Y в G) – подгруппы в G.

2) $\bigcap\limits_{x \in X} G_x = 1$.

3) $G_Y \trianglelefteq G(Y)$, и $G(Y)/G_Y$ изоморфна подгруппе из S_Y. Если $G = S_X$, то $G(Y)/G_Y \simeq S_Y$.

8.2. (Т) Пусть $G \leq S_X$ и $x \in X$. Тогда

1) $|x^G| = |G : G_x|$;

2) если группа G транзитивна, то $|G| = |X| \cdot |G_x|$;

3) если $g \in G$, то $G_{x^g} = g^{-1} G_x g$.

8.3. Пусть $G \leq S_n$ и g – p-элемент из G для некоторого простого числа p, не делящего n. Тогда p не делит $|Fix(g)|$.

8.4. Пусть G – транзитивная группа перестановок множества X, $x \in X$, и $H \leq G$.

1) H транзитивна (на X) $\Leftrightarrow$ $G_x H = G$.

2) H регулярна $\Leftrightarrow$ $G_x H = G$ и $G_x \cap H = 1$.

3) Если H регулярна, то $|H| = |X|$.

8.5. Пусть $G \leq S_X$, $N \trianglelefteq G$ и N регулярна (на X). Тогда $G = N \lambda G_x$ для всех $x \in X$.

8.6. Пусть G – абелева транзитивная подгруппа в S_X.

1) G регулярна.

2) G – максимальная абелева подгруппа в S_X.

8.7. Центр неабелевой группы перестановок не транзитивен.

8.8. Если A – циклическая транзитивная подгруппа из S_n, то $A = \langle a \rangle$, где a – цикл длины n.

8.9. Пусть G – конечная транзитивная подгруппа в S_X и $x \in X$. Тогда $N_G(G_x)$ действует транзитивно на множестве $Fix(G_x)$.

8.10. Каждая транзитивная подгруппа группы S_n содержит не менее $n - 1$ перестановок, не имеющих неподвижных точек.

8.11. (Лемма Бернсайда) Если $G \leq S_X$ и t – число её орбит, то

$$t|G| = \sum_{g \in G} |Fix(g)|.$$

8.12. Пусть G – абелева группа перестановок, имеющих k орбит, и пусть $m_1, \ldots, m_k$ – мощности этих орбит. Тогда

$$H.O.K.(m_1, \ldots, m_k) \leq |G| \leq m_1 \ldots m_k,$$

где левая часть обозначает наименьшее общее краткое чисел $m_1, \ldots, m_k$.

8.13. Пусть G – транзитивная подгруппа группы S_X и $x \in X$.

1) Если $G_x < H < G$ и $B := x^H$, то $\{Bg \mid g \in G\}$ есть система импримитивности группы G.

2) G примитивна $\Leftrightarrow$ G_x – максимальная подгруппа в G.

8.14. Пусть H – подгруппа транзитивной группы перестановок G. Тогда если H транзитивна, регулярна или примитивна, то любая сопряжённая с ней подгруппа H^g ($g \in G$) также транзитивна, регулярна или примитивна соответственно.

8.15. Пусть p – простое число. Тогда любая транзитивная подгруппа группы S_p примитивна.

8.16. Пусть $G = \langle (13), (1\ 2\ 3\ 4) \rangle$ – подгруппа из S_4. Показать, что группа G импримитивна и указать её стабилизаторы точек и системы импримитивностн.

8.17. Указать все (с точностью до сопряжённости, см. 8.14) транзитивные, регулярные и примитивные подгруппы в S_4.

8.18. 1) Группа S_n n-транзитивна.

2) Группа A_n $(n-2)$-транзитивна.

3) Указать все $(n-1)$-транзитивные подгруппы в S_n.

8.19. Пусть G – транзитивная подгруппа из S_X, $x \in X$ и $k \in \mathbb{N}$. Равносильны условия:

(1) G $(k+1)$-транзитивна;

(2) G_x действует k-транзитивно на множестве $X \setminus \{x\}$.

8.20. Если G – k-транзитивная подгрупа в S_n, то $|G|$ делится на $n(n-1)\ldots(n-k+1)$.

8.21. Указать все $(n-2)$-транзитивные подгруппы в S_n.

8.22. Каждая 2-транзитивная группа перестановок примитивна.

8.23. Если $G \leq S_X$, G примитивна и $1 < N \trianglelefteq G$, то N транзитивна.

8.24. Пусть $G \leq S_X$ и $H \leq S_Y$. Равносильны условия:

(1) G подобна H;

(2) существует взаимно однозначное отображение f из X на Y такое, что отображение $g \mapsto f^{-1}gf$ $(g \in G)$ является взаимно однозначным отображением G на H.

8.25. Доказать утверждения 1) и 2), сформулированные во введении к этому параграфу.

8.26. (Т) Пусть $G = (X, \cdot)$ – группа.

1) При любом $g \in G$ отображение $R_g := (X \to X \mid x \mapsto xg)$ есть перестаиовка, а отображение

$$\mathcal{R}_G := (G \to S_X \mid g \mapsto R_g)$$

есть регулярное представление группы G перестановками (которое называется *(правым) регулярным представлением* группы G).

В частности, $\mathcal{R}_G(G) \simeq G$ (теорема Кэли, 1.28).

2) При любом $g \in G$ $L_g := (X \to X \mid x \mapsto g^{-1}x) \in S_X$ и отображение

$$\mathcal{L}_G := (G \to S_X \mid g \mapsto L_g)$$

есть регулярное представление группы G перестановками (которое называется *левым регулярным представлением* группы G).

3) Представления $\mathcal{R}_G$ и $\mathcal{L}_G$ эквивалентны.

4) $C_{S_X}(\mathcal{R}_G(G)) = \mathcal{L}_G(G)$ и $C_{S_X}(\mathcal{L}_G(G)) = \mathcal{R}_G(G)$.

8.27. (Т) Пусть $H \le G$ и X – множество всех правых смежных классов G по H.

1) При любом $g \in G$ $R_{H,g} := (X \to X \mid Ht \mapsto Htg \ (t \in G)) \in S_X$ и отображение

$$\mathcal{R}_{G,H} := (G \to S_X \mid g \mapsto R_{H,g})$$

есть транзитивное представление группы G перестановками (которое называется *представлением группы G перестановками смежных классов по H*).

Указать стабилизаторы точек группы $\mathcal{R}_{G,H}(G)$ и $Ker(\mathcal{R}_{G,H})$.

2) Пусть $K \le G$. Тогда

$$\mathcal{R}_{G,H} \text{ эквивалентно } \mathcal{R}_{G,K} \Leftrightarrow H \text{ и } K \text{ сопряжены в } G.$$

3) Каждое транзитивное представление группы G эквивалентно представлению $\mathcal{R}_{G,K}$ для некоторой подгруппы K из G. Более того, если $G \le S_X$, то G подобна $\mathcal{R}_{G,K}(G)$, где $K = G_x$ для некоторого $x \in X$.

8.28. 1) Пусть $H := \langle a,b \rangle$, где $a = (12345)$ и $b = (2354)$. Тогда H – 2-транзитивная подгруппа порядка 20 в S_5 и $K := \langle a, b^2 \rangle$ – транзитивная подгруппа порядка 10 в A_5.

2) Используя 1), найти в S_6 транзитивную подгруппу, изоморфную S_5, а в A_6 – транзитивную подгруппу, изоморфную A_5.

8.29. Пусть $H \leq G$ и $X = \{H\}^G$ – класс подгрупп, сопряжённых с H.

1) При любом $g \in G$ $C_g := (X \to X \mid H^t \mapsto H^{tg}\ (t \in G)) \in S_X$ и отображение

$$\mathcal{C}_{G,H} := (G \to S_X \mid g \mapsto C_g)$$

есть транзитивное представление группы G перестановками.

2) $\mathcal{C}_{G,H}$ эквивалентно представлению $\mathcal{R}_{G,N_G(H)}$.

8.30. Пусть H – истинная подгруппа конечного индекса n группы G.

1) $G/H_G \simeq\leq S_n$. В частности, $|G/H_G|$ делит $n!$ и $|H : H_G|$ делит $(n-1)!$

2) Если группа G проста, то $|G|$ делит $\frac{n!}{2}$.

8.31. При $n \neq 4$

а) группа S_n не имеет истинных подгрупп индекса, меньшего n, отличных от A_n;

б) группа A_n не имеет истинных подгрупп индекса, меньшего n.

8.32 Пусть $n \neq 1$ и $x \in \{1, \ldots, n\}$.

1) $(S_n)_x$ – максимальная подгруппа в S_n.

2) $(A_n)_x$ – максимальная подгруппа в A_n.

8.33. Конечная группа перестановок, содержащая нечётную перестановку, имеет нормальную подгруппу индекса 2.

8.34. Если конечная группа G содержит подгруппу H простого индекса p и $H_G = 1$, то

а) p является наибольшим простым делителем порядка G,

б) p^2 не делит $|G|$,

в) $C_G(P) = P$ для любой силовской p-подгруппы P из G.

8.35. Группа, имеющая подгруппу индекса 2, 3 и 4, непроста.

8.36. Если группа G имеет подгруппу индекса 5 или 6 и содержит элемент порядка большего чем 6, то G непроста.

8.37. Группа G непроста, если она имеет подгруппу H и элемент a такие, что

1) $|G : H| = 7$, $o(a) > 12$;

2) $|G : H| = 8$, $o(a) > 15$;

3) $|G : H| = 9$, $o(a) > 20$;

4) $|G : H| = 10$, $o(a) > 30$;

5) $|G : H| = n$, $o(a) = p > n$, где p – простое число и $n \in \mathbf{N}$.

8.38. 1) Если группа G порядка hf имеет подгруппу H порядка h и если $f \leq p$, где p – наименьший простой делитель h, то $H \trianglelefteq G$.

2) Обобщить утверждение 1) на случай периодической группы G.

8.39. Пусть G – конечная группа, $\mathcal{P}$ – её регулярное представление перестановками и g – элемент порядка n из G. Тогда $\mathcal{P}(g)$ есть произведение независимых циклов, каждый из которых имеет длину n.

8.40. Пусть G – группа чётного порядка и её силовская 2-подгруппа P циклическая. Тогда G имеет нормальную подгруппу N такую, что $G = N \lambda P$.

8.41. Пусть $G = AB$, где A и B – подгруппы в G, $A \cap B = 1$ и $|A| = 2n$ с нечётным n. Тогда G имеет нормальную подгруппу индекса 2.

8.42. Пусть $G = AB$, где A и B – подгруппы в G, и $|A \cap B|$ нечётен. Предположим, что силовская 2-подгруппа T подгруппы A циклическая. Тогда G имеет нормальную подгруппу N такую, что $G = N \lambda T$.

8.43. Если $|G| = p^n m$, где $m \leq 2p$ и p – простое число ($m, n \in \mathbb{N}$), то G имеет нормальную подгруппу порядка p^n или p^{n-1}.

8.44. Пусть $n \in \{1, 2, 3\}$, W – обычное n-мерное эвклидово пространство и F – некоторая фигура в нём (т. е. любое множество точек из W).

1) Множество всех движений W с операцией умножения движений (как перестановок) является группой (группа $\mathbf{E}(n)$).

2) Множество всех движений W, совмещающих фигуру F с собой, есть подгруппа в $\mathbf{E}(n)$ (*группа симметрий* фигуры F в W).

8.45. 1) Определить элементы группы $\mathbf{E}(1)$, которые а) составляют на месте по крайней мере две точки, б) оставляют на месте точно одну точку, в) не оставляют на месте ни одной точки.

2) Группа $\mathbf{E}(1)$ состоит из всех отображений вида $x \mapsto x + a$ (*сдвигов*) и $x \mapsto -x + a$, где $a \in \mathbf{R}$, если отождествить (введением координат) прямую с множеством $\mathbf{R}$ всех вещественных чисел.

3) Указать в $\mathbf{E}(1)$ регулярную подгруппу.

4) $\mathbf{E}(1) \simeq D(\mathbf{R}^+)$.

8.46. Каковы группы симметрий следующих фигур на прямой:

1) точка,

2) отрезок $[a, b]$,

3) интервал (a, b)?

8.47. 1) Множество всех отображений вида $x \mapsto ax + b$, где $a, b \in \mathbf{R}$ и $a \neq 0$, есть подгруппа в $S_{\mathbf{R}}$ (*аффинная группа прямой*), изоморфная группе из 1.46 и имеющая в качестве подгруппы группу $\mathbf{E}(1)$.

2) В группе пункта 1) указать регулярную нормальную подгруппу.

8.48. 1) Найти стабилизатор двух точек в группе $\mathbf{E}(2)$.

2) Найти стабилизатор G_A произвольной точки A в $\mathbf{E}(2)$ (показав, что для любого $h \in G_A$ существует поворот r с центром в точке A такой, что hr^{-1} оставляет на месте две точки). Доказать, что $G_A \simeq D(T)$, где T – одномерный тор (1.17). Каковы орбиты группы G_A?

3) Множество всех сдвигов плоскости есть регулярная подгруппа $\mathbf{R}(2) \simeq \mathbf{R}^+ \times \mathbf{R}^+$ в $\mathbf{E}(2)$ и $\mathbf{E}(2) = \mathbf{R}(2) \lambda G_A$, где A – произвольная точка плоскости.

8.49. Рассмотрим на плоскости некоторую прямоугольную систему координат и каждую точку (x,y) представим себе как комплексное число $z = x + iy$. Тогда поворот около точки O на угол φ против часовой стрелки может быть задан формулой $z \mapsto e^{i\varphi} z$, симметрия относительно оси Ox – формулой $z \mapsto \bar{z}$ и сдвиг плоскости на вектор $\vec{OM}$, где $M = (a, b)$, – формулой $z \mapsto z + c$, где $c = a + ib$.

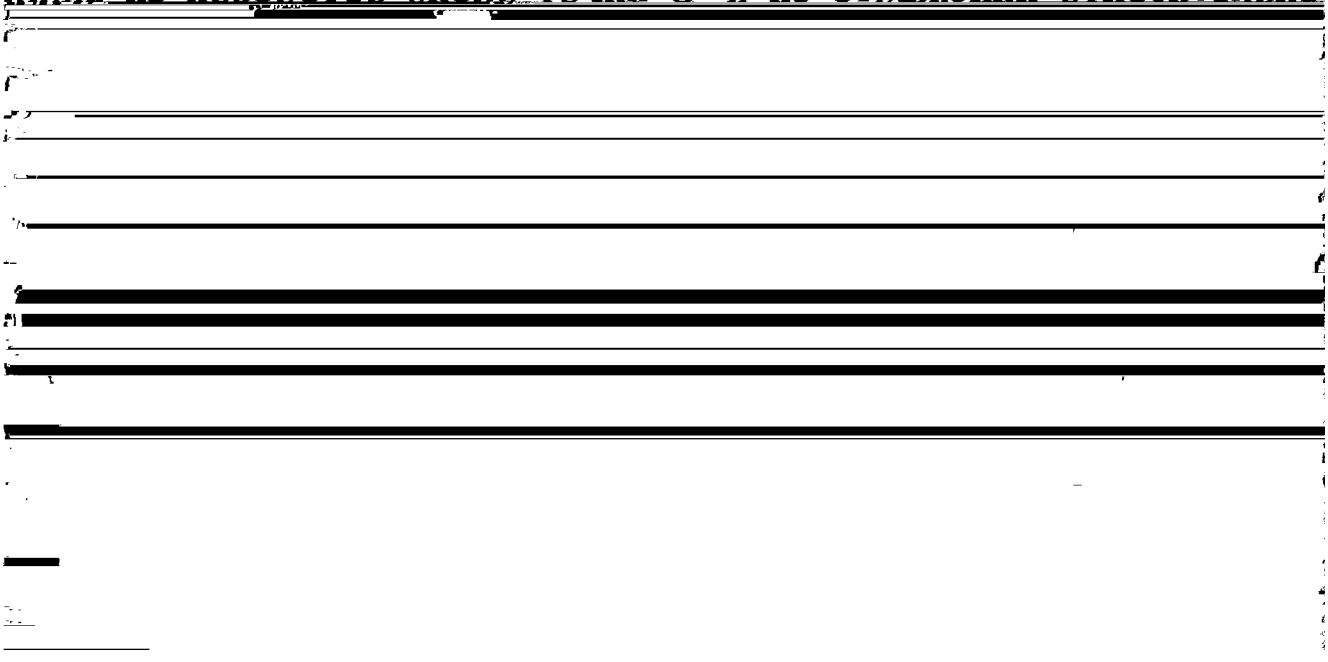
1) При этом соглашении каждое движение плоскости задаётся одной из формул:

$$z \mapsto e^{i\varphi} z + c \quad \text{и} \quad z \mapsto e^{i\varphi} \bar{z} + c,$$

где $0 \leq \varphi < 2\pi$ и $c \in \mathbf{C}$ ($z \in \mathbf{C}$).

2) Найти все периодические элементы группы $\mathbf{E}(2)$.

8.50. Пусть F – плоская фигура конечного диаметра с центром тяжести O. Известно, что группа симметрий фигуры F может состоять лишь из поворотов около точки O и из отражений относительно



14.4. Пусть конечная абелева группа G имеет разложение (*) со свойством (**) и разложение $G = \langle b_1 \rangle \times \ldots \times \langle b_n \rangle$ с подобным свойством. Тогда $m = n$ и $|\langle a_i \rangle| = |\langle b_i \rangle|$ для всех i.

Какова группа G, имеющая единственное разложение вида (*) со свойством (**)?

14.5. Пусть $n_k(G)$ обозначает число элементов порядка k в группе G.

1) Перечислить все ненулевые значения $n_k(G)$ для каждой из следующих групп G:

$$Z_2 \times Z_4,\ Z_2 \times Z_2 \times Z_4,\ Z_3 \times Z_4,\ Z_p \times Z_{p^2} \times Z_{p^3} \text{ и } Z_{p^m} \times Z_{p^n},$$

где p – простое число и $m, n \in \mathbf{N}$.

2) Для каждой из групп, перечисленных в пункте 1), найти число циклических подгрупп каждого порядка.

14.6. Для произвольных конечных абелевых групп A и B равносильны условия (в обозначениях из 14.5):

(1) $n_k(A) = n_k(B)$ для всех $k \in \mathbf{N}$;

(2) $A \simeq B$.

14.7. Пусть G – прямое произведение k циклических подгрупп порядка m ($k, m \in \mathbf{N}$). Определить число всех циклических подгрупп порядка m в G.

14.8. В группе $G = Z_p \times Z_{p^3}$, где p – простое число, указать элемент порядка p^2, который не содержится ни в каком прямом множителе группы G.

14.9. Пусть $l, m, n \in \mathbf{N}$.

1) $Z_l \simeq Z_m \times Z_n \Leftrightarrow l = mn$ и $(m,n) = 1$.

2) $Z_m \times Z_n \simeq Z_k \times Z_d$, где $k = [m,n]$ и $d = (m,n)$.

14.10. (Т) Абелева группа, порождённая конечным числом n элементов, является прямым произведением не более чем n циклических подгрупп.

14.11. $\underbrace{\mathbf{Z}^+ \times \ldots \times \mathbf{Z}^+}_{m \text{ раз}} \simeq \underbrace{\mathbf{Z}^+ \times \ldots \times \mathbf{Z}^+}_{n \text{ раз}} \Leftrightarrow m = n.$

14.12. Пусть A, B, C – конечно порождённые абелевы группы такие, что $A \times C \simeq B \times C$. Тогда $A \simeq B$. (См. также 14.65.)

14.13. Группа $\mathbf{Q}^+$ не является прямой суммой двух собственных подгрупп.

14.14. 1) Если $G = G_1 \times \ldots \times G_n$ – прямое произведение подгрупп $G_1, \ldots, G_n$ группы G, то $G \simeq G_1 \hat{\times} \ldots \hat{\times} G_n$.

2) Если $G = G_1 \hat{\times} \ldots \hat{\times} G_n$, то $G = \hat{G}_1 \times \ldots \times \hat{G}_n$ и $\hat{G}_i \simeq G_i$ для всех $i \in \{1, \ldots, n\}$. (Подгруппы $\hat{G}_i$ определены во введении к § 14.)

14.15. Пусть $G_1, \ldots, G_n$ – нормальные подгруппы в G.

1) Если $G = G_1 \times \ldots \times G_n$, то при любых различных i и j $\langle G_i, G_j \rangle = G_i \times G_j$ (и, следовательно, $g_i g_j = g_j g_i$ для любых $g_i \in G_i$ и $g_j \in G_j$).

2) Если $G = G_1 \ldots G_n$ и $\langle G_i, G_j \rangle = G_i \times G_j$ для любых различных i и j, то будет ли $G = G_1 \times \ldots \times G_n$?

14.16. Пусть σ – перестановка множества $\{1, \ldots, n\}$.

1) Если $G = G_1 \times \ldots \times G_n$, где $G_1, \ldots, G_n$ – подгруппы из G, то $G = G_{\sigma(1)} \times \ldots \times G_{\sigma(n)}$.

2) $G_1 \hat{\times} \ldots \hat{\times} G_n \simeq G_{\sigma(1)} \hat{\times} \ldots \hat{\times} G_{\sigma(n)}$.

14.17. Пусть $G = G_1 \times \ldots \times G_n$.

1) $Z(G) = Z(G_1) \times \ldots \times Z(G_n)$.

2) $G' = G'_1 \times \ldots \times G'_n$.

3) Если группа G конечна, то

$\Phi(G) = \Phi(G_1) \times \ldots \times \Phi(G_n)$,

$O_p(G) = O_p(G_1) \times \ldots \times O_p(G_n)$ для любого простого числа p.

14.18. 1) Для нормальных подгрупп A, B, C группы G равносильны условия:

(а) $G = (A \times B) \times C$;

(б) $G = A \times (B \times C)$;

(в) $G = A \times B \times C$.

2) Для любых групп A, B, C $(A \times B) \times C \simeq A \times (B \times C) \simeq A \times B \times C$.

14.19. 1) Если $G = A \times B$ и $g = (a, b)$ $(a \in A, b \in B)$, то $C_G(g) = C_A(a) \times C_B(b)$.

2) Если $G = A \times B$, $A \leq G$, $B \leq G$ и $g = ab$ с $a \in A$, $b \in B$, то $C_G(g) = C_A(a) \times C_B(b)$.

14.20. Если группа A имеет r классов сопряжённых элементов, а группа B – s классов сопряжённых элементов, то группа $A \times B$ имеет $r \cdot s$ классов сопряжённых элементов.

14.21. Пусть $G = A \times B$, A_1 и A_2 – подгруппы в A, B_1 и B_2 – подгруппы в B.

1) $(A_1 \times B_1) \cap (A_2 \times B_2) = (A_1 \cap A_2) \times (B_1 \cap B_2)$.

2) $\langle A_1 \times B_1,\ A_2 \times B_2 \rangle = \langle A_1, A_2 \rangle \times \langle B_1, B_2 \rangle$.

3) Если $A_1 \trianglelefteq A$ и $B_1 \trianglelefteq B$, то $A_1 \times B_1 \trianglelefteq A \times B$ и $A \times B / A_1 \times B_1 \simeq$ $\simeq A/A_1 \times B/B_1$.

14.22. Пусть $G = A \times B$, где A и B – периодические группы с $\pi(A) \cap$ $\cap\, \pi(B) = \varnothing$ и $H \leq G$.

1) $H = (A \cap H) \times (B \cap H)$.

2) $N_G(H) = N_A(A \cap H) \times N_B(A \cap H)$.

3) A и B – характеристические подгруппы в G.

4) $Aut(G) \simeq Aut(A) \times Aut(B)$.

5) Если группа A имеет s_1 классов сопряжённых подгрупп (из них n_1 нормальных в A), а группа B – s_2 классов сопряжённых подгрупп (из них n_2 нормальных в B), то $A \times B$ имеет $s_1 s_2$ классов сопряжённых подгрупп (из них $n_1 n_2$ нормальных в $A \times B$).

6) Привести пример группы $G = A \times B$ с периодическими группами A, B и с $\pi(A) \cap \pi(B) \neq \varnothing$, для которой утверждения 1)–5) не верны.

14.23. Пусть $G = G_1 \times \ldots \times G_n$.

1) Если φ – гомоморфизм из некоторой группы X в G, то существуют гомоморфизмы $\alpha_i : X \to G_i$ $(i = 1, \ldots, n)$ такие, что $\varphi(x) =$ $= (\alpha_1(x), \ldots, \alpha_n(x))$ при $x \in X$ и $Ker(\alpha) = Ker(\alpha_1) \cap \ldots \cap Ker(\alpha_n)$.

2) Если γ_i есть гомоморфизм G_i на некоторую группу H_i при $i \in \{1, \ldots, n\}$, то отображение

$$\gamma : (g_1, \ldots, g_n) \mapsto (\gamma_1(g_1), \ldots, \gamma_n(g_n)) \quad ((g_1, \ldots, g_n) \in G)$$

есть гомоморфизм группы G в группу $H = H_1 \times \ldots \times H_n$ с ядром $Ker(\gamma) =$ $= Ker(\gamma_1) \times \ldots \times Ker(\gamma_n)$.

14.24. Пусть $G = G_1 \times \ldots \times G_n$.

1) $Aut(G)$ имеет подгруппу A, изоморфную группе $Aut(G_1) \times \ldots$ $\ldots \times Aut(G_n)$.

2) Если G_i характеристична в G для всех $i \in \{1, \ldots, n\}$, то $Aut(G) \simeq$ $\simeq Aut(G_1) \times \ldots \times Aut(G_n)$.

3) Если $G_1 = \ldots = G_n$, то $Aut(H)$ имеет подгруппу S такую, что $S \simeq S_n$ и $\langle S, A \rangle = A \wr S$ (A – как 1)).

14.25. Пусть $G = A \times A$, где A – абелева группа. Пусть $A_1 := \{(a, 1) \mid a \in A\}$ и $A_2 := \{(1, a) \mid a \in A\}$ (так что $G = A_1 \times A_2$).

1) Для любого $\varphi \in Aut(A)$ множество $M_\varphi := \{(a, \varphi(a)) \mid a \in A\}$ есть подгруппа в G и $G = A_1 \times M_\varphi = A_2 \times M_\varphi$.

2) Каждая подгруппа K группы G такая, что $G = A_1 \times K = A_2 \times K$ совпадает с подгруппой M_φ при некотором $\varphi \in Aut(A)$.

14.26. Пусть $G = A \times B$, $A_1 \le A$, $B_1 \le B$, $|A_1| = |B_1|$ и φ – взаимно однозначное отображение из A_1 на B_1. Пусть

$$M_\varphi := \{(a_1, \varphi(a_1)) \mid a_1 \in A_1\}.$$

1) $M_\varphi \le G \Leftrightarrow \varphi$ – изоморфизм.

2) $M_\varphi \trianglelefteq G \Leftrightarrow \varphi$ – изоморфизм, $A_1 \le Z(A)$ и $B_1 \le Z(B)$.

3) Если $M_\varphi \trianglelefteq G$, то G/M_φ есть центральное произведение двух подгрупп, изоморфных A и B, а именно, если ε – естественный изоморфизм G на G/M_φ, то

$G^\varepsilon = \hat{A}^\varepsilon * \hat{B}^\varepsilon$, $\hat{A}^\varepsilon \simeq A$, $\hat{B}^\varepsilon \simeq B$, $\hat{A}^\varepsilon \cap \hat{B}^\varepsilon = \hat{A}_1^\varepsilon = \hat{B}_1^\varepsilon \simeq A_1$, $\hat{A}^\varepsilon / \hat{A}^\varepsilon \cap \cap \hat{B}^\varepsilon \simeq A / A_1$, $\hat{B}^\varepsilon / \hat{A}^\varepsilon \cap \hat{B}^\varepsilon \simeq B / B_1$; причём $(a_1, 1)^\varepsilon = (1, \varphi(a_1)^{-1})^\varepsilon$ для всех $a_1 \in A_1$. (Здесь $\hat{X} := \{(x,1) \mid x \in X\}$ для $X \subseteq A$ и $\hat{Y} := \{(1, y) \mid y \in Y\}$ для $Y \subseteq B$.)

14.27. (Т) Пусть $G = A \times B$, $A_1 \le Z(A)$, $B_1 \le Z(B)$, $A_1 \simeq B_1$ и φ – некоторый изоморфизм A_1 на B_1. Положим

$$N_\varphi := \{(a_1, \varphi(a_1^{-1}) \mid a_1 \in A_1\}.$$

Тогда $N_\varphi \trianglelefteq G$ и если ε – естественный изоморфизм G на G/N_φ, то выполняется заключение пункта 3) предыдущей задачи с заменой в нем последнего равенства равенством $(a_1, 1)^\varepsilon = (1, \varphi(a_1))^\varepsilon$.

(Согласно определению из введения к § 14, G^ε называется φ-*центральным произведением* A и B, что записывается так: $G^\varepsilon = A *_\varphi B$.)

14.28. Пусть $G_1, \ldots, G_n$ – подгруппы группы G. Рассмотрим группу $D := G_1 \hat{\times} \ldots \hat{\times} G_n$ $(= \hat{G}_1 \times \ldots \times \hat{G}_n$ согласно 14.14) и отображение

$$\pi := (D \to G \mid (g_1, \ldots, g_n) \mapsto g_1 \ldots g_n).$$

1) $\pi(\hat{G}_i) = G_i$.

2) π есть гомоморфизм $\Leftrightarrow [G_i, G_j] = 1$ для всех i, j с $i \ne j$.

3) $\pi(D) = G \Leftrightarrow G = G_1 \ldots G_n$,

14.29. При условии предыдущей задачи равносильны утверждения:

(1) π есть гомоморфизм из D на G (и, значит, $G \simeq D/Ker(\pi)$);

(2) существует гомоморфизм γ из D на G такой, что $\gamma(\hat{G}_i) = G_i$ и $Ker(\gamma) \cap \hat{G}_i = 1$ для всех $i \in \{1, \ldots, n\}$;

(3) $G = G_1 * \ldots * G_n$.

14.30. Если $G = A * B$, где $A, B \le G$, то $A \cap B \subseteq Z(G)$ и $G \simeq A *_\varphi B$, где φ – тождественное отображение $A \cap B$ на себя.

14.31. Пусть A, B и G – группы. Равносильны условия:

(1) $G = \tilde{A} * \tilde{B}$ – (внутреннее) центральное произведение подгрупп $\tilde{A}$ и $\tilde{B}$, где $\tilde{A} \simeq A$ и $\tilde{B} \simeq B$;

(2) $G \simeq A *_{\varphi} B$ – (внешнее) центральное произведение групп A и B для некоторого изоморфизма φ подгруппы из $Z(A)$ на подгруппу из $Z(B)$;

(3) существует гомоморфизм γ из $A \times B$ на G такой, что $Ker(\gamma) \cap \cap \hat{A} = 1 = Ker(\gamma) \cap \hat{B}$.

14.32. Пусть A и B – группы и φ – изоморфизм некоторой подгруппы A_1 из $Z(A)$ на подгруппу B_1 из $Z(B)$.

1) $A *_{\varphi} B \simeq B *_{\varphi^{-1}} A$.

2) Если A конечна, то $A *_{\varphi} B \simeq A \Leftrightarrow B_1 = B$.

3) Если центры групп A и B циклические и ψ – любой изоморфизм A_1 на B_1, то будут ли $A *_{\psi} B \simeq A *_{\varphi} B$?

14.33. Пусть $G = Z_{p^k} *_{\varphi} Z_{p^l}$, где p – простое число, $\{k, l\} \subseteq \mathbb{N}$, и φ – изоморфизм между подгруппами порядка p^n записанных множителей. Тогда $G \simeq Z_{p^k} \times Z_{p^{l-n}}$, если $k \geq l$.

14.34. Пусть $G_i = A *_{\varphi_i} B$ $(i = 1, 2)$, где

$$A = \langle a \rangle_{p^3} \times \langle x \rangle_{p^2}, \quad B = \langle b \rangle_{p^3} \times \langle y \rangle_{p^2},$$

$$A_1 = \langle a_1 \rangle_p \times \langle x_1 \rangle_p, \quad B_1 = \langle b_1 \rangle_p \times \langle y_1 \rangle_p$$

(p – простое число, $a_1 = a^{p^2}$, $x_1 = x^p$, $b_1 = b^{p^2}$, $y_1 = y^p$),

$$\varphi_1 : a_1 \mapsto b_1, \ x_1 \mapsto y_1,$$

$$\varphi_2 : a_1 \mapsto y_1, \ x_1 \mapsto b_1.$$

Тогда

$$G_1 \simeq Z_{p^3} \times Z_{p^2} \times Z_{p^2} \times Z_p.$$

$$G_2 \simeq Z_{p^3} \times Z_{p^3} \times Z_p \times Z_p.$$

14.35. Пусть A и B – группы, $A_1 \leq Z(A)$, $B_1 \leq Z(B)$ и $A_1 \simeq B_1$. Предположим, что каждый автоморфизм группы A_1 индуцируется некоторым автоморфизмом группы A (или каждый автоморфизм B_1 индуцируется автоморфизмом B). Тогда

$$A *_{\varphi} B \simeq A *_{\psi} B$$

для любых изоморфизмов φ и ψ из A_1 на B_1.

14.36. Пусть $G_1, \ldots, G_n$ – группы, $Z_i \leq Z(G_i)$ и $Z_i \simeq Z_1$ для всех $i \in \{1, \ldots, n\}$. Тогда существуют группа $H = H_1 * \ldots * H_n$, где $H_i \leq H$, и изоморфизмы β_i из G_i на H_i ($i \in \{1, \ldots, n\}$) такие, что $H_i \cap H_j = \bigcap_{k=1}^{n} H_k = Z_i^{\beta_i}$ для всех $i, j \in \{1, \ldots, n\}$ с $i \neq j$.

14.37. Пусть $G = A * B$ и $H = C * D$ – внутренние центральные произведения такие, что

$$A \simeq C \simeq Z_{4m} \ (m \in \mathbb{N}), \ B \simeq D_8, \ D \simeq Q_8 \text{ и } |A \cap B| = |C \cap D| = 2.$$

Тогда $G \simeq H$.

14.38. Пусть $G = A \times B$, $A \leq G$, $B \leq G$ и $H \leq G$. Если компонента H в A (относительно данного прямого разложения) совпадает с A, то $H \cap A \trianglelefteq A$.

14.39. Пусть H – подпрямое произведение групп A и B (т.е. H – подгруппа из $A \times B$, компоненты которой в A и B совпадают с A и B соответственно). Положим $\hat{X} := \{(x,1) \mid x \in X\}$ для $X \subseteq A$ и $\hat{Y} := \{(1,y) \mid y \in Y\}$ для $Y \subseteq B$.

1) Существуют (единственно определённые) подгруппы A_0 в A и B_0 в B такие, что $H \cap \hat{A} = \hat{A}_0$ и $H \cap \hat{B} = \hat{B}_0$.

2) $A_0 \trianglelefteq A$, $B_0 \trianglelefteq A$ и $\hat{A}_0 \times \hat{B}_0 \trianglelefteq A \times B$.

3) $H / \hat{A}_0 \simeq B$ и $H / \hat{B}_0 \simeq A$.

4) $H / \hat{A}_0 \times \hat{B}_0 \simeq A / A_0 \simeq B / B_0$.

5) Существует изоморфизм ψ из A/A_0 на B/B_0 такой, что

$$H = \{(a,b) \in A \times B \mid (aA_0)^{\psi} = bB_0\}.$$

6) $|H| = |A \| B_0| = |A_0 \| B|$.

14.40. Пусть A и B – произвольные группы с изоморфными факторгруппами $A/A_0 \simeq B/B_0$. Тогда для любого изоморфизма ψ из A/A_0 на B/B_0 множество

$$H_\psi := \{(a,b) \in A \times B \mid (aA_0)^{\psi} = bB_0\}$$

есть подпрямое произведение групп A и B. При этом $H_\psi \cap \hat{A} = \hat{A}_0$, $H_\psi \cap \hat{B} = \hat{B}_0$ в обозначениях из 14.39. Кроме того, $H_\psi / \hat{A}_0 \times \hat{B}_0 \simeq A / A_0$.

(Группа H_ψ называется *ψ-подпрямым произведением групп A и B* (с объединёнными фактор-группами A/A_1 и B/B_1).)

14.41. Пусть G – ψ-подпрямое произведение групп Z_{p^k} и Z_{p^l}, где p – простое число, $\{k, l\} \subseteq \mathbf{N}$, и ψ – изоморфизм между факторгруппами порядка p^n этих групп. Тогда $G \simeq Z_{p^k} \times Z_{p^{l-n}}$, если $k \geq l$.

14.42. Найти все подпрямые произведения групп A и B в следующих случаях:

а) $A = Z_4$, $B = Z_2$;

б) $A = Z_4$, $B = Z_6$;

в) A и B – конечные группы взаимно простых порядков;

г) $A = Z_9$, $B = D_6$;

д) $A = Z_4$, $B = Z_2 \times Z_2$.

14.43. Если M и N – нормальные подгруппы группы G, то $G/M \cap N$ изоморфна подпрямому произведению групп G/M и G/N.

14.44. Пусть $G = ABC$, где A, B, C – нормальные подгруппы в G, и пусть $N = AB \cap AC \cap BC$. Тогда

$$G/N = AN/N \times BN/N \times CN/N.$$

14.45. Пусть $G = \langle G_i \mid i \in I \rangle$, где $G_i \leq G$ и $I = \{1, \ldots, n\}$. Положим $N_i = \langle G_j^G \mid j \in I \setminus \{i\} \rangle$ при $i \in I$ и $N = \bigcap_{i \in I} N_i$. Тогда

$$G/N = \mathop{\times}_{i=1}^{n} G_i N/N.$$

14.46. Если группа порождается конечным множеством своих минимальных нормальных подгрупп, то она является прямым произведением некоторых из этих подгрупп.

14.47. Подгруппа конечной группы G, порождённая всеми её минимальными нормальными подгруппами, называется *цоколем* группы G и обозначается через $Soc(G)$. Доказать, что любая нормальная подгруппа из G, содержащаяся в $Soc(G)$, является прямым произведением некоторого множества минимальных нормальных подгрупп группы G.

14.48. Следующие условия конечной группы G равносильны:

(1) для любой нормальной подгруппы N группы G в G имеется подгруппа M такая, что $G = N \times M$;

(2) $G = Soc(G)$;

(3) G является прямым произведением нескольких простых нормальных подгрупп.

14.49. Минимальная подгруппа конечной группы G является прямым произведением нескольких простых групп, сопряжённых между собой в G.

14.50. Если G – конечная группа и $\langle g^G \rangle \neq G$ для всех $g \in G$, то $G' \neq G$.

14.51. (Т) Конечная группа G автоморфно проста (т. е. не имеет собственных характеристических подгрупп) тогда и только тогда, когда она является прямым произведением некоторого множества изоморфных простых подгрупп.

14.52. Пусть p – простое число. Найти все нормальные и все характеристические подгруппы каждой из следующих групп:

1) $A_5 \times Z_p$,

2) $A_5 \times Z_p \times Z_p$,

3) $A_5 \times A_5 \times Z_p$.

14.53. Пусть $G = G_1 \times \ldots \times G_n$ – прямое произведение подгрупп G_i. Тогда если $N \trianglelefteq G$ и $N' = N$, то $N = (N \cap G_1) \times \ldots \times (N \cap G_n)$.

14.54. Пусть $G = G_1 \times \ldots \times G_n$ – прямое произведение конечных простых подгрупп G_i, среди которых имеется точно m абелевых.

1) Если $m \leq 1$, то каждая неединичная нормальная подгруппа группы G является прямым произведением некоторого множества подгрупп G_i.

2) Дать описание всех нормальных и всех характеристических подгрупп группы G при любом m.

14.55. Пусть G – группа и $H \subseteq G \times G$. Равносильны условия:

(1) $H \leq G \times G$ и $H \simeq G$;

(2) существуют эндоморфизмы α и β группы G с $Ker(\alpha) \cap Ker(\beta) = 1$ и $\alpha\beta \neq 1$ такие, что $H = \{(\alpha(g), \beta(g)) \mid g \in G\}$.

14.56. Пусть G – группа и α, β, γ, δ – её эндоморфизмы такие, что $Ker(\alpha) \cap Ker(\beta) = 1$, $Ker(\gamma) \cap Ker(\delta) = 1$. Положим $G_{\alpha,\beta} = \{(\alpha(g), \beta(g)) \mid g \in G\}$ и $G_{\gamma,\delta} = \{(\gamma(g), \delta(g)) \mid g \in G\}$ (согласно предыдущей задаче это подгруппы из $G \times G$, изоморфные G). Равносильны условия:

(1) $G_{\alpha,\beta} = G_{\gamma,\delta}$;

(2) существует автоморфизм φ группы G такой, что $\alpha = \varphi\gamma$ и $\beta = \varphi\delta$.

14.57. Описать все подгруппы, изоморфные A_5, в группе $A_5 \times A_5$. Показать, что число их равно $|Aut(A_5)| + 2$. Обобщить результат на случай любой простой группы G.

14.58. Пусть G – Ω-группа и $G = \underset{i=1}{\overset{n}{\times}} G_i$, где G_i – Ω-простая (т. е. не имеющая собственных нормальных Ω-подгрупп) Ω-подгруппа в G. Пусть S_1 – прямое произведение всех множителей G_i, которые Ω-изоморфны G_1. Тогда любая нормальная Ω-подгруппа H из G, Ω-изоморфная G_1, содержится в S_1.

14.59. (Теорема Крулля–Ремака–Шмидта). Пусть G – Ω-группа, удовлетворяющая условиям минимальности и максимальности для Ω-подгрупп (см. определение в конце задачи). Пусть

$$G = G_1 \times \ldots \times G_m = H_1 \times \ldots \times H_n,$$

где G_i и H_j – неединичные неразложимые в прямое произведение Ω-подгрупп Ω-подгруппы из G. Тогда $m = n$ и существует нормальный Ω-автоморфизм α группы G такой, что при подходящей перенумерации подгрупп H_j для любого $i \in \{1, \ldots, m\}$

$$G = G_1 \times \ldots \times G_{i-1} \times H_i \times \ldots \times H_n \text{ и } G_i^{\alpha} = H_i.$$

(Говорят, что Ω-группа удовлетворяет *условию минимальности* (*условию максимальности*) для Ω-подгрупп, если во всяком множестве ее Ω-подгрупп имеется минимальный (соответственно, максимальный) по включению элемент.)

14.60. Пусть A и B – подгруппы группы G и $G = A \times B$. Пусть α – некоторый гомоморфизм группы A в $Z(B)$ и $C := \{aa^{\alpha} \mid a \in A\}$. Тогда $G = C \times B$, причём $C = A \Leftrightarrow Ker(\alpha) = A$ (т. е. α тривиален).

14.61. (Т) Пусть G – группа с условиями максимальности и минимальности для нормальных подгрупп и $G_1, \ldots, G_m, H_1, \ldots, H_n$ – её неединичные неразложимые в прямое произведение подгруппы.

1) Пусть $G = G_1 \times \ldots \times G_m = H_1 \times \ldots \times H_n$. Тогда $m = n$ и существует нормальный автоморфизм α группы G такой, что при подходящей перенумерации подгрупп H_i будет $G_i^{\alpha} = H_i$ (и, следовательно, $G_i' = H_i'$ по 12.50).

2) Пусть $G = G_1 \times \ldots \times G_m$. Равносильны условия:

(а) любое разложение G в прямое произведение неединичных неразложимых подгрупп получается из данного перестановкой множителей;

(б) при любых различных i и j из $\{1, \ldots, m\}$ не существует нетривиальных гомоморфизмов из G_i в $Z(G_j)$ (для конечной группы G это означает, что $(|G_i / G_i'|, |Z(G_j)|) = 1$).

14.62. Пусть $\{G_i \mid i \in I\}$ – некоторое множество подгрупп группы G. Говорят, что G есть *прямое произведение подгрупп* G_i с $i \in I$ (запись:

$G = \underset{i\in I}{\times} G_i$), если $G_i \trianglelefteq G$ для всех $i \in I$ и каждый элемент из G однозначно, с точностью до порядка множителей, записывается в виде произведения конечного числа элементов, взятых из некоторых подгрупп G_i.

1) Если $|I| = n \in \mathbb{N}$ и $\{G_i \mid i \in I\} = \{H_1, \ldots, H_n\}$, то $G = \underset{i\in I}{\times} G_i \Leftrightarrow G = H_1 \times \ldots \times H_n$.

2) **Равносильны условия:**

(а) $G = \underset{i\in I}{\times} G_i$;

(б) $G = \langle G_i \mid i \in I\rangle$ и для любого конечного подмножества J из I $\langle G_i \mid i \in J\rangle = \underset{i\in I}{\times} G_i$.

3) **Если** $G = \underset{i\in I}{\times} G_i$, то $Z(G) = \underset{i\in I}{\times} Z(G_i)$ и $G' = \underset{i\in I}{\times} G'_i$.

14.63. Пусть I – множество и каждому $i \in I$ сопоставлена некоторая группа G_i (может быть $G_i = G_j$ при $i \neq j$). Обозначим через M – множество всех функций f из I в $\bigcup_{i\in I} G_i$ таких, что

а) $f(i) \in G_i$ для всех $i \in I$ и

б) $f(i) \neq 1$ лишь для конечного множества индексов i из I.

Определим на M умножение $\cdot$ по правилу

$$(f\cdot g)(i) = f(i)g(i) \quad (f, g \in M).$$

1) $(M, \cdot)$ – группа. (Эта группа обозначается через $\underset{i\in I}{\times} G_i$ и называется (внешним) *прямым произведением групп* G_i *с* $i \in I$.)

2) Если $I = \{1, \ldots, n\}$, то $\underset{i\in I}{\times} G_i \simeq G_1 \times \ldots \times G_n$. Можно ли здесь вместо знака $\simeq$ поставить знак $=$?

3) Существует множество подгрупп $\{\tilde{G}_i \mid i \in I\}$ группы $G = \underset{i\in I}{\times} G_i$ такое, что $\tilde{G}_i \trianglelefteq G$, $\tilde{G}_i \simeq G_i$ для всех $i \in I$, и $G = \underset{i\in I}{\times} \tilde{G}_i$.

4) Если $G = \underset{i\in I}{\times} G_i$, то для любого $s \in S_I$ отображение $\tilde{s} : f \mapsto s^{-1}f$ ($f \in G$) есть автоморфизм группы G ($s^{-1}f(i) = f(s^{-1}(i))$).

14.64. Пусть $\{G_i \mid i \in I\}$ и $\{H_j \mid j \in J\}$ – множества групп.

1) Если $I = J$ и $G_i \simeq H_i$ для всех $i \in I$, то $\underset{i\in I}{\times} G_i \simeq \underset{i\in I}{\times} H_j$.

2) Если $I \cap J = \varnothing$, то $\left(\underset{i\in I}{\times} G_i\right) \times \left(\underset{i\in J}{\times} H_j\right) \simeq \underset{i\in I\cup J}{\times} G_i$, где $G_i = H_i$ при $i \in J$.

14.65. Пусть $G = (M, +)$, где M – множество всех бесконечных последовательностей $(a_1, a_2, \ldots)$ целых чисел, а $+$ – операция на M, определяемая равенством

$$(a_1, a_2, \ldots) + (b_1, b_2, \ldots) = (a_1 + b_1, a_2 + b_2, \ldots).$$

1) G – группа.
2) $G \times \mathbf{Z}^+ \simeq G$.
3) $G \times G \simeq G$.

(Следовательно, из $A \times B \simeq A \times C$ не следует, что $B \simeq C$.)

14.66. Пусть I и G_i – как в 14.63 и пусть F – множество всех функций f из I в $\bigcup_{i \in I} G_i$ таких, что $f(i) \in G_i$ для всех $i \in I$. Определим на F операцию $\cdot$ по правилу $(f \cdot g)(i) = f(i)g(i)$ $(f, g \in M)$. Тогда $(F, \cdot)$ – группа, а $\times_{i \in I} G_i$ – её подгруппа.

(Группа $(F, \cdot)$ обозначается через $\overline{\times}_{i \in I} G_i$ и называется *декартовым произведением групп* G_i *с* $i \in I$.)

§ 15. Полупрямые произведения и сплетения

Согласно определению из § 4, запись $G = A \lambda B$ означает, что группа G является полупрямым произведением своих подгрупп A и B, т. е. $G = AB$, $A \trianglelefteq G$ и $A \cap B = 1$.

Пусть A и B – произвольные группы и φ – гомоморфизм группы B в группу $Aut(A)$. Тогда множество $A \times B$ с операцией

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2^{\varphi(b_1^{-1})}, b_1 b_2)$$

является группой (см. 15.1). Она обозначается через

$A \lambda_\varphi B$ и называется *полупрямым произведением групп A и B (относительно φ)*. Положим $\tilde{a} := (a, 1)$ для $a \in A$ и $\tilde{b} := (1, b)$ для $b \in B$. Отображения $i_A : a \mapsto \tilde{a} (a \in A)$ и $i_B : b \mapsto \tilde{b}$ $(b \in B)$ (являющиеся изоморфизмами по 15.2) называются *каноническими вложениями* групп A и B в G.

Пусть G – группа и $H = G \lambda_{id} Aut(G)$, где id – тождественный изоморфизм $Aut(G)$ на $Aut(G)$. Группа, получающаяся из H заменой каждого элемента $(g, 1)$ элементом g $(g \in G)$ и каждого элемента $(1, a)$ элементом a $(a \in A)$, обозначается через

$Hol(G)$ и называется *голоморфом группы G*.

Пусть A, B – группы, X – множество и $\mathcal{P}$ – гомоморфизм из B в симметрическую группу S_X. Пусть $H := \times_{x \in X} A$ (внешнее прямое произведение $|X|$ экземпляров группы A; элементами его являются всевозможные функции h из X в A такие, что $h(x) \neq 1$ только для конечного числа элементов $x \in X$). Согласно 14.63, существует изоморфизм σ из S_X в $Aut(H)$ такой, что $\sigma(s)$: $h \mapsto s^{-1}h$ $(s^{-1}h(x) = h(s^{-1}(x)))$. (В случае, когда $X = \{1, \ldots, n\}$, элементы из H записываются в виде последовательностей $h = (a_1, \ldots, a_n)$ с $a_i \in A$ и $\sigma(s) : (a_1, \ldots, a_n) \mapsto (a_{s^{-1}(1)}, \ldots, a_{s^{-1}(n)})$.) Тогда композиция $\mathcal{P}\sigma$ есть гомоморфизм из B в $Aut(H)$, и группа

$A \wr_{\mathcal{P}} B := H \lambda_{\mathcal{P}\sigma} B$ называется *сплетением группы A с помощью группы B относительно $\mathcal{P}$* или, короче, *$\mathcal{P}$-сплетением A с B*. Если в этом определении взять $H := \overline{\times}_{x \in X} A$, то полученная группа

$A \bar{\wr}_{\mathcal{P}} B := H \lambda_{\mathcal{P}\sigma} B$ называется *декартовым $\mathcal{P}$-сплетением A с B*. В обоих случаях группа H называется *базой* рассматриваемого сплетения. Вместо $A \wr_{\mathcal{P}} B$ пишется:

$A \wr B$, если $B \leq S_X$ и $\mathcal{P}$ – тождественное отображение B в S_X, и пишется:

$A \wr_r B$, если $\mathcal{P}$ – правое регулярное представление B (впрочем, часто индекс r здесь опускают, если B не задана как группа перестановок какого-либо множества). Подобные сокращения используются и при записи декартова сплетения.

Пусть A и B – подгруппы группы G и $H = \langle A^G \rangle$. Говорят, что G есть ***(внутреннее) сплетение подгруппы A с подгруппой B***, и пишут:

$G = A \wr' B$, – если $G = H \lambda B$ и H есть прямое произведение всех подгрупп группы G, сопряжённых с A в G (т. е. $H = \underset{K \in \mathcal{K}}{\times} K$, где $\mathcal{K} = \{A\}^G$).

Напомним (см. § 9), что группа G называется группой Фробениуса, если $G = N \lambda H$, $N \trianglelefteq G$, $H \leq G$ и $H \cap H^g = 1$ для всех $g \in G \setminus H$; N называется ядром и H – дополнительным множителем группы G.

15.1. Объект $A \lambda_\varphi B$, определённый во введении к этому параграфу, действительно является группой.

15.2. Пусть $G = A \lambda_\varphi B$ – полупрямое произведение групп A и B. Положим $\tilde{a} = (a, 1)$ для $a \in A$ и $\tilde{b} = (1, b)$ для $b \in B$.

1) Отображения $i_A : a \mapsto \tilde{a}$ $(a \in A)$ и $i_B : b \mapsto \tilde{b}$ $(b \in B)$ являются изоморфизмами групп A и B на некоторые подгруппы $\tilde{A}$ и $\tilde{B}$ из G соответственно.

2) $G = \tilde{A} \lambda \tilde{B}$ и $\tilde{a}^{\tilde{b}} = \widetilde{a^{\varphi(b)}}$ для всех $a \in A$ и $b \in B$.

15.3. Пусть A и B – группы. Равносильны условия:

(1) $G = A_1 \lambda B_1$, где $A_1 \simeq A$ и $B_1 \simeq B$;

(2) $G \simeq A \lambda_\varphi B$ для некоторого гомоморфизма φ.

15.4. Пусть $G = A \lambda B$.

1) $b^G \cap B = b^B$ для любого $b \in B$.

2) Любые два элемента из B, сопряжённые в G, сопряжены в B.

3) $C_B(a) = B \cap B^a$ для любого $a \in A$.

4) Утверждения 1) – 3), вообще говоря, не верны в случае, когда $G = AB$, $A \trianglelefteq G$, но $A \cap B \neq 1$.

15.5. Пусть $G = A \lambda B$, $b \in B$ и $B_1 \subseteq B$.

1) $C_G(b) = C_A(b) \lambda C_B(b)$.

2) $C_G(B_1) = C_A(B_1) \lambda C_B(B_1)$.

3) $N_G(B_1) = N_A(B_1) \lambda N_B(B_1)$.

15.6. Пусть G – конечная группа Фробениуса с ядром N и дополнительным множителем H.

1) $C_G(h) \subseteq H$ для всякого $h \in H \setminus \{1\}$.
2) $N = (G \setminus H^G) \cup \{1\}$.
3) $C_G(n) \subseteq N$ для всякого $n \in N \setminus \{1\}$.

15.7. Пусть $G = N \lambda H$. Равносильны условия:
(1) G – группа Фробениуса с ядром N;
(2) ни один неединичный элемент из N не перестановочен ни с одним неединичным элементом из H.

15.8. Пусть $G = A \lambda B$, A – абелева минимальная нормальная подгруппа в G и $B_G = 1$.
1) A – единственная минимальная нормальиая подгруппа в G.
2) $C_{Z(B)}(a) = 1$ для всех $a \in A \setminus \{1\}$.
3) Если $Z(B) \neq 1$, то $A \lambda Z(B)$ – группа Фробениуса с ядром A.

15.9. Определить все (с точностью до изоморфизма) полупрямые произведения вида $\mathbf{Z}^+ \lambda_\varphi \mathbf{Z}^+$.

15.10. Определить голоморфы следующих групп:
1) Z_2,
2) Z_3,
3) $Z_2 \times Z_2$.
4) $\mathbf{Z}^+$.

15.11. $Hol(S_3) \simeq S_3 \times S_3$.

15.12. Если G – совершенная группа (т. е. $Aut(G) = Inn(G)$ и $Z(G) = 1$), то $Hol(G) \simeq G \times G$.

15.13. Следующие условия группы G равносильны:
(1) G – совершенная группа;
(2) всякий раз, когда G есть нормальная подгруппа какой-либо группы X, будет $X = G \times C_X(G)$.

15.14. Пусть $H = \{(a, g) \mid g \in G,\ a \in Aut(G)\}$ с операцией

$$(a_1, g_1)(a_2, g_2) = (a_1 a_2, g_1^{a_2} g_2).$$

Тогда $H \simeq Hol(G)$.

15.15. Пусть $H := Hol(G) = G \lambda A$, где $A = Aut(G)$.
1) $C_H(G) = \{gi(g)^{-1} \mid g \in G\} \simeq G$.
2) $G\,Inn(G) = GC_H(G) = C_H(G) \lambda Inn(G)$ и $H = C_H(G) \lambda Inn(G)$.
3) $Z(H) = C_H(A) = \{g \in Z(G) \mid g^a = g\}$.

15.16. Пусть $H := Hol(G) = G \lambda A$, где $A = Aut(G)$.
1) $N_H(A) = Z(H) \times A$.
2) $C_H(A) = Z(H) \times Z(A)$.
3) $N_H(A)/C_H(A) \simeq Inn(A)$.

15.17. Если $G = A \lambda B$ и $C_B(A) = 1$, то G изоморфна подгруппе из $Hol(A)$, содержащей подгруппу A.

15.18. Пусть G – конечная группа, $Z(G) = 1$ и $Aut(G) = I \lambda K$, где $I = Inn(G)$. Рассмотрим гомоморф G: $Hol(G) = G \lambda (I \lambda K)$. Тогда $G \lambda K \simeq$ $\simeq I \lambda K$.

15.19. Пусть $G = A \lambda B$, причём B действует на A точно (т. е. $C_B(A) = 1$) и неприводимо (т. е. в A нет собственных B-инвариантных подгрупп). Тогда если каждая подгруппа простого порядка из B нормальна в B, то G – группа Фробениуса с ядром A.

15.20. Пусть G и H – группы, $G = A \lambda B$, α – гомоморфизм $A \to H$ и β – гомоморфизм $B \to H$. Предположим, что $\alpha(a^b) = \alpha(a)$ для всех $a \in A$ и $b \in B$. Тогда отображение

$$\gamma : ab \mapsto \alpha(a)\beta(b) \quad (a \in A,\ b \in B)$$

является гомоморфизмом $G \to H \Leftrightarrow [\alpha(A), \beta(B)] = 1$.

15.21. Пусть A и B – группы, $A_1 \le Z(A)$, $B_1 \le Z(B)$ и φ – изоморфизм A_1 на B_1. Предположим, что существует гомоморфизм $\gamma : A \to Aut(B)$ такой, что $\gamma(A_0) = 1$ и $\gamma(A)$ действует тождественно на B_1.

1) В группе $G = B \lambda_\gamma A$ множество

$$N = \{(a_1, \varphi(a_1^{-1})) \mid a_1 \in A_1\}$$

есть нормальная подгруппа.

2) Для любого $X \subseteq G$ обозначим через $\overline{X}$ образ X при естественном гомоморфизме G на G/N. Тогда

$$\overline{G} = \overline{B}\overline{A},\ \overline{B} \simeq B,\ \overline{A} \simeq A,\ \overline{B} \trianglelefteq \overline{G},\ \overline{B} \cap \overline{A} \le Z(\overline{G}),\ \overline{A} \cap \overline{B} \simeq A_1 \simeq B_1 \simeq N.$$

(Имея в виду аналогию с полупрямым и центральным произведениями, группу $\overline{G}$ можно назвать *полуцентральным* (точнее $((\varphi, \gamma))$-*полуцентральным*) *произведением* групп B и A.)

15.22. Построить полуцентральное произведение двух групп, изоморфное группе кватернионов Q_8.

15.23. Пусть $G = A \wr B$, где $B \le S_n$ $(n \in N)$. Тогда существуют подгруппы $A_1, \ldots, A_n$ в G и изоморфизм $b \mapsto \tilde{b}$ из B в G такие, что $G =$ $= H \lambda \tilde{B}$, где $H = \times_{i=1}^{n} A_i$, и $A_i^{\tilde{b}} = A_{b(i)}$ для всех i.

15.24. Пусть $G = A \wr_{\mathcal{P}} B$, где $\mathcal{P}$ – гомоморфизм из B в S_X, и H – база G (следовательно, $G = H \lambda_{\mathcal{P}\sigma} B$, где σ – изоморфизм из S_X в H, определённый во введении к § 15). Пусть i_H и i_B – канонические вложения групп H и B в G (т.е. $i_H(h) = \tilde{h} = (h, 1)$, $i_B(b) = \tilde{b} = (1, b)$), $\tilde{H} := i_H(H)$ и $\tilde{B} := i_B(B)$. Для любого $x \in X$ положим

$$A_x := \{\tilde{h} \in \tilde{H} \mid h(y) = 1 \text{ для всех } y \in X \setminus \{x\}\}.$$

1) $A_x \leq \tilde{H}$ и $A_x \simeq A$ для всех $x \in X$.

2) $\tilde{H} = \underset{x \in X}{\times} A_x$.

3) $G = \tilde{H} \lambda \tilde{B}$ и $A_x^{\tilde{b}} = A_{\mathcal{P}(b)(x)}$ для всех $x \in X$.

15.25. Пусть G, A, B – группы и $n \in \mathbb{N}$. Равносильны условия:

(1) $G = (A_1 \times \ldots \times A_n) \lambda B_1$, где $A \simeq A_1 \leq G$, $B \simeq B_1 \leq G$ и $\{A_1, \ldots, A_n\} = \{A_1\}^G$ (равносильно: $G = A_1 \wr_r B_1$ и $|\{A_1\}^G| = n$);

(2) $G \simeq A \wr_{\mathcal{P}} B$, где $\mathcal{P} = \mathcal{R}_{B,F}$ – представление B на смежных классах по некоторой её подгруппе F индекса n.

15.26. Пусть G, A, B – группы и $\mathcal{P}$ – изоморфизм из B в S_X.

1) $A \wr_{\mathcal{P}} B \simeq A \times B \Leftrightarrow |X| = 1$.

2) Если A, B и X конечны, то $|A \wr_{\mathcal{P}} B| = |A|^{|X|} |B|$.

3) Указать все тройки $A, B, \mathcal{P}$, для которых группа $A \wr_{\mathcal{P}} B$ абелева.

15.27. Пусть $G = Z_n \wr S_2$ ($\simeq Z_n \wr_r Z_2$), где n – нечётное число. Тогда $G \simeq Z_n \times D_{2n}$.

15.28. 1) $Z_2 \wr_r Z_2 \simeq D_8$.

2) Определить строение группы $Z_2 \wr_r Z_3$. Указать все её нормальные подгруппы.

15.29. Пусть $G = Z_4 \wr S_2$.

1) G имеет элемент x такой, что $C_G(x) = \langle x \rangle$.

2) Найти $Z(G)$.

15.30. Пусть $m, n \in \mathbb{N}$, M – множество всех диагональных матриц из $GL(n, \mathbb{C})$, порядок которых делит m, а S – множество всех матриц-перестановок из $GL(n, \mathbb{C})$ ($S \simeq S_n$). Тогда $\langle M, S \rangle \simeq Z_m \wr S_n$.

15.31. Пусть $G = S_{mn}$, где $m, n \in \mathbb{N}$. Тогда G имеет подгруппу, изоморфную $S_m \wr S_n$.

15.32. Пусть G – группа, K – кольцо с единицей и KG – групповое кольцо G над K (см. § 6). Тогда группа $GL(n, KG)$ имеет подгруппу, изоморфную $G \wr S_n$.

15.33. Пусть G – группа и n – натуральное число. Тогда в группе $Aut(\underbrace{G \times \ldots \times G}_{n \text{ раз}})$ имеется подгруппа, изоморфная $Aut(G) \wr S_n$.

15.34. Пусть G имеет подгруппы A и H такие, что $|G : H| = 2$ и $H = A \times A^g$, где $g \in G \setminus H$ и $g^2 \in Z(H)$. Тогда существует инволюция $t \in G \setminus H$ такая, что $G = A \wr' \langle t \rangle$ ($\simeq A \wr S_2$).

15.35. $Z_2 \wr \langle (12)(3) \rangle \simeq (Z_2 \wr S_2) \times Z_2$ ($(12)(3) \in S_3$).

15.36. Если A – группа и $B \leq S(X, Y)$ (подгруппа Юнга группы $S_{X \dot\cup Y}$, см. 7.30), то

$$A \wr B \simeq (A \wr B^X) \times (A \wr B^Y),$$

где $B^X := \{b|_X \mid b \in B\} \leq S_X$ и $B^Y := \{b|_Y \mid b \in B\} \leq S_Y$.

15.37. Если $A_1 \leq A$, $B_1 \leq B$, $\mathcal{P}$ – гомоморфизм B в S_X и $\mathcal{P}_1 = \mathcal{P}|_{B_1}$, то $A_1 \wr_{\mathcal{P}_1} B_1 \simeq \leq A \wr_{\mathcal{P}} B$.

15.38. Если $A_1 \leq A$ и $B_1 \leq B$, то $A_1 \wr_r B_1 \simeq \leq A \wr_r B$.

15.39. Пусть $G = A \wr B$, где A – абелева группа и $B \leq S_n$. Пусть H – база этого сплетения ($H = \underbrace{A \times \ldots \times A}_{n \text{ раз}}$).

1) $H_1 := \{(a_1, \ldots, a_n) \in H \mid a_1 \ldots a_n = 1\}$ есть B-допустимая подгруппа в H, изоморфная $\underbrace{A \times \ldots \times A}_{n-1 \text{ раз}}$.

2) Если $A' \leq A_1 \leq A$, то H имеет B-допустимую подгруппу, изоморфную $(\underbrace{A \times \ldots \times A}_{n-1 \text{ раз}}) \times A_1$.

15.40. Каков центр сплетения $G \wr S_n$?

15.41. Пусть $G = A \overline{\wr}_r B$, $A \neq 1$, H – база в G и $D := \{f \in H \mid f(x) = const$ для $x \in B\}$. По 15.24, $G = \tilde H \lambda \tilde B$, где $\tilde H := i_H(H)$ и $\tilde B := i_B(B)$. Пусть $\tilde D := i_H(D)$.

1) Если $1 < N \trianglelefteq G$, то $N \cap \tilde H \neq 1$.

2) $C_G(\tilde B) = \tilde D$ и $Z(G) = Z(\tilde D)$.

3) Если $exp(A) = m$ и $exp(B) = n$ ($m, n \in \mathbb{N}$), то $exp(G) = mn$.

15.42. Пусть $G = A \wr_r B$, H – база в G, $K := \{f \in H \mid \prod\limits_{b \in B} f(b) \in A'\}$, $\tilde K := i_H(K)$ и $\tilde B := i_B(B)$. Тогда $G' = \tilde K \tilde B'$.

15.43. Если $G = A \wr_r B$, где $A \neq 1$ и B бесконечна, то $Z(G) = 1$.

15.44. Если A и B – p-группы (p – простое число), то

а) $A \wr_r B$ – p-группа,

б) $A \tilde{\wr}_r B$ – p-группа $\Leftrightarrow$ порядки элементов группы A ограничены в совокупности.

15.45. Группа $Z_p \wr_r Z_{p^\infty}$ является p-группой и имеет единичный центр. (Сравните с 5.12.)

15.46. Пусть $G = \mathbf{Z}^+ \wr_r \mathbf{Z}^+$. Тогда G изоморфна подгруппе

$$\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \text{ из } GL_2(\mathbf{R}),$$

где α – трансцендентное число.

§ 16. Свободные группы и определяющие соотношения

Пусть G – группа с порождающим множеством X. Говорят, что G ***порождается множеством X свободно*** или что G есть ***свободная группа со свободным порождающим множеством X***, если G обладает следующим "свойством универсальности": каждая функция α из X в произвольную группу H может быть продолжена до гомоморфизма из G в H. (Такое продолжение γ единственно: $\gamma(x_1^{m_1} \cdot \ldots \cdot x_n^{m_n}) = \gamma(x_1)^{m_1} \cdot \ldots \cdot \gamma(x_n)^{m_n} = \alpha(x_1)^{m_1} \cdot \ldots \cdot \alpha(x_n)^{m_n}$ при $x_1, \ldots, x_n \in X$ и $m_1, \ldots, m_n \in \mathbf{Z}$.) Мощность множества X называется *рангом* этой свободной группы (относительно X). Более общим является понятие "группы с порождающим множеством X и определяющим множеством соотношений R". Для его определения необходимо ввести ряд понятий и, в частности, уточнить выражение "соотношение между элементами множества X". В этом параграфе

X есть некоторое множество.

Предположим, что X непусто, и положим $X_1 = \{(x, 1) \mid x \in X\}$ и $X_{-1} = \{(x, -1) \mid x \in X\}$. Очевидно, $X_1 \cap X_{-1} = \varnothing$. *Слово над X*, или, короче, *X-слово*, – это пустая (обозначаемая через 1) или конечная последовательность элементов из $X_1 \cup X_{-1}$:

$$((x_1, \varepsilon_1), (x_2, \varepsilon_2), \ldots, (x_n, \varepsilon_n)) \qquad (1)$$

($x_i \in X$, $\varepsilon_i \in \{1, -1\}$). Число n называется *длиной слова* (1); длина пустого слова равна 0. Обычно слово (1) записывают в виде

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}, \qquad (2)$$

причем вместо x^1 пишут также просто x. В дальнейшем мы используем условную запись слова в виде (2), возвращаясь при необходимости к записи (1) (такая необходимость возникнет, если некоторые элементы из X записаны как слова вида (2) над X в некоторой группе; см., например, задачу 16.26). Для непустых слов $a = x_1^{\varepsilon_1} \ldots x_m^{\varepsilon_m}$ и $b = y_1^{\delta_1} \ldots y_n^{\delta_n}$ ($x_i, y_j \in X$; $\varepsilon_i, \delta_j \in \{1, -1\}$) положим $ab := x_1^{\varepsilon_1} \ldots x_m^{\varepsilon_m} y_1^{\delta_1} \ldots y_n^{\delta_n}$ (слово длины $m + n$), $a^{-1} := x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1}$, а также $1a = a1 = a$, $1^{-1} = 1$, $a^n := \underbrace{a \ldots a}_{n \text{ раз}}$ при $n \in \mathbf{N}$ и $a^b = b^{-1}ab$.

Пусть W – произвольное (может быть пустое) множество слов над X и $S = \{xx^{-1}, x^{-1}x \mid x \in X\}$. Слова a и b над X называются *W-эквивалентными* (запись: $a \sim_W b$), если b можно получить из a посредством конечного числа вставок и удалений каких-либо слов из $W \cup S$ (т. е. если существует последовательность X-слов $a_1, \ldots, a_n$ такая, что $a_1 = a$, $a_n = b$, и для любых двух соседних членов последовательности существуют слова u и v такие, что один из них равен uv, а другой – uzv для некоторого $z \in W \cup S$).

Запись вида $u = v$, где u и v – X-слова, называется *соотношением над X*, или *X-соотношением* (или соотношением между элементами множества X). Пусть $R = \{u_i = v_i \mid i \in I\}$ – некоторое множество X-соотношений. Говорят, что X-соотношение $u = v$ *выводится* из R (или *является следствием* соотношений множества R), если слово uv^{-1} W-эквивалентно пустому слову, где $W = \{u_i v_i^{-1} \mid i \in I\}$. Множества X-соотношений R_1 и R_2 называются *эквивалентными* (запись: $R_1 - R_2$), если каждое соотношение любого из них выводится из соотношений другого. Соотношения r_1 и r_2 называются *эквивалентными* (запись: $r_1 \sim r_2$), если $\{r_1\} \sim \{r_2\}$.

Пусть теперь X – подмножество группы G. *Значением слова* (2) (или (1)) *в группе* G называется элемент $x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \ldots \cdot x_n^{\varepsilon_n}$ группы G (здесь $x_i^{\varepsilon_i}$ – степень элемента x_i в G); значением пустого слова считается единичный элемент группы G. Скажем, что соотношение $u = v$ *выполнено* (или *справедливо*) в группе G, если значения слов u и v в G равны. Говорят, что множество R соотношений над X есть *определяющее множество соотношений* группы G над X, и пишут

$G = \langle X \mid R \rangle$, если

1) $G = \langle X \rangle$,

2) соотношения из R выполнены в G, и

3) каждое X-соотношение, выполненное в G, выводится из R.

Такая группа G обладает важным свойством "R-универсальности", подобным свойству универсальности свободной группы (см. 16.20, 16.21). Далее

$\mathfrak{W}(X)$ обозначает множество всех X-слов,

$\mathfrak{R}(X)$ – множество всех X-соотношений и

$\mathfrak{W}_R := \{u_i v_i^{-1} \mid i \in I\}$ для $R = \{u_i = v_i \mid i \in I\} \subseteq \mathfrak{R}(X)$.

Пусть $W \subseteq \mathfrak{W}(X)$. Очевидно, отношение $\sim_W$ рефлексивно, симметрично и транзитивно. Все X-слова, W-эквивалентные X-слову a, образуют класс $[a]_W$ W-эквивалентных X-слов. Множество всех классов W-эквивалентных X-слов относительно операции, заданной правилом $[a]_W[b]_W = [ab]_W$, является группой (16.1), которая обозначается через

$\langle X \parallel W \rangle$, а также через

$\langle X \parallel R \rangle$, когда $W = \mathfrak{W}_R$ при $R \subseteq \mathfrak{R}(X)$. В последнем случае вместо $\sim_W$ и $[a]_W$ пишут также $\sim_R$ и $[a]_R$ соответственно. (Группу $\langle X \parallel W \rangle$ иногда

обозначают через $Grp(X : W)$.) Если $G = \langle X \mid R \rangle$, где $X \subseteq G$ и $R \subseteq \mathcal{R}(X)$, то $G \simeq \langle X \parallel R \rangle$ (16.19).

При пустом W W-эквивалентность называют просто *эквивалентностью* и вместо $\sim_W$ и $[a]_W$ пишут соответственно $\sim$ и $[a]$. Оказывается (см. 16.2), что группа $\langle X \parallel \varnothing \rangle$ свободно порождается множеством $\{[x] \mid x \in X\}$ и в каждом её классе $[a]$ содержится точно одно несократимое слово (слово называется *сократимым*, если в нём рядом стоят два символа x и x^{-1} (в любом порядке) для некоторого $x \in X$). Так как отображение $x \mapsto [x]$ $(x \in X)$ взаимно однозначно, то можно рассмотреть группу

$F(X)$, получающуюся из $\langle X \parallel \varnothing \rangle$ заменой каждого элемента $[x]$ при $x \in X$ элементом x (без изменения других элементов). Тогда $F(X)$ есть свободная группа со свободным порождающим множеством X (16.3).

При $X = \{x_1, \ldots, x_m\}$ и $W = \{w_1, \ldots, w_n\}$ вместо $\langle X \parallel W \rangle$ пишут: $\langle x_1, \ldots, x_m \parallel w_1, \ldots, w_n \rangle$; подобно поступают при записи выражений $\langle X \parallel R \rangle$ и $G = \langle X \mid R \rangle$. Заметим, что запись $G = \langle x_1, \ldots, x_m \mid r_1, \ldots, r_n \rangle$ не предполагает, что $x_1, \ldots, x_m$ попарно различны.

Если $G \simeq \langle X \parallel S \rangle$, где S – множество слов или соотношений над X, то говорят, что (X, S) есть *порождающее представление* или *генетический код* группы G.

Если μ – функция, в область определения которой входит X, и w – X-слово, то $w^{(\mu)}$ обозначает слово, получающееся из w заменой каждого элемента $x \in X$ элементом x^{μ}, и

$$W^{(\mu)} := \{w^{(\mu)} \mid w \in W\} \text{ для } W \subseteq \mathcal{W}(X),$$

$$R^{(\mu)} := \{u^{(\mu)} = v^{(\mu)} \mid (u = v) \in R\}^{\cdot} \text{ для } R \subseteq \mathcal{R}(X).$$

16.1. Пусть X – произвольное множество и W – множество X-слов.

1) Равенством $[a]_W[b]_W = [ab]_W$ операция умножения классов W-эквивалентных X-слов определяется правильно (т. е. определение не зависит от выбора представителей класса).

2) Множество всех классов W-эквивалентных X-слов с операцией умножения классов (определённой в 1)) – группа (группа $\langle X \parallel W \rangle$).

16.2. (Т) Пусть $G := \langle X \parallel \varnothing \rangle$.

1) Отображение $\mu : x \mapsto [x]$ $(x \in X)$ есть взаимно однозначное отображение из X в G.

2) В каждом классе $[u]$ $(u \in \mathcal{W}(X))$ имеется точно одно несократимое слово. (В частности, $|\,[u] \cap (X \cup X_{-1})\,| \leq 1$ при $u \in \mathcal{W}(X)$.)

3) G – свободная группа со свободным порождающим множеством $X^{\mu} = \{[x] \mid x \in X\}$.

16.3. Пусть $F(X)$ – группа, определённая во введении к § 16 (определение корректно ввиду 16.2(1)) и пусть $\bar{u}$ означает значение слова

$u \in \mathcal{W}(X)$ в $F(X)$, т.е. $\bar{u} = x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdot \ldots \cdot x_n^{\varepsilon_n}$, если $u = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ ($x_i \in X$, $\varepsilon_i = \pm 1$).

1) $F(X) = \{\bar{u} \mid u \in \mathcal{W}(X)\}$, $\bar{u} = \bar{v} \Leftrightarrow [u] = [v]$, $\bar{u} \cdot \bar{v} = \overline{uv}$ для всех u, $v \in \mathcal{W}(X)$.

2) Отображение $\bar{u} \mapsto [u]$ ($\bar{u} \in F(X)$, $u \in \mathcal{W}(X)$) есть (правильно определенный) изоморфизм из $F(X)$ на $\langle X \parallel \varnothing \rangle$).

3) $F(X)$ есть свободная группа со свободным порождающим множеством X.

4) Всякая свободная группа со свободным порождающим множеством Y таким, что $|Y| = |X|$, изоморфна $F(X)$. В частности, любые две свободные группы одного и того же ранга изоморфны.

16.4. 1) Если $|X| = 1$, то $F(X)$ – бесконечная циклическая группа.

2) Если $|X| > 1$, то группа $F(X)$ неабелева.

16.5. Пусть $W \subseteq \mathcal{W}(X)$). Тогда $\langle X \parallel W \rangle$ изоморфна фактор-группе группы $\langle X \parallel \varnothing \rangle$. А именно отображение

$$\gamma : [u] \mapsto [u]_W \quad ([u] \in \langle X \parallel \varnothing \rangle, \ u \in \mathcal{W}(X))$$

есть гомоморфизм из $\langle X \parallel \varnothing \rangle$) на $\langle X \parallel W \rangle$, причём

$$Ker(\gamma) = \{[u] \mid u \in [1]_W\} = \langle \{[w] \mid w \in W\}^{\langle X \parallel \varnothing \rangle} \rangle .$$

16.6. Если n – целое число и $n \neq 0$, то $\langle a \parallel a^n \rangle$ – циклическая группа порядка $|n|$. Доказать это, а) пользуясь только определением группы $\langle X \parallel W \rangle$, б) с помощью 16.5.

16.7. $\langle a, b \parallel aba^{-1}b^{-1} \rangle$ – прямое произведение двух бесконечных циклических групп.

16.8. Какова группа $\langle a, b \parallel a^3, b^2, aba^{-1} \rangle$?

16.9. Пусть $R \subseteq \mathcal{R}(X)$) и $G = \langle X \parallel R \rangle$. Тогда для любого X-соотношения $u = v$ из R в группе G верно равенство $[u]_R = [v]_R$ (т.е. $[u]_W = [v]_W$, где $W = \mathcal{W}_R$).

16.10. Группа $\langle a, b \parallel ab = ba^k, ba = ab^l \rangle$, где k и l – неединичные натуральные числа, конечна.

16.11. Пусть $R \subseteq \mathcal{R}(X)$ и $u, v \in \mathcal{W}(X)$. Равносильны условия:

(1) соотношение $u = v$ выводится из R;

2) $[u]_R = [v]_R$.

16.12. Пусть $u, v, s, t \in \mathcal{W}(X)$.

1) Соотношение $us = vt$ выводится из соотношений $u = v$ и $s = t$.

2) Соотношение $u = u$ выводится из любого множества X-соотношений.

16.13. Пусть $u, v, s, t \in \mathcal{W}(X)$. Равносильны условия:

(1) $u = v \sim s = t$;

(2) $[u]_W = [v]_W \Leftrightarrow [s]_W = [t]_W$ для любого $W \subseteq \mathcal{W}(X)$.

16.14. Пусть $u, v, s, t \in \mathcal{W}(X)$.

1) $u = v \sim uv^{-1} = 1$.

2) $u = v \sim v = u$.

3) $u = 1 \sim u^{-1} = 1$.

4) $u = v \sim sut = svt$.

5) $uv = t \sim uss^{-1}v = t$.

6) $sus^{-1} = 1 \sim u = 1$.

7) $uv = 1 \sim vu = 1$.

16.15. Пусть R_1 и R_2 – множества X-соотношений.

1) Если R_2 выводится из R_1, то $\langle X \parallel R_1 \cup R_2 \rangle = \langle X \parallel R_1 \rangle$.

2) $R_1 \sim R_2 \Leftrightarrow \langle X \parallel R_1 \rangle = \langle X \parallel R_2 \rangle$.

16.16. Пусть $G = \langle X \rangle$. Тогда существует множество R X-соотношений такое, что $G = \langle X \mid R \rangle$.

16.17. Пусть $G = (X, \cdot)$ – группа. Тогда $G = \langle X \mid R \rangle$, где R – множество всех соотношений вида $xy = z$, где $x, y, z \in X$ и $x \cdot y = z$.

16.18. Пусть $G = \langle X \rangle$ и R – некоторое множество X-соотношений, выполненных в G. Равносильны условия.

(1) $G = \langle X \mid R \rangle$;

(2) каждому элементу g из G можно поставить в соответствие X-слово $w(g)$ так, что

а) g есть значение слова $w(g)$ в G,

б) $w(x^{\varepsilon}) = x^{\varepsilon}$ при $x \in X$ и $\varepsilon = \pm 1$,

в) для любых $g, h \in G$ соотношение $w(g)w(h) = w(gh)$ выводится из R.

16.19. Пусть $R \subseteq \mathcal{R}(X)$.

1) Если $G = \langle X \mid R \rangle$ $(X \subseteq G)$, то $G \simeq \langle X \parallel R \rangle$, а именно отображение

$$\varphi := (\langle X \parallel R \rangle \to G \mid [u]_R \mapsto u_G (u \in \mathcal{W}(X)),$$

где u_G – значение в G слова u в G, есть (правильно определенный) изоморфизм из $\langle X \parallel R \rangle$ на G.

2) Если $G = \langle X \parallel R \rangle$, то $G \simeq \langle X^{\psi} \mid R^{(\psi)} \rangle$, где $\psi := (X \to G \mid x \mapsto [x]_R)$.

16.20. Пусть $G = \langle X \| R \rangle$, где $R \subseteq \mathcal{R}(X)$. Тогда для любого отображения μ из X в произвольную группу H такого, что все соотношения из $R^{(\mu)}$ выполнены в H, существует гомоморфизм γ из G в H такой, что $[x]_R^{\gamma} = x^{\mu}$ для всех $x \in X$ (*свойство R-универсальности* группы $G = \langle X \| R \rangle$).

16.21. Пусть $G = \langle X \mid R \rangle$, где $R \subseteq \mathcal{R}(X)$, и μ – отображение из X в некоторую группу H. Равносильны условия:

(1) μ может быть продолжено до гомоморфизма из G в H;

(2) соотношения из $R^{(\mu)}$ выполнены в H (в этом случае говорят, что "μ сохраняет соотношения из R" или, что "μ согласовано с R"). (*Свойство R-универсальности* группы $G = \langle X \mid R \rangle$.)

16.22. Пусть $G = \langle X \mid R \rangle$ – конечная группа. Если существует взаимно однозначное отображение $\varphi: X \to G$ такое, что $G = \langle X^{\varphi} \rangle$ и соотношения из $R^{(\varphi)}$ выполнены в G, то $G = \langle X^{\varphi} \mid R^{(\varphi)} \rangle$ и φ можно продолжить до автоморфизма группы G.

16.23. Пусть $R \cup \{r\} \subseteq \mathcal{R}(X)$. Равносильны условия:

(1) соотношение r выводится из R;

(2) для любого отображения μ из X в произвольную группу H из того, что соотношения из R^{μ} выполнены в H, следует, что r^{μ} выполнено в H.

16.24. Показать, что соотношение $a^2 = 1$ не является следствием соотношений $a^4 = 1$ и $ab = ba^3$.

16.25. $\langle a, b \| abab^{-1} \rangle$ – неабелево полупрямое произведение двух бесконечных циклических групп.

16.26. Пусть $G = \langle a \rangle \simeq Z_3$ $(a \in G)$.

1) $G = \langle a \mid a^3 = 1 \rangle$.

2) $G \neq \langle a, a^{-1} \mid a^3 = 1 \rangle$.

3) $G = \langle a, a^{-1} \mid a^3 = 1, ((a, 1), (a^{-1}, 1)) = 1 \rangle$. (Последнее соотношение нельзя записать в виде $aa^{-1} = 1$, так как ввиду принятого нами соглашения об условной записи слов в форме (2) оно будет истолковано как тривиальное соотношение $((a, 1), (a, -1)) = 1$.)

16.27. (Теорема Дика) Пусть $G = \langle X \| W \rangle$ и $H = \langle X \| W \cup W_1 \rangle$, где W и W_1 – множества X-слов. Тогда $H \simeq G/N$, где $N = \langle \widetilde{W}_1^G \rangle$ и $\widetilde{W}_1 = \{[w_1]_W \mid w_1 \in W_1\}$.

16.28. Группа $\langle a, b \| a^3 = 1 \rangle$ имеет фактор-группу, изоморфную группе $Z_3 \times \mathbf{Z}^+$.

16.29. Пусть $m, n \in \mathbf{N}$.

1) $\langle a, b \parallel a^m, b^n, a^{-1}b^{-1}ab\rangle \simeq Z_m \times Z_n$.

2) $\langle a, b \parallel a^m, b^n\rangle$ – бесконечная группа, если $mn \neq 1$.

16.30. Если φ – гомоморфизм группы $G = \langle X \mid R\rangle$, то будет ли $G^\varphi = \langle X^\varphi \mid R^{(\varphi)}\rangle$?

16.31. Пусть $W \subseteq \mathcal{W}(X)$ и ψ – отображение X на некоторое множество X^ψ. Тогда $\langle X^\psi \parallel W^{(\psi)}\rangle$ – гомоморфный образ группы $\langle X \parallel W\rangle$.

Если ψ взаимно однозначно, то $\langle X^\psi \parallel W^{(\psi)}\rangle \simeq \langle X \parallel W\rangle$.

16.32. Пусть $R \subseteq \mathcal{R}(X)$ и G – группа. Равносильны условия:

(1) существует отображение ψ из X в G такое, что $G = \langle X^\psi\rangle$ и соотношения из $R^{(\psi)}$ выполнены в G;

(2) G изоморфна фактор-группе группы $\langle X \parallel R\rangle$.

16.33. 1) $Q_8 \simeq \langle a, b \parallel a^{-1}ba = b^{-1}, b^{-1}ab = a^{-1}\rangle \simeq \langle a, b \parallel a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1}\rangle$.

2) Какова группа $\langle a, b \parallel a^4 = b^4 = 1, b^{-1}ab = a^{-1}\rangle$?

16.34. 1) $D_\infty \simeq \langle a, b \parallel a^2, b^2\rangle \simeq \langle c, d \parallel c^2, c^{-1}dcd\rangle$.

2) $D_{2n} \simeq \langle a, b \parallel a^n = 1, b^2 = 1, b^{-1}ab = a^{-1}\rangle$.

16.35. Какова группа $\langle a, b \parallel a^2, b^5, a^{-1}bab^{-2}\rangle$?

16.36. Пусть p – простое число. Какова группа $G = \langle a, b, c \parallel a^p = b^p = c^2 = 1, ab = ba, ca = bc\rangle$?

16.37. $\mathbf{Q}^+ \simeq \langle a_1, a_2, \ldots, a_n, \ldots \parallel a_2^2 = a_1, a_3^3 = a_2, \ldots, a_n^n = a_{n-1}, \ldots\rangle$.

16.38. $\mathbf{Q}(p) \simeq \langle a_1, a_2, \ldots, a_n, \ldots \parallel a_2^p = a_1, \ a_3^p = a_2, \ldots, a_{n+1}^p = a_n, \ldots\rangle$.

16.39. $Z_{p^\infty} \simeq \langle a_1, a_2, \ldots, a_n, \ldots \parallel a_1^p = 1, \ a_2^p = a_1, \ldots, a_{n+1}^p = a_n, \ldots\rangle$.

16.40. Пусть $R \subseteq \mathcal{R}(X)$, $w \in \mathcal{W}(X)$ и $y \notin X$. Тогда $\langle X \cup \{y\} \parallel R \cup \{y = w\}\rangle \simeq \langle X \parallel R\rangle$.

16.41. Пусть $R \subseteq \mathcal{R}(X)$ и из R выводится соотношение $x = u$, где $x \in X$ и $u \in \mathcal{W}(X \setminus \{x\})$. Тогда $\langle X \parallel R\rangle \simeq \langle X \setminus \{x\} \parallel R_1\rangle$, где R_1 получается из R заменой в каждом соотношении из R элемента x словом u.

16.42. Пусть $G = \langle X \mid R\rangle$ и Y – подмножество из X такое, что каждый элемент y из Y является значением в G некоторого слова w_y над $X \setminus Y$. Тогда $G = \langle X \setminus Y \mid R_1\rangle$, где R_1 – множество всех соотношений, получающихся заменой в соотношениях из R каждого элемента y из Y словом w_y.

16.43. $\langle a, b, c \parallel b^2, (bc)^2\rangle \simeq \langle x, y, z \parallel y^2, z^2\rangle$.

16.44. $\langle a, b, c \parallel b^{-1}cb = a, c^{-1}ac = b, a^{-1}ba = c\rangle \simeq \langle a, b \parallel aba = bab\rangle$.

16.45. Какова группа $\langle a, b, c, d \parallel ab = c, bc = d, cd = a, da = b\rangle$?

16.46. 1) $S_3 \simeq \langle a, b \parallel a^3 = 1, b^2 = 1, (ab)^2 = 1\rangle \simeq \langle x, y \parallel x^2, y^2, (xy)^3\rangle \simeq$
$\simeq \langle r, f \parallel f^2, frfr^{-2}\rangle$.

2) $A_4 \simeq \langle a, b \parallel a^3 = 1, b^3 = 1, (ab)^2 = 1\rangle \simeq \langle c, d \parallel c^3 = 1, d^2 = 1,$
$(cd)^3 = 1\rangle$.

3) $S_4 \simeq \langle a, b \parallel a^4 = 1, b^3 = 1, (ab)^2 = 1\rangle$.

4) $A_5 \simeq \langle a, b \parallel a^5 = 1, b^3 = 1, (ab)^2 = 1\rangle$.

16.47. В группе $G = \langle a, b \mid a^{-1}ba = b^2\rangle$ элементы a и b имеют бесконечные порядки.

16.48. Пусть $G = \langle a, b \mid a^m = 1, b^n = 1, bab^{-1} = a^s\rangle$, где $\{m, n, s\} \subseteq \mathbf{N}$. Тогда $o(b) = n$, $o(a) = (m, s^n - 1)$ и $G = \langle a\rangle \lambda \langle b\rangle$.

16.49. Определить порядки групп $G = \langle a, b \parallel a^3 = b^3 = 1, ba = a^2b^2\rangle$ и $H = \langle a, b \parallel a^3 = b^6 = 1, ba = a^2b^2\rangle$.

16.50. 1) Если $a^4 = b^4 = 1$ и $ba = a^2b^2$, то $ab = (ba)^2$ и $(ba)^5 = 1$.

2) $\langle a, b \parallel a^4 = b^4 = 1, ba = a^2b^2\rangle \simeq \langle c, d \parallel c^4 = d^5 = 1, dc = cd^2\rangle$.

Каков порядок групп пункта 2)?

16.51. Доказать, что

$$\langle a, b \parallel a^5 = b^5 = 1,\ ba = a^2b^2\rangle \simeq \langle c, d \parallel c^5 = d^{11} = 1,\ dc = cd^3\rangle,$$

и определить порядок группы.

16.52. 1) В каждом из следующих случаев найти фактор-группу группы G по её подгруппе H (предварительно доказав, что $H \trianglelefteq G$) и определить порядки групп G и H:

а) $G = \langle a, b \mid a^4 = 1, a^2 = (ab)^2 = b^2\rangle$, $H = \langle a^2\rangle$;

б) $G = \langle a, b, c \mid a^{2m} = b^2 = (ab)^2 = c^2 = 1,\ ac = ca,\ bc = cb\rangle$,
$H = \langle a^m, c\rangle$, $(m \in \mathbf{N})$;

в) $G = \langle a, b \mid a^{-1}ba = b^{-1}\rangle$, $H = \langle a^2\rangle$;

г) $G = \langle a, b \mid a^2 = b^2\rangle$, $H = \langle a^2\rangle$.

2) Группы пунктов в) и г) изоморфны.

16.53. Пусть $G = \langle a, b, c, d \mid a^2 = b^2 = c^3 = d^3 = 1, a^{-1}ca = d, ab = ba,$
$cd = dc, b^{-1}cb = c^2, b^{-1}db = d^2\rangle$. Тогда

1) $G = (\langle c\rangle \times \langle d\rangle) \lambda (\langle a\rangle \times \langle b\rangle)$,

2) $\langle c\rangle \times \langle d\rangle$ – минимальная нормальная подгруппа в G.

16.54. Пусть $G = \langle a, b, c \mid a^3 = b^3 = 1, c = b^{-1}a^{-1}ba, ac = ca, bc = cb\rangle$. Тогда $o(a) = o(b) = o(c) = 3$ и $G = (\langle a\rangle \times \langle c\rangle)\lambda \langle b\rangle = (\langle b\rangle \times \langle c\rangle)\ \lambda \langle a\rangle$.

16.55. 1) Если группа G порождается конечным множеством X, то в любом её порождающем множестве имеется конечное подмножество, также порождающее G.

2) Если $G = \langle X \mid R\rangle$, где множество R конечно, то в любом ее определяющем множестве X-соотношений содержится конечное подмножество, также являющееся определяющим множеством X-соотношений группы G.

16.56. В группе $\mathbf{Q}^+$ указать подгруппу, изоморфную группе $G = \langle \{a_n \mid n \in \mathbf{Z}\} \parallel \{a_n = a_{n+1}^2 \mid n \in \mathbf{Z}\}\rangle$. Показать, что

1) $G = \bigcup\limits_{n\in\mathbf{Z}} \langle a_n\rangle$ и $\langle a_n\rangle < \langle a_{n+1}\rangle$ для всех $n \in \mathbf{N}$;

2) отображение φ: $a_{n+1} \mapsto a$ $(n \in \mathbf{Z})$ продолжается (единственным образом) до автоморфизма $\hat{\varphi}$ группы G;

3) в подгруппе $G\lambda \langle\hat{\varphi}\rangle$ из $Hol\,(G)$ подгруппы $\langle a_n\rangle$ $(n \in \mathbf{Z})$ сопряжены между собой.

16.57. Пусть $G = F(\{x, y\})$ и $M = \{x^n\, yx^n \mid n \in \mathbf{Z}, n \geq 0\}$. Тогда $\langle M\rangle = \langle M \parallel \varnothing\rangle$. Следовательно, среди подгрупп свободной группы ранга 2 имеются свободные группы счётного (а значит, и любого конечного) ранга.

§ 17. Конечные p-группы

Всюду в этом параграфе p обозначает простое число, P – конечную p-группу, а m, n – натуральные числа.

Если g – элемент порядка n, то циклическую группу $\langle g \rangle$ будем обозначать также через $\langle g \rangle_n$. Следующие обозначения стандартны.

$cl(P)$ – класс нильпотентности P.

$d(P)$ – минимальное число порождающих (порядок минимального порождающего множества) группы P.

$m(P)$ – ранг P, т.е. наибольшее из натуральных чисел n таких, что P содержит элементарную абелеву подгруппу порядка p^n.

$r_s(P)$ – секционный ранг P, т. е. $max\{m(H/K) \mid K \trianglelefteq H \leq P\}$.

$\Omega_i(P) := \langle g \in P \mid g^{p^i} = 1 \rangle$. Подгруппа $\Omega_1(P)$ называется *нижним слоем* группы P.

$\mho_i(P) = \langle g^{p^i} \mid g \in P \rangle$.

Если a – наибольший из порядков абелевых подгрупп в P, то

$\mathcal{A}(P) := \{A \mid A \leq P, A' = 1, |A| = a\}$,

$J(P) := \langle A \mid A \in \mathcal{A}(P) \rangle$ – *подгруппа Томпсона* группы P.

$SCN(P)$ – множество всех максимальных абелевых нормальных подгрупп из P, или, что то же самое, множество самоцентрализаторных (т.е. совпадающих со своим централизатором в P) нормальных подгрупп из P.

$SCN_k(P) := \{A \in SCN(P) \mid m(A) \geq k\}$.

p-группа P называется:

регулярной, если для любых $x, y \in P$ $(xy)^p = x^p y^p c_1^p \ldots c_m^p$ при некоторых $c_1, \ldots, c_m \in \langle x, y \rangle'$;

специальной, если либо она – элементарная абелева, либо $\Phi(P) = P' = Z(P) \simeq E_{p^n}$ для некоторого $n \in \mathbb{N}$;

экстраспециальной, если она неабелева специальная p-группа, у которой $|Z(P)| = p$;

группой максимального класса, если её порядок есть p^n, где $n \geq 2$, и класс равен $n - 1$.

Пусть $n \geq 3$, $x = e^{2\pi i / p^n}$ и $y = e^{2\pi i / p}$ так, что $Z_{p^n} = \langle x \rangle$ и $Z_p = \langle y \rangle$, и пусть φ – некоторый гомоморфизм из Z_p в $Aut(Z_{p^n})$. Положим

$M_{p^n} := \langle x \rangle \lambda_\varphi \langle y \rangle$, где $\varphi(y): x \mapsto x^{1+p^{n-2}}$ $(n \geq 3)$. Всякая изоморфная M_{p^n} группа H называется *полуабелевой* или *модулярной* группой и, очевидно, имеет вид: $H = \langle a \rangle p^n \lambda \langle b \rangle_p$, где $a^b = a^{1+p^{n-2}}$.

Если $p = 2$ и $n \geq 4$, то:

$SD_{2^n} := \langle x \rangle_{2^n} \lambda_\varphi \langle y \rangle_2$, где $\varphi(y): x \mapsto x^{-1+2^{n-2}}$; всякая изоморфная ей группа называется *полудиэдральной группой* порядка 2^n.

$Q_{2^n} := \langle a, b \| a^{2^{n-1}} = b^4 = 1,\ a^{2^{n-2}} = b^2,\ a^b = a^{-1} \rangle$ $(n \geq 3)$; всякая изоморфная ей группа иазывается *кватернионной группой* (или *обобщённой группой кватернионов*) порядка 2^n.

$E(p) := \langle a, b, c \| a^p = b^p = c^p = 1, a^c = ab, b^c = b \rangle$ $(p > 2)$.

Неабелева группа, все собственные подгруппы которой абелевы, называется *группой Миллера–Морено*, а неабелева группа, все подгруппы которой нормальны в ней, называется *гамильтоновой*.

$A * B$ обозначает центральное произведение 2-групп A и B с объединёнными центральными подгруппами порядка 2 в случае, когда и A и B имеют лишь по одной такой подгруппе (в этом случае $A * B$ определено однозначно по 14.27).

17.1. 1) Всякая конечная p-группа нильпотентна.

2) Если $P \geq N \neq 1$, то $Z(P) \cap N \neq 1$ и $[P, N] < N$.

3) Группы порядков p и p^2 абелевы.

17.2. (T) Пусть P – группа порядка p^n.

1) $\Phi(P) = P' \mho_1(P)$.

2) $P/\Phi(P) \simeq E_{p^d}$ для некоторого $d \in \mathbb{N}$.

3) $d(P) = d$. Более того, подмножество X из P есть минимальное порождающее множество группы P если и только если $X = \{x_1, \ldots, x_d\}$ и $P/\Phi(P) = \langle \overline{x_1} \rangle \times \ldots \times \langle \overline{x_d} \rangle$, где $\overline{x_i} := x_i \Phi(P) \in P/\Phi(P)$.

17.3. 1) Если $H \leq P$, то $\Phi(H) \leq \Phi(P)$.

2) Если P/P' – циклическая группа, то P – циклическая группа.

17.4. Пусть P – 2-группа.

1) $\Phi(P) = \mho_1(P)$.

2) Если $P = AB$, где $A \leq P$ и $B \trianglelefteq P$, то $\Phi(P) = \Phi(A)\Phi(B)[A, B]$.

17.5. Если $N \trianglelefteq P$, то

1) $d(P/N) \leq d(P)$,

2) $d(P/N) = d(P) \Leftrightarrow N \leq \Phi(P)$.

17.6. Пусть $N \trianglelefteq P$. Равносильны условия:

(1) $P \setminus N$ не имеет элементов порядка $\leq p^m$;

(2) $\Omega_m(P) \subseteq N$;

(3) $\Omega_m(P) = \Omega_m(N)$.

17.7. Если $P = \langle x, y \rangle \neq \langle x \rangle$ $(x, y \in P)$, то $\langle x, x^y \rangle < P$.

17.8. Пусть P – неабелева группа порядка p^3.

1) P – экстраспециальная группа.

2) $x^p = xP'$ для любого $x \in P \setminus Z(P)$.

3) Если $p = 2$, то P изоморфна D_8 или Q_8.

4) Если $p > 2$ и $exp\,(P) = p$, то $P \simeq E(p)$ и, следовательно, $P = (\langle a \rangle_p \times \langle z \rangle_p) \lambda \langle b \rangle_p$, где $a^b = az$, $z^b = z$.

5) Если $p > 2$ и $exp(P) > p$, то $P \simeq M_{p^3}$.

6) $M_8 \simeq Q_8$.

7) Для групп пунктов 3)–5) выписать все максимальные подгруппы, все нормальные подгруппы, $\Omega_1(P)$ и $\mho_1(P)$.

17.9. 1) Если $|P| = p^n$, то $cl(P) \leq n - 1$.

2) Если $cl(P) = n - 1$ (т. е. P – группа максимального класса), то $|Z(P)| = p$.

3) Если $|P'| = p^m$, то $cl(P) \leq m + 1$.

17.10. Если $cl(P) = c$ и $exp\,(P/P') = p^m$, то $exp\,(P) \leq p^{mc}$.

17.11. 1) Если P абелева, то $d(P) = m(P) = r_s(P)$.

2) $r_s(P) = max\{d(H) \mid H \leq P\}$.

3) Если $N \lhd P$, то,

а) $d(P) \leq d(P/N) + d(N)$,

б) $m(P) \leq m(P/N) + m(N)$,

в) $r_s(P) \leq r_s(P/N) + r_s(N)$.

17.12. Если $|P/P'| = p^3$ и P' – циклический, то $r_s(P) \leq 3$.

17.13. Пусть $P = \langle a, b \rangle$, где $o(a) = 8$, $b^2 = a^4$ и $a^b = a^{-1}$, т.е. $P \simeq Q_{16}$. Найти:

1) $Z(P)$, P', $\Phi(P)$,

2) порядки элементов и классы сопряжённых элементов в P,

3) все максимальные подгруппы в P,

4) все нормальные подгруппы и все (с точностью до изоморфизма) гомоморфные образы группы P,

5) $cl(P)$, $m(P)$, $r_s(P)$.

17.14. Пусть $P = \langle a \rangle_4 \lambda \langle b \rangle_4$, $b^{-1}ab = a^{-1}$.

1) $P' = \langle a^2 \rangle$.

2) $Z(P) = \Phi(P) = \Omega_1(P) = \langle a^2 \rangle \times \langle b^2 \rangle$.

3) Указать максимальные подгруппы в P.

4) $\langle a^2b^2\rangle$ – единственная максимальная циклическая подгруппа порядка 2 в P и, следовательно, характеристична в P.

5) $P/\langle a^2b^2\rangle \simeq Q_8$.

17.15. Пусть P – группа порядка p^4, порождённая элементами a и b такими, что $o(a) = o(b) = p^2$, и $a^b = a^{1+p}$. Определить:

1) $Z(P)$, P' и $cl(P)$,

2) все максимальные подгруппы и $\Phi(P)$,

3) $\Omega_1(P)$.

17.16. Неабелева метациклическая группа порядка p^4 при $p > 2$ изоморфна либо группе M_{p^4}, либо группе из предыдущей задачи.

17.17. (Т) Группа порядков p^n, обладающая циклической подгруппой индекса p, изоморфна одной из групп: Z_{p^n} $(n \geq 1)$, $Z_{p^{n-1}} \times Z_p$ $(n \geq 2)$, M_{p^n} $(n \geq 3)$, D_{2^n} $(n \geq 3)$, Q_{2^n} $(n \geq 3)$, SD_{2^n} $(n \geq 4)$.

17.18. Для группы $P = \langle a\rangle_{p^{n-1}} \times \langle b\rangle_p$ найти:

а) все максимальные подгруппы и $\Phi(P)$,

б) все нециклические подгруппы,

в) $\Omega_i(P)$ $(1 \leq i \leq n-1)$.

Доказать, что подгруппа $\langle a^{p^{n-2}}\rangle$ характеристична в P.

17.19. Пусть $P \simeq M_{p^n}$, $n \geq 3$ и $p^n \neq 8$, а именно пусть $P = \langle a\rangle_{p^{n-1}} \lambda \langle b\rangle_p$, где $a^b = a^{1+p^{n-2}}$.

1) $P' = \langle a^{p^{n-2}}\rangle \simeq Z_p$.

2) $\Phi(P) = Z(P) = \langle a^p\rangle \simeq Z_{p^{n-2}}$.

3) $cl(P) = 2$.

4) P имеет точно $p + 1$ максимальных подгрупп: $\langle a^p\rangle \times \langle b\rangle$ и $\langle ab^j\rangle$, где $j \in \{0, \ldots, p-1\}$.

5) $\Omega_i(P) = \langle a^{p^{n-1-i}}, b\rangle$ для всех $i \in \{1, \ldots, n-1\}$.

6) Для любого $x \in P \setminus Z(P)$ $C_G(x) = \langle x\rangle Z(P)$ и $x^P = xP'$.

17.20. Пусть P – группа диэдра D_{2^n}, $n \geq 3$, т.е. $P = \langle a\rangle_{2^{n-1}} \lambda \langle b\rangle_2$ и $a^b = a^{-1}$.

1) $Z(P) = \langle a^{2^{n-2}}\rangle$ и $P/Z(P) \simeq D_{2^{n-1}}$.

2) $cl(P) = n - 1$, т. е. P – группа максимального класса.

3) $P' = \Phi(P) = \langle a^2\rangle$.

4) P имеет точно три максимальные подгруппы:

$$\langle a\rangle,\ \langle a^2\rangle \lambda \langle b\rangle \simeq D_{2^{n-1}} \text{ и } \langle a^2\rangle \lambda \langle ab\rangle \simeq D_{2^{n-1}}.$$

5) Все элементы из $P \setminus \langle a \rangle$ имеют порядок 2.

6) Элементы порядка 2 составляют 3 класса сопряжённых элементов с представителями $a^{2^{n-2}}$, b и ab, причём

$(a^{2^{n-2}})^P = \{a^{2^{n-2}}\}$,

$b^P = b\langle a^2 \rangle, C_P(b) = Z(P) \times \langle b \rangle$,

$(ab)^P = ab\langle a^2 \rangle, C_P(ab) = Z(P) \times \langle ab \rangle$.

7) Максимальные подгруппы и подгруппы из $\langle a \rangle$ являются единственными нормальными подгруппами в P.

8) Любые две несопряжённые инволюции, не входящие в $Z(P)$, порождают P.

9) P имеет точно 2 класса сопряжённых четверных подгрупп с представителями $T_0 = Z(P) \times \langle b \rangle$ и $T_1 = Z(P) \times \langle ab \rangle$.

10) Для любой четверной подгруппы T: $C_P(T) = T$ и $N_P(T) = \langle T, a^{2^{n-3}} \rangle \simeq D_8$.

11) Определить $m(P)$ и $r_s(P)$.

17.21. Пусть $P \simeq Q_{2^n}$ $(n \geq 3)$, т. е. $P = \langle a \rangle_{2^{n-1}} \langle b \rangle_4$, $a^{2^{n-2}} = b^2$ и $a^b = a^{-}$ Провести исследование строения группы P по типу задачи 17.20. В частности, показать, что:

P имеет единственную инволюцию;

$P/Z(P) \simeq D_{2^{n-1}}$;

$cl(P) = n - 1$ (т. е. P – группа максимального класса);

P имеет точно три максимальные подгруппы:

$$\langle a \rangle, \langle a^2 \rangle \langle b \rangle \simeq Q_{2^{n-1}}, \langle a^2 \rangle \langle ab \rangle \simeq Q_{2^{n-1}};$$

$P \setminus \langle a \rangle$ состоит из двух классов сопряжённых элементов порядка 4;

$m(P) = 1$, $r_s(P) = 2$.

17.22. Пусть $P \simeq SD_{2^n}$, а именно $P = \langle a \rangle_{2^{n-1}} \langle b \rangle_2$, где $a^b = a^{-1+2^{n-2}}$ $(n \geq 4)$.

1) $Z(P) = \langle a^{2^{n-2}} \rangle_2$ и $P/Z(P) \simeq D_{2^{n-1}}$.

2) $cl(P) = n - 1$ (P – группа максимального класса).

3) $P' = \Phi(P) = \langle a^2 \rangle$ – циклическая группа порядка 2^{n-2}.

4) P имеет точно 3 максимальные подгруппы:

$$\langle a \rangle, \langle a^2 \rangle \lambda \langle b \rangle \simeq D_{2^{n-1}} \text{ и } \langle a^2 \rangle \langle ab \rangle \simeq Q_{2^{n-1}}$$

5) $\Omega_1(P)$ – диэдральная группа порядка 2^{n-1}.

6) $N \lhd P \Leftrightarrow N < P$ или $N \leq P'$.

7) Найти все (с точностью до изоморфизма) гомоморфные образы группы P.

8) $P \setminus \langle a \rangle$ состоит из элементов порядков 2 и 4.

9) Найти централизаторы элементов и классы сопряжённых элементов группы P. Показать, что P имеет 2 класса сопряжённых инволюций и 2 класса сопряжённых элементов порядка 4.

10) P имеет 1 класс четверных подгрупп и 1 класс кватернионных подгрупп порядка 8. Если V – четверная или кватернионная подгруппа в P, то $C_P(V) = Z(V)$ и $|N_P(V): V| = 2$.

11) Если D – диэдральная подгруппа порядка $2^m \geq 8$ из P, то максимальная циклическая подгруппа из D содержится в $\langle a \rangle$.

12) Определить $m(P)$ и $r_s(P)$.

17.23. Определить все конечные p-группы, имеющие только циклические максимальные подгруппы.

17.24. Определить все конечные p-группы, имеющие точно одну нециклическую максимальную подгруппу.

17.25. Пусть P – неабелева p-группа. Если P имеет две абелевы максимальные подгруппы, то P имеет точно $p + 1$ абелеву максимальную подгруппу и $cl(P) = 2$.

17.26. Если P имеет абелеву подгруппу индекса p^2, то P имеет нормальную абелеву подгруппу индекса p^2. (J. L. Alperin)

17.27. Какие из неабелевых групп задачи 17.17 имеют лишь абелевы максимальные подгруппы?

17.28. Следующие условия конечной p-группы P равносильны:

(1) P – неабелева группа, все собственные подгруппы которой абелевы (т. е. P – группа Миллера–Морено);

2) $|G : Z(P)| = p^2$ и $Z(P) = \Phi(P)$;

3) $P = \langle a, b \rangle$ для некоторых $a, b \in P$ и $|P'| = p$.

17.29. Конечная p-группа P является группой Миллера–Морено тогда и только тогда, когда она одного из следующих типов:

а) группа кватернионов Q_8;

б) $\langle a \rangle_{p^{m+1}} \lambda \langle b \rangle_{p^n}$, $a^b = a^{1+p^m}$;

в) $(\langle a \rangle_{p^m} \times \langle z \rangle_p) \lambda \langle b \rangle_{p^n}$, $a^b = az$, $z^b = z$, $n \geq m \geq 1$. (L. Redei, 1947)

17.30. Для групп P Миллера–Морено типов б) и в) из 17.29 найти $Z(P)$, P', $\Phi(P)$, $\Omega_1(P)$ и все максимальные подгруппы в P. В каких случаях $\Omega_1(P) \subseteq Z(P)$?

17.31. Пусть P – конечная p-группа такая, что $C_G(a) = C_G(a^m)$ для любого элемента $a \in P$ и любой его степени $a^m \neq 1$, то P есть или абелева группа, или группа экспоненты p. (Л. С. Казарин)

17.32. Если $P/Z(P)$ имеет циклическую подгруппу индекса p, то $P/Z(P)$ изоморфна E_{p^2} или D_{2^n}.

17.33. Пусть $P/Z(P) \simeq E_4$. Тогда либо P – группа Миллера–Морено, либо $P = Z(P) * T$, где $T \simeq Q_8$ или $T \simeq D_8$. И обратно.

17.34. Пусть P – конечная 2-группа. Тогда для любой инволюции $j \in P \setminus Z(P)$ $C_P(j)$ не является группой максимального класса.

17.35. Не существует конечной группы, все максимальные подгруппы которой кватернионные.

17.36. (Т) Пусть P – группа порядка p^n.

1) Если P имеет лишь одну подгруппу порядка p, то P – циклическая или кватернионная.

2) Если P имеет лишь одну подгруппу порядка p^m, где $1 < m < n$, то P – циклическая.

17.37. Пусть G – конечная группа, $1 < H < G$ и $H \leq \langle g \rangle$ для всех $g \in G \setminus H$. Тогда либо G – циклическая p-группа ($p \geq 2$), либо $G \simeq Q_{2^n}$ и $|H| = 2$.

17.38. (Т) Пусть G – конечная гамильтонова группа (т. е. неабелева группа, все подгруппы которой нормальны в ней). Тогда G – нильпотентная группа чётного порядка, в которой силовские подгруппы нечётных порядков абелевы, а силовская 2-подгруппа изоморфна Q_8 или $Q_8 \times E_{2^m}$ при $m \geq 1$. И обратно.

17.39. 1) Группа M_{p^n} при $p^n \neq 8$ имеет точно один класс ненормальных сопряжённых подгрупп.

2) Определить число классов ненормальных сопряжённых подгрупп в каждой из групп: Q_{16}, $Q_8 \times Z_4$, $Q_8 * Z_4$, D_8 и D_{16}.

17.40. Пусть $P \simeq Z_{2^n} \wr Z_2$ с $n \geq 2$, т. е. $P = (\langle a \rangle_{2^n} \times \langle b \rangle_{2^n}) \lambda \langle c \rangle_2$ и $a^c = b$. Положим, $a_1 = a^{2^{n-1}}$, $b_1 = b^{2^{n-1}}$, $z = a_1 b_1 (= (ab)^{2^{n-1}} = (a^{-1}b)^{2^{n-1}})$.

1) $|P| = 2^{2n+1}$, $exp(P) = 2^{n+1}$.

3) $cl(P) = n + 1$.

4) $P' = \langle a^{-1}b \rangle_{2^n}$, $P / P' \simeq Z_{2^n} \times Z_2$.

5) $\Phi(P) = \langle a^2 \rangle \times \langle ab \rangle = \langle a^2 \rangle \times \langle a^{-1}b \rangle$.

6) P имеет точно три максимальные подгруппы: $M_1 = \langle a \rangle \times \langle b \rangle$, $M_2 = (\langle a^2 \rangle \times \langle ab \rangle) \lambda \langle c \rangle$ и $M_3 = \langle a^2 \rangle \langle ac \rangle$.

7) P имеет точно 3 класса сопряжённых инволюций: $\{z\}$, $\{a_1, b_1\}$ и $c^P = P'c$.

8) $T := \langle a_1 \rangle \times \langle a_2 \rangle \simeq E_4$ и $T \lhd P$.

9) $T_1 := \langle z \rangle \times \langle c \rangle \simeq E_4$ и все четверные подгруппы из P, отличные от T, сопряжены с T_1.

10) Каждый элемент из $P \setminus M_1$ сопряжён в P с элементом из $\langle a \rangle c$, элементы из $\langle a \rangle c$ попарно не сопряжены в P, и $(a^i c)^P = (a^i c)^{\langle a \rangle} = P' a^i c$ $(i \in \mathbf{Z})$. $o(a^i c) = 2o(a^i) = 2^{n+1}/(2^n, i)$.

11) $P \setminus M_1$ имеет точно один класс d^G элементов порядка 4, где $d = a_1 c$.

12) $P'\langle c \rangle \simeq D_{2^{n+1}}$.

13) $Q := P'\langle d \rangle \simeq Q_{2^{n+1}}$, $Q = \langle d^P \rangle \lhd P$ и Q – единственная подгруппа из P, изоморфная $Q_{2^{n+1}}$.

14) $\Omega(P) = TQ$ и $P/\Omega_1(P) \simeq Z_{2^{n-1}}$

15) $P = Q\langle ac \rangle$, $(ac)^2 = ab$.

16) $M_2 = Z(P)Q \simeq Z_{2^n} * Q_{2^{n+1}}$.

17) Если $Q < H < P$, то $H = Z(H)Q$ и $T \leq H$.

18) Если H – неабелева подгруппа из P, то $Z(H) \leq Z(P)$.

19) Если $X \lambda A \leq P$, где X – нециклическая подгруппа из P и A – циклическая подгруппа порядка 2^n из P, то $P = X \lambda A$.

20) $m(P) = 2$ и $r_s(P) = 3$.

17.41. Пусть P – одна из групп $D_8 \times Z_2$, $Q_8 \times Z_2$, и $D_8 * Z_4$. Найти:

а) $|P|$ и $exp\,(P)$,

б) $Z(P)$, P', $\Phi(P)$,

в) все максимальные подгруппы в P,

г) все инволюции и $\Omega_1(P)$,

д) $m(P)$ и $r_s(P)$.

В каких случаях P специальна или экстраспециальна?

17.42. $P \in \{D_8 \times D_8, D_8 \times Q_8, Q_8 \times Q_8\}$. Найти $Z(P)$, P', $\Phi(P)$, максимальные подгруппы и число элементов каждого порядка в P, $\Omega_1(P)$, $d(P)$, $m(P)$ и $r_s(P)$. Сколько подгрупп, изоморфных $E_{2^{m(P)}}$ имеет P.

17.43. Пусть $|P| = 16$ и $m(P) = 3$. Тогда P – группа одного из следующих типов:

1) $P = (\langle a\rangle_2 \times \langle b\rangle_2) \lambda \langle c\rangle_4$, $a^c = b$, $b^c = a$;

2) $P \simeq Z_2 \times D_8$.

В обоих случаях найти $Z(P)$, P', $\Phi(P)$, максимальные подгруппы и $\Omega_1(P)$.

17.44. Если $H = \langle a, b\rangle \leq P (a, b \in P)$ и $[P, H] = H' \simeq Z_p$, то $G = HC_G(H)$. (В. А. Шериев, 1967)

17.45. (Т) **Группа порядка p^n является экстраспециальной группой тогда и только тогда, когда она является центральным произведением с объединёнными центрами нескольких неабелевых групп порядка p^3 (и тогда $n = 2r + 1$, где r – число множителей).**

17.46. 1) $D_8 * Z_4 \simeq Q_8 * Z_4$.

2) $D_8 * D_8 \simeq Q_8 * Q_8$.

17.47. 1) Доказать, что $D_8 * D_8 \not\simeq D_8 * Q_8$, прояснив строение этих групп. А именно, для каждой группы $P \in \{D_8 * D_8, D_8 * Q_8\}$ найти:

а) $|P|$ и $exp(P)$,

б) $Z(P)$, P', $\Phi(P)$,

в) все максимальные подгруппы в P,

г) все инволюции и $\Omega_1(P)$,

д) $m(P)$ и $r_s(P)$.

2) Группа $P = D_8 * D_8$ имеет подгруппы Q и E такие, что $P = Q \lambda E$, $Q \simeq Q_8$ и $E \simeq E_4$.

3) Группа $P = D_8 * D_8$ не имеет факторизации пункта 2). Более того, каждая четверная подгруппа из P содержит $Z(P)$.

17.48. Группа $P = D_8 * D_8 * D_8$ может быть представлена в виде $P = E \lambda V$, где $E \simeq E_{16}$ и $V \simeq E_8$.

17.49. 1) Каждая абелева p-группа регулярна.

2) p-группа класса 2 при $p > 2$ регулярна.

3) Конечная 2-группа регулярна тогда и только тогда, когда она абелева.

17.50. Пусть P – регулярная p-группа. Тогда для любого $n \in \mathbf{N}$ и любых $x_1, \ldots, x_m \in P$

$$(x_1 \ldots x_m)^{p^n} = x_1^{p^n} \ldots x_m^{p^n} t_1^{p^n} \ldots t_k^{p^n}, \quad \text{где} \quad t_i \in \langle x_1, \ldots, x_m\rangle', \ k \in \mathbf{N}.$$

17.51. Пусть $H = \langle x_1, \ldots, x_n\rangle$, $n \geq 1$ и $\bigcap_{i=1}^{n} \langle x_i\rangle \neq 1$. Тогда не существует группы G такой, что $G/Z(G) \simeq H$.

17.52. Если $Z(P)$ и $Z(P/\mho_1(Z(P)))$ – циклические группы, то и группа P циклическая.

17.53. Пусть $P = E \lambda \langle x \rangle$, где $E \simeq E_8$ и $o(x) = 2$. Тогда $|C_P(x)| \geq 4$.

17.54. Пусть $P = E \lambda \langle x \rangle$, где $E \simeq E_{2^n}$ $(n \geq 1)$ и $o(x) = 2$. Тогда

1) $C_E(x) \supseteq [x, E]$,

2) $|C_E(x)| \geq 2^{[\frac{n+1}{2}]}$.

17.55. Граница для $|C_E(x)|$ в предыдущей задаче является точной, т. е. для любого $n \geq 1$ существует группа $P = E \lambda \langle x \rangle$ такая, что $E \simeq E_{2^n}, o(x) = 2$ и $|C_E(x)| = 2^{[\frac{n+1}{2}]}$

17.56. Для конечной p-группы P и натурального числа k равносильны условия:

1) $SCN_k(P) \neq \varnothing$;

2) P – имеет нормальную подгруппу, изоморфную E_{p^k}.

17.57. Если P – 2-группа и $SCN_3(P) \neq \varnothing$ то для любой инволюции t из P будет $SCN_3(C_P(t)) \neq \varnothing$.

17.58. Пусть P имеет нормальную подгруппу, изоморфную E_8 (т. е. $SCN_3(P) \neq \varnothing$). Тогда каждая нормальная подгруппа из P, изоморфная E_4, содержится в некоторой нормальной в P подгруппе, изоморфной E_8.

17.59. 1) Если $J(P) \leq H \leq P$, то $J(H) = J(P)$.

2) $J(P)$ характеристична в любой подгруппе из P, в которой она содержится.

3) Какие из подгрупп $Z(P)$, P', $\Phi(P)$, $\Omega_1(P)$ и $\mho_1(P)$ обладают свойством 2) на месте $J(P)$?

17.60. Пусть $P \in Syl_2(Hol(E_8))$. Тогда:

1) $P = E \lambda D$, где $E \simeq E_8$ и $D \simeq D_8$;

2) $J(P) \simeq E_{16}$.

§ 18. Автоморфизмы p-групп. Действия групп на p-группах

В этом параграфе p есть простое число, P – конечная p-группа и m, n – натуральные числа. Обозначения и термины, связанные с p-группами, объяснены в § 17.

18.1. Пусть H – характеристическая подгруппа группы G.

1) Отображение $\varphi\colon \alpha \mapsto \alpha|_H$ ($\alpha \in Aut(G)$) есть гомоморфизм из $Aut(G)$ в $Aut(H)$ с ядром $Ker(\varphi) = C_{Aut(G)}(H)$. Следовательно,

$$Aut(G)/C_{Aut(G)}(H) \simeq \leq Aut(H).$$

2) Отображение $\psi\colon \alpha\colon \mapsto \hat{\alpha}$ ($\alpha \in Aut(G)$), где $\hat{\alpha}\colon gH \mapsto g^{\alpha}H$ при $g \in G$, есть гомоморфизм $Aut(G) \to Aut(G/H)$ с ядром $Ker(\psi) = C_{Aut(G)}(G/H)$ ($= \{\alpha \in Aut(G) \mid g^{\alpha} \in gH$ для всех $g \in G\}$). Следовательно,

$$Aut(G)/C_{Aut(G)}(H/G) \simeq \leq Aut(G/H).$$

18.2. (Т) Пусть P – группа порядка p^n и $d = d(P)$.

1) Существует гомоморфизм

$$\gamma : Aut(P) \to Aut(P/\Phi(P)) \simeq GL_d(\mathbb{Z}_p),$$

ядро которого есть p-группа. А именно

$$\gamma : \alpha \mapsto \hat{\alpha}(\alpha \in Aut(P)), \text{ где } \hat{\alpha} : g\Phi(P) \mapsto g^{\alpha}\Phi(P),$$

и, следовательно, $Ker\,(\gamma) = C_{Aut(P)}(P/\Phi(P))$.

2) $|C_{Aut(P)}(P/\Phi(P))|$ делит $p^{d(n-d)}$ и

$$|Aut\,(P)| \text{ делит } p^{d(n-d)}(p^d - 1)\,(p^d - p)\ \ldots\ (p^d - p^{d-1}).$$

18.3. (Т) Пусть A – p'-подгруппа из $Aut\,(P)$.

1) $A \simeq \leq Aut(P/\Phi(P))$.

2) $P = [P, A]C_P(A)$ и $[P, A] = [[P, A], A]$.

3) Если P абелева, то $P = [P, A] \times C_P(A)$.

4) Если A централизует некоторый субнормальный ряд группы P, то $A = 1$.

18.4. Пусть $G = \langle a \rangle_{p^n} \lambda \langle b \rangle_m$, где p не делит m. Тогда либо $\langle b \rangle \trianglelefteq G$, либо $C_G(b) = \langle b \rangle$.

18.5. (Т) Если P – абелева группа, A – p'-подгруппа из $Aut(P)$ и A централизует $\Omega_1(P)$, то $A = 1$.

18.6. Пусть $G = P \lambda H$, где $P \in Syl_p(G)$, и $N_G(H) \ll G$. Тогда $P = [P, H] * C_P(H)$, где $*$ – знак внутреннего центральиого произведения (см. § 14), и $H \ll [P, H] \lambda H$.

18.7. Пусть $G = P \lambda (H \lambda \langle t \rangle)$ – конечная группа, где P – p-подгруппа, H – p'-подгруппа и t – инволюция в G. Предположим, что t централизует или инвертирует P. Тогда $[H, t]$ централизует P.

18.8. (Т) Пусть $P = \langle x \rangle \simeq Z_p^n$.

1) $Aut(P)$ – абелева группа порядка $p^{n-1}(p-1)$.

2) Если $p > 2$, то группа $Aut(P)$ циклическая и её силовская p-подгруппа порождена автоморфизмом α, где $x^\alpha = x^{1+p}$.

3) Если $p = 2$ и $n \geq 2$, то $Aut(P) = \langle \alpha \rangle_{2^{n-2}} \times \langle \beta \rangle_2$, где $x^\alpha = x^5$ и $x^\beta = x^{-1}$.

4) Какова группа $C_{Aut(P)}(P/\Phi(P))$?

18.9. $Hol(Z_p^n) \simeq \mathbf{Z}^+_{p^n} \lambda_\varphi \mathbf{Z}^\cdot_{p^n}$, где $x^{\varphi(y)} = xy$ при $x \in \mathbf{Z}^+_{p^n}$ и $y \in \mathbf{Z}^\cdot_{p^n}$.

18.10. Если $G = \langle a \rangle_{169} \lambda \langle b \rangle_{15}$, то $G = (\langle a \rangle \lambda \langle b^5 \rangle) \times \langle b^3 \rangle$.

18.11. Если $P \simeq Z_{2^m} \times Z_{2^n}$ и $m > n$, то $Aut(P)$ – 2-группа.

18.12. Какова группа $Aut(Z_4 \times Z_2)$?

18.13. Пусть $P = \langle a \rangle_{2^m} \times \langle b \rangle_2$ и $m > 2$. Тогда $|Aut(P)| = 2^{m+1}$ и

$$Aut(P) = ((\langle \alpha \rangle_{2^{m-2}} \times \langle \beta \rangle_2) \lambda \langle \gamma \rangle_2) \times \langle \delta \rangle_2,$$

где $(a, b)^\alpha = (a^5, b)$, $(a, b)^\beta = (ab, b)$, $(a, b)^\gamma = (a, a^{2^{m-1}} b)$, $(a, b)^\delta = (a^{-1}, b)$. При этом

$$\alpha^\gamma = \alpha, \ \beta^\gamma = \alpha^{2^{m-3}} \beta \text{ и } \langle \alpha \rangle \times \langle \beta \rangle \times \langle \delta \rangle = C_{Aut(P)}(\Omega_1(P)).$$

18.14. Если $P \simeq \underbrace{Z_{p^m} \times \ldots \times Z_{p^m}}_{\text{и раз}}$, то $Aut(P) \simeq GL_n(Z_{p^m})$ (см. 6.20).

(Прямое произведение нескольких циклических групп равных порядков называется *гомоциклической группой*.)

18.15. Пусть $P = \langle a_1 \rangle_{p^m} \times \ldots \times \langle a_n \rangle_{p^m}$.

1) $P = \langle a_1 x_1 \rangle \times \ldots \times \langle a_n x_n \rangle$ для любых $x_i \in \Phi(P)$.

2) Число последовательностей $(b_1, \ldots, b_n)$ элементов из P таких, что $P = \langle b_1 \rangle \times \ldots \times \langle b_n \rangle$, равно $|GL_n(p)| \cdot |\Phi(P)|^n$.

3) $Aut(P)/C \simeq GL_n(\mathbf{Z}_p)$, где $C := C_{Aut(P)}(P/\Phi(P))$, и $|C| = |\Phi(P)|^n = p^{(m-1)n^2}$.

18.16. Пусть $P = \langle a \rangle_4 \times \langle b \rangle_4$ и $A = Aut(P)$.

1) Отображение φ с $(a, b)^\varphi = (ab, ab^{-1})$ не может быть продолжено до автоморфизма группы P.

2) $|A| = 2^5 \cdot 3$.

3) A имеет силовскую 2-подгруппу

$$T := (\langle \alpha \rangle_2 \times \langle \beta \rangle_2) \lambda (\langle \gamma \rangle_4 \lambda \langle \delta \rangle_2),$$

где $(a, b)^\alpha = (a^{-1}, b)$, $(a, b)^\beta = (a, b^{-1})$, $(a, b)^\gamma = (b, ab^2)$, $(a, b)^\delta = (b, a)$. При этом $\langle \gamma \rangle \lambda \langle \delta \rangle \simeq D_8$, $\alpha^\gamma = \alpha^\delta = \beta$, $\beta^\gamma = \beta^\delta = \alpha$.

4) $O_2(A) = \langle \alpha \rangle \times \langle \beta \rangle \times \langle \gamma^2 \rangle \times \langle \gamma\delta \rangle = C_{Aut(P)}(P/\Phi(P)) = C_{Aut(P)}(\Phi(P))$.

5) $T \simeq E_4 \wr Z_2$.

6) $A = O_2(A) \lambda S$, где $S \simeq S_3$.

18.17. 1) $Aut(D_{2^n})$ – 2-группа при $n \geq 3$, а именно, $Aut(D_{2^n}) \simeq Hol(Z_{2^n})$.

2) $Aut(D_8) \simeq D_8$.

18.18. 1) $Aut(Q_{2^n})$ – 2-группа при $n > 3$,

2) $Aut(Q_8) \simeq S_4$.

18.19. Пусть $P \simeq D_8 \times Z_2$.

1) $|Aut(P)| = 2^6 = 64$.

2) $Out(P) \simeq D_8 \times Z_2$.

3) В $Aut(P)$ имеется подгруппа E, изоморфная E_{16} и содержащая подгруппу $C_{Aut(P)}(P/\Phi(P)) \simeq E_8$.

18.20. Пусть $P \simeq Q_8 \times Z_2$.

1) $|Aut(P)| = 2^6 \cdot 3$.

2) Силовская 2-подгруппа из $Aut(P)$ имеет вид $E \lambda F$, где $E \simeq E_{16}$ и $F \simeq E_4$.

18.21. Пусть $P \simeq M_{p^n}$ (полуабелева группа). Тогда $Aut(P)$ разрешима, а именно $Aut(P)/O_p(Aut(P)) \simeq \leq Z_{p-1} \times Z_{p-1}$.

В частности, $Aut(M_{p^n})$ – 2-группа.

18.22. Пусть $P \simeq E(p)$, т. е. $P = (\langle a \rangle_p \times \langle z \rangle_p) \lambda \langle b \rangle_p$, $p > 2$, $z \in Z(P)$ и $a^b = az$. Тогда $Aut(P) \simeq Hol(E_{p^2})$.

18.23. Пусть $G = E \lambda (\langle x \rangle_n \lambda \langle \tau \rangle_2)$, где $E \simeq E_2{}^m$, и $\langle x \rangle \lambda \langle \tau \rangle \simeq D_{2n}$ с нечётным n. Пусть $\langle x \rangle$ действует регулярно на E (т.е. $E\langle x \rangle$ – группа Фробениуса с ядром E). Тогда $|C_E(\tau)| = |E|^{1/2}$ и все инволюции из $E\langle x \rangle \setminus E$ сопряжены с τ в $E\langle \tau \rangle$.

18.24. Пусть $G = P \lambda A$, $P \in Syl_p(G)$ и $B \leq P$. Если A централизует подгруппы B и $C_P(B)$, то A централизует P.

18.25. ($A \times B$-лемма Томпсона) Пусть $A \times B \leq Aut(P)$, A – p'-группа, B – p-группа. Если A централизует $C_P(B)$, то $A = 1$.

18.26. Пусть P, A, B – подгруппы конечной группы G такие, что $P \trianglelefteq G$, P и B – p-группы, $A = O^p(A)$ и $[A, B] = 1$. Тогда если $[C_p(B), A] = 1$, то $[P, A] = 1$.

18.27. Пусть $B \leq P \trianglelefteq G$, P – p-группа и $C_P(B) \subseteq B$. Тогда $O^p(C_G(B)) \subseteq C_G(P)$.

18.28. Пусть $G = P \lambda R$, где $P \in Syl_p(G)$. Если R централизует $P/Z(P)$ (т. е. $[P, R] \subseteq Z(P)$), то $P = [P, R] \times C_P(R)$.

18.29. Пусть $G = T \lambda S$, где $|S| = 3$ и T изоморфна одной из групп Z_4, E_4, Q_8, D_8. Тогда либо $G = T \times S$, либо $T = [T, S]$.

18.30. $Hol(Q_8) = Q \lambda (E \lambda S)$, где $Q \simeq Q_8$, $E \simeq E_4$, $S \simeq S_3$, $E \lambda S \simeq S_4$ и $Q \lambda E \simeq Q_8 * Q_8$.

18.31. Пусть $G = Q \lambda R$, где $Q \in Syl_2(G)$ и $Q \simeq Q_{2^n}$ ($n \geq 3$). Тогда если $C_R(Q) = 1$ (т.е. R действует точно на Q), то либо $R = 1$, либо $G \simeq SL(2, 3)$.

18.32. Пусть $P \simeq D_8 * D_8$ ($\simeq Q_8 * Q_8$).

1) P имеет точно две подгруппы, изоморфных Q_8.

2) $|Aut(P)| = 2^7 \cdot 3$ и $Aut(P)/Inn(P) \simeq S_3 \wr Z_2$.

3) Пусть B – подгруппа порядка 3 из $Aut(P)$, действующая без неподвижных точек (полурегулярно) на $P/Z(P)$. Тогда любые две инволюции из P, сопряжённые относительно B, перестановочны.

18.33. Пусть $P \simeq D_8 * Q_8$.

1) P не имеет подгруппы, изоморфной E_8.

2) P имеет автоморфизм порядка 5.

3) Существует точно одно нетривиальное расщепляемое расширение P с помощью Z_5.

18.34. Пусть $P = H_1 \times \ldots \times H_n$, где $H_i \simeq D_{2^m}$ ($n, m \in \mathbb{N}$, $m \geq 3$). Пусть $Z(H_i) = \langle z_i \rangle$.

1) Каждый элемент из $Aut(P)$ индуцирует перестановку на множестве $\{z_1, ..., z_n\}$.

2) $\{\alpha \in Aut(P) \mid z_i^\alpha = z_i$ при $i \in \{1, ... n\}\}$ есть 2-подгруппа в $Aut(P)$.

18.35. (Т) Пусть $p > 2$ и A – p'-подгруппа из $Aut(P)$. Если A централизует $\Omega_1(P)$, то $A = 1$.

18.36. В группе $GL_2(\mathbf{Z}_p)$ нет подгрупп, изоморфиых E_8.

18.37. Пусть $G = P \lambda E$, где P – p-группа, $p > 2$, и $E \simeq E_{2^n}$, $n \leq 3$. Если $C_E(P) = 1$, то E нормализует некоторый элемент из $SCN_3(P)$.

18.38. Пусть $p > 2$ и $P = \langle a, b, c \mid\mid a^{p^2} = b^{p^3} = c^{p^4} = 1, b^a = b^{1+p^2}, c^b = c^{1+p^3}, a^c = a^{1+p}\rangle$. Тогда:

1) $P = \langle a\rangle \circ \langle b\rangle \circ \langle c\rangle$ и, следовательно, $|P| = p^9$;

2) $Z(P) = \Phi(P) = \langle a^p\rangle \times \langle b^p\rangle \times \langle c^p\rangle$;

3) $P' = \langle a^p\rangle \times \langle b^{p^2}\rangle \times \langle c^{p^3}\rangle$;

4) $Aut(P)$ – p-группа.

(М. В. Хорошевский)

18.39. (Теорема Гашютца) Пусть P – p-группа, $M \lhd P$ и γ – гомоморфизм P в $Z(M)$ с ядром M.

1) Отображение $\alpha : x \mapsto xx^\gamma$ $(x \in P)$ есть автоморфизм порядка p группы P.

2) Если $Z(M) \subseteq Z(P)$, то α – внешний автоморфизм.

3) Если $|P| > p$, то $p \mid\mid Out(P)|$.

18.40. Из теоремы Машке о матрицах (6.69) вывести следующие утверждения.

1) (Теорема Машке для групп) Пусть $P \simeq E_{p^n}$ и A – p'-подгруппа из $Aut(P)$. Тогда для любой A-допустимой подгруппы P_1 из P в P имеется A-допустимая подгруппа P_2 такая, что $P = P_1 \times P_2$.

2) Пусть $G = P \lambda H$, где $P \simeq E_{p^n}$ и H – p'-группа. Тогда для любой нормальной в G подгруппы P_1 из P в P имеется нормальная в G подгруппа P_2 такая, что $P = P_1 \times P_2$.

18.41. Пусть $G = K \lambda A$ – конечная группа, $(|K|, |A|) = 1$ и пусть $K = L \times M$ – прямое произведение своих подгрупп L и M, причём L A-инвариантна. Тогда $K = L \times M_1$, где M_1 – A-инвариантная подгруппа в K. (В. Д. Мазуров, 1992)

18.42. Пусть G – сверхразрешимая группа и P – нормальная элементарная абелева подгруппа порядка p^n в G. Тогда $G/C_G(P)$

изоморфна подгруппе треугольной группы $T_n(\mathbf{Z}_p)$ (см. § 6). В частности, каждая p'-подгруппа в $G/C_G(P)$ изоморфна подгруппе из $\underbrace{Z_{p-1} \times \ldots \times Z_{p-1}}_{n}$.

18.43. Если $G = P \lambda H$ – сверхразрешимая группа, $P \in Syl_2(G)$ и $C_H(P) = 1$, то подгруппа H абелева.

18.44. Пусть $G = E \lambda D$, где $E \simeq E_{p^2}$, $D \simeq D_{2q}$, p и q – простые нечётные числа и $q \mid p-1$. Предположим, что E не имеет D-инвариантных подгрупп порядка p. Тогда $G = AB$, где A – подгруппа порядка pq и $B \simeq Z_{2p}$.

18.45. Пусть $G = Hol(E_9)$.
1) $G = E \lambda H$, где $E \simeq E_9$ и $H \simeq GL_2(3)$.
2) В G нет элементов порядка 9.
3) G имеет точно три класса сопряжённых элементов порядка 3.
4) G имеет точно два класса сопряжённых элементов порядка 6.

18.46. Определить строение группы $Aut(Z_4 \wr Z_2)$.

18.47. Изучить группу $Aut(D(Z_4 \times Z_4))$.

§ 19. Линейные группы

Первичные понятия и обозначения, связанные с матрицами и линейными группами, введены в § 6.

В данном параграфе F – некоторое поле, q – степень простого числа, $\mathbf{F}_q$ – поле из q элементов, p – простое число и $m, n \in \mathbf{N}$.

Пусть $V \simeq V(n, F)$ – векторное пространство размерности n над полем F и

$GL(V)$ – группа всех обратимых линейных операторов на V. Как отмечалось в § 6, для любой упорядоченной базы B пространства V существует "естественный" изоморфизм i_B из $GL(V)$ на $GL_n(F)$, сопоставляющий оператору его матрицу в базе B. Положим $det(\alpha) = det(i_B(\alpha))$ (определение не зависит от выбора B) и

$SL(V) := \{\alpha \in GL(V) \mid det(\alpha) = 1\}$ (подгруппа в $GL(V)$).

Пусть $Z := Z(GL_n(F))$. Определим группы:

$PGL_n(F) := GL_n(F)/Z$ – *проективная общая линейная группа* степени n над F,

$PSL_n(F) := SL_n(F)\,Z/Z$ $(\simeq SL_n(F)/Z(SL_n(F)))$ – *проективная специальная линейная группа* степени n над F. Подобно определяются группы $PGL(V)$ и $PSL(V)$.

Одномерные подпространства из $V \simeq V(n, F)$ называются *прямыми*, а подпространства размерности $n-1$ – *гиперплоскостями* в V.

В группе $GL_n(F)$ имеются подгруппы $T_n(F)$, $UT_n(F)$ и $Diag_n(F)$ (треугольная, унитреугольная и диагональная подгруппы; см. § 6).

При $F = \mathbf{F}_q$ пишут $GL_n(q)$, $SL_n(q)$, $PGL_n(q)$, $PSL_n(q)$, $T_n(q)$, $UT_n(q)$ и $Diag_n(q)$ вместо $GL_n(F)$, $SL_n(F)$, $PGL_n(F)$, $PSL_n(F)$, $T_n(F)$, $UT_n(F)$ и $Diag_n(F)$ соответственно. Иногда $PSL_n(q)$ обозначают через $L_n(q)$.

Напомним определения некоторых матриц, введённые в § 6:

e_n – единичная $n \times n$-матрица;

o – нулевая матрица ясного из контекста размера;

при фиксированном n:

$t_{ij}(f) := e_n + fe(i, j)$, где $e(i, j)$ – $n \times n$-матрица, в которой на (i, j)-ом месте стоит f, а на остальных местах – нули;

$d_i(f) := e_n + (f - 1)\,e(i, i)$.

В задачах вводятся *аффинные группы* $AGL_n(F)$ (19.47), *симплектические группы* $Sp_{2n}(F)$ (19.41) и *унитарные группы* $U(n)$, $GU_n(q)$ (19.45, 19.46). В 19.1 повторены некоторые задачи из § 6 и § 12.

19.1. (Т) Пусть $n \geq 2$ и F – поле.

1) Если V – векторное пространство размерности n над полем F, то $GL(V) \simeq GL_n(F)$.

2) $GL_n(F) = SL_n(F) \lambda A$, где $A \simeq F^*$.

3) $Z(GL_n(F)) = \{fe_n \mid f \in F^*\} \simeq F^*$.

4) $Z(SL_n(F)) = Z(GL_n(F)) \cap SL_n(F)$.

5) $SL_n(F) = \langle t_{ij}(\alpha) \mid \alpha \in F, i \neq j \rangle$.

6) $GL_n(F) = \langle t_{ij}(\alpha), d_1(\beta) \mid \alpha, \beta \in F, \beta \neq 0, i \neq j \rangle$.

7) $GL_n(F)' = SL_n(F)$, если $|F| > 2$ или $n > 2$.

8) $SL_n(F)' = SL_n(F)$, если $|F| > 3$ или $n > 2$.

19.2. Пусть $G = GL_n(F)$, $D = Diag_n(F)$ и $Mon_n(F)$ – множество всех мономиальневых матриц из G, т. е. матриц, содержащих в каждой строке и каждом столбце точно один иенулевой элемент.

1) $D \simeq \underbrace{F^* \times \ldots \times F^*}_{n}$.

2) $N_G(D) = Mon_n(F) = D \lambda H \simeq F^* \wr S_n$, где $H \simeq S_n$.

19.3. (Т) 1) $|GL_n(q)| = q^{n(n-1)/2}(q^n - 1)(q^{n-1} - 1) \ldots (q - 1)$, $|Z(GL_n(q))| = q - 1$.

2) $|SL_n(q)| = |PGL_n(q)| = |GL_n(q))|/(q - 1)$.

3) $|PSL_n(q)| = |SL_n(q)|/k$, где $k = |Z(SL_n(q))| = (n, q - 1)$.

19.4. Пусть $G = GL_n(q)$, $S = SL_n(q)$ и $P = UT_n(q)$, где q есть степень p.

1) P есть силовская p-подгруппа в G и в S.

2) $N_G(P) = T_n(q) = P \lambda D$, где $D = Diag_n(q) \simeq \underbrace{Z_{q-1} \times \ldots \times Z_{q-1}}_{n}$.

3) $N_S(P) = P \lambda D_1$, где $D_1 = D \cap S \simeq \underbrace{Z_{q-1} \times \ldots \times Z_{q-1}}_{n-1}$.

4) $C_G(P) = Z(P) \times Z(G)$.

19.5. 1) Кольцо $M_n(q)$ имеет подкольцо, изоморфное полю $\mathbf{F}_{q^n}$.

2) Группа $GL_n(q)$ имеет циклическую подгруппу порядка $q^n - 1$. (Всякая такая подгруппа называется *циклом Зингера* в $GL_n(q)$.)

19.6. Пусть $V \simeq V(2, \mathbf{F}_q)$, $q = p^m$, $G = GL(V)$, $S = SL(V)$ и пусть v, $w \in V \setminus \{0\}$. Положим $P(v) := \{g \in G \mid v^g = v\}$.

1) $P(v) \in Syl_p(G)$.

2) $P(v) = P(w) \Leftrightarrow \mathbf{F}_q v = \mathbf{F}_q w$.

3) $Syl_p(G) = \{P(v) \mid v \in V \setminus \{0\}\}$, $|Syl_p(G)| = q + 1$.

4) $N_G(P(v)) = \{g \in G \mid \mathbf{F}_q v^g = \mathbf{F}_q v\} \simeq T_2(q)$.

5) $P(v) \cap P(w) = 1$, если $P(v) \neq P(w)$.

19.7. Пусть $V \simeq V(n, F)$ и L – множество всех прямых (т. е. одномерных подпространств) из V.

1) Для любого $x \in PSL(V)$ отображение σ_x: $Fv \mapsto Fv^x$ $(= Fv^g$ для любого $g \in x)$ есть (правильно определённая) перестановка множества L.

2) Группа $PSL(V)$ действует 2-транзитивно на L (с помощью отображения $x \mapsto \sigma_x$).

3) Если $F = \mathbf{F}_q$, то $|L| = (q^n - 1)/(q - 1)$.

19.8. Пусть $g \in GL(V)$, где $V \simeq V(n, F)$.

1) Если g оставляет на месте каждую прямую из V, то $g \in Z(GL(V))$.

2) Пусть $k \in \{2, \ldots, n-1\}$ и g оставляет на месте все k-мерные подпространства из V. Каков оператор g?

19.9. Оператор t из $GL(V)$ называется *трансвекцией* пространства V, если существует гиперплоскость W в V такая, что $w^t = w$ для всех $w \in W$ и $v^t - v \in W$ для всех $v \in W$ (т.е. t централизует ряд $\{0\} < W^+ < V^+$).

1) Существует упорядоченная база B в V, в которой матрица трансвекции t имеет вид $t_B = t_{n1}(1)$.

2) Все трансвекции группы $GL(V)$ сопряжены в ней.

3) При $n > 2$ все трансвекции группы $GL(V)$ сопряжены в $SL(V)$.

19.10. (Т) 1) Группа $PSL_n(F)$ проста, если она не есть $PSL_2(2)$ или $PSL_2(3)$.

2) Пусть $N \trianglelefteq GL_n(F)$. Если $|F| > 3$ или $n > 2$, то либо $N \leq Z(GL_n(F))$, либо $N \geq SL_n(F)$.

19.11. $GL_2(2) = SL_2(2) \simeq PSL_2(2) \simeq S_3$.

19.12. 1) $GL_2(3) = SL(2, 3) \lambda \langle a \rangle$, где $o(a) = 2$.

2) $SL_2(2) = Q \lambda \langle b \rangle$, где $Q \simeq Q_8$ и $o(b) = 3$.

3) $Z := Z(GL_2(3)) = Z(SL_2(3)) \simeq Z_2$.

4) $PSL_2(3) \simeq A_4$.

5) $PGL_2(3) \simeq S_4$.

6) Пересечение двух различных силовских 2-подгрупп из $GL_2(3)$ равно $O_2(GL_2(3)) = Q$.

7) Силовские 2-подгруппы в $GL_2(3)$ полудиэдральные.

8) $C_{GL_2(3)}(a) = \langle a \rangle \times Z \simeq E_4$ (a – элемент со свойством пункта 1)).

9) $C_{GL_2(3)}(b) = \langle b \rangle \times Z \simeq Z_6$ (b – элемент со свойством пункта 2)).

10) Сколько классов сопряжённых инволюций в группе $GL_2(3)$?

11) $GL_2(3)$ – разрешимая группа 2-длины 2.

19.13. 1) $GL_2(4) = SL_2(4) \times \langle a \rangle$, где $o(a) = 3$.

2) $SL_2(4) \simeq A_5$.

19.14. Группы $GL_2(\mathbf{Z}_4)$ и $GL_2(\mathbf{Z}_2 \oplus \mathbf{Z}_2)$ разрешимы. Указать их порядок, ряд коммутантов, центр и фактор-группу по центру.

19.15. 1) $GL_2(5) = SL_2(5) \lambda \langle a \rangle$, где $o(a) = 4$.
2) $| Z(GL_2(5)) | = 4$, $| Z(SL_2(5)) | = 2$.
3) Каковы подгруппы $UT_2(5)$ и $T_2(5)$?
4) Силовская 2-подгруппа в $SL_2(5)$ изоморфна Q_8.
5) $SL_2(5) = AB$, где $A \simeq SL_2(3)$, $B \simeq Z_5$ и $\langle A, a \rangle = A \lambda \langle a \rangle$.
6) $PSL_2(5) \simeq A_5$.
7) $PGL_2(5) \simeq S_5$.

19.16. Пусть $G = SL_2(5)$.
1) Определить число классов сопряжённых элементов в G. Для каждого класса указать некоторый его представитель (элемент класса) g и найти $C_G(g)$ и $| g^G |$.
2) Определить все классы сопряжённых подгрупп группы G. А именно, для каждого класса указать некоторый его представитель H и найти $N_G(H)$ и мощность класса.
3) Указать все максимальные подгруппы в G.

19.17. Определить строение централизаторов следующих элементов в группе $GL_2(q)$:

$$g_1 = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix} \quad \text{с} \quad a \neq 1,$$

$$g_2 = \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \quad \text{с} \quad a \neq 0.$$

19.18. Пусть $G = GL_2(F)$.
1) Если $g = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix} \in G$, то

$$C_G(g) = \left\{ \begin{pmatrix} x & y \\ ay & x + by \end{pmatrix} \in G \mid x, y \in F \right\} - \text{абелева группа.}$$

2) Централизатор в G любого её нецентрального элемента абелев.

19.19. Пусть $G = GL_2(F)$, где F – поле.
1) Определить все инволюции в G.
2) Подсчитать число инволюций в G в случае, когда $F = \mathbf{F}_q$.

19.20. Если $char(F) \neq 2$, то
1) группа $SL_2(F)$ имеет точно одну инволюцию,
2) группа $GL_2(F)$ не имеет конечных простых неабелевых подгрупп чётного порядка (простых неабелевых групп нечётного порядка не существует по теореме Фейта–Томпсона, см. § 13).

19.21. Пусть $G = SL_2(q)$.

1) $|G| = q(q-1)(q+1)$.

2) G имеет элементарную абелеву подгруппу порядка q и циклические подгруппы порядков $q-1$ и $q+1$.

3) Силовские подгруппы нечётного порядка, отличного от q, в группе G – циклические.

19.22. Пусть $q = p^m$ и $p \neq 2$.

1) Группа $SL_2(q)$ имеет кватернионную силовскую 2-подгруппу.

2) Группа $PSL_2(q)$ имеет диэдральную силовскую 2-подгруппу.

3) Группа $GL_2(q)$ не имеет подгрупп, изоморфных E_8.

19.23. В каждой из групп $G \in \{PGL_2(p^m), PSL_2(p^m)\}$ указать некоторую силовскую p-подгруппу P и её нормализатор $N_G(P)$. Определить число силовских p-подгрупп. Показать, что $C_G(P) = P$.

19.24. Пусть $G = PSL_2(7)$, $P \in Syl_2(G)$, $Q \in Syl_3(G)$ и $R \in Syl_7(G)$.

1) $N_G(Q) \simeq S_3$.

2) $N_G(R)$ – неабелева группа порядка 21.

3) G имеет подгруппу, изоморфную S_4.

4) $N_G(T) = T$.

5) G имеет точно 2 класса сопряжённых четверных подгрупп.

6) G имеет точно 2 класса сопряжённых подгрупп, изоморфных S_4.

7) Описать все максимальные подгруппы в G. Указать их число.

19.25. (Т) Если $q^2 \equiv 1 \pmod 5$, то группа $PSL_2(q)$ имеет подгруппу, изоморфную $PSL_2(5)$.

19.26. $PSL_2(9) \simeq A_6$.

19.27. 1) $|GL_3(q)| = q^3(q^3-1)(q^2-1)(q-1)$.

2) Найти централизатор трансвекции $g = t_{31}(1)$ в группе $GL_3(q)$.

3) Найти $Z(UT_3(q))$.

19.28. Пусть $G = SL_3(3)$ и $\tau = diag(1, -1, -1)$ (инволюция).

1) $C_G(\tau) = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & d & e \end{pmatrix} \middle| a(be-cd) = 1 \right\} \simeq GL_2(3)$.

2) Силовская 3-подгруппа в $SL_3(3)$ неабелева.

19.29. Пусть $G = SL_3(q)$, q – нечётно и $\tau = diag(-1, -1, 1)$ – инволюция в G.

1) $C_G(\tau) \simeq GL_2(q)$.

2) Пусть φ – естественный гомоморфизм G на $G/Z(G)$. Тогда $C_{G^\varphi}(\tau^\varphi) \simeq C_G(\tau)/Z$, где $|Z| = (3, q-1)$.

19.30. Пусть $G = GL_3(q)$ и $H = \langle a \rangle \times \langle b \rangle$, где $a = diag(\alpha, \alpha, 1)$ и $b = diag(1, \beta, \beta)$ с $\{\alpha, \beta\} \subseteq \mathbf{F}_q \setminus \{0, 1\}$. Найти $C_G(H)$ и $C_G(H) \cap SL_3(q)$.

19.31. Пусть $G = GL_3(q)$, где $q = 2^n$, и $g = t_{31}(1)$.

1) $C_G(j) = UT_3(q) \lambda D$, где $D \simeq Z_{q-1} \times Z_{q-1}$.

2) Если $\bar{g}$ – образ g при естественном гомоморфизме $G \to \bar{G}$, где $\bar{G} := G/Z(G) = PGL_3(q)$, то $C_{\bar{G}}(\bar{g}) \simeq C_G(g)/C_G(g) \cap Z(G)$ и $C_{\bar{G}}(\bar{g}) = Q \lambda \langle a \rangle_{q-1}$, где $Q \simeq UT_3(q)$ $(Z(Q) \simeq E_q)$.

19.32. Пусть $G = SL_4(q)$, где $q = 2^m$, и $t = \begin{pmatrix} e_2 & o \\ e_2 & e_2 \end{pmatrix}$.

1) t – инволюция в G.

2) $C_G(t) = A \lambda B$, где $A \simeq E_{q^4}$ и $B \simeq SL_2(q)$.

19.33. Пусть $G = GL_n(q)$, $n = r + s$, $\{r, s\} \subseteq \mathbf{N}$ и

$$A_{r,s} := \left\{ \begin{pmatrix} e_r & o \\ x & e_s \end{pmatrix} \middle| \, x - r \times s \text{-матрица над } \mathbf{F}_q \right\}.$$

Тогда $A_{r,s}$ – элементарная абелева подгруппа порядка q^{rs} в G.

19.34. Пусть $G = SL_n(q)$, q нечётно, и

$$t = diag(\underbrace{-1, \ldots, -1}_{k \text{ раз}}, 1, \ldots, 1) \ (k \text{ чётно}).$$

Тогда $C_G(t)$ есть расширение нормальной подгруппы N, изоморфной $SL_k(q) \times SL_{n-k}(q)$, с помощью Z_{q-1}.

19.35. Найти централизатор C инволюции $t_{n1}(1)$ в группе $G = SL_n(2^m)$. Показать, что $|O_2(C)| = 2^{m(2n-3)}$ и $Z(O_2(C)) \simeq E_{2^m}$. Какова группа $C/O_2(C)$?

19.36. Пусть $G = GL_n(F)$, где F – поле характеристики 2, и t – инволюция из G. Тогда множество всех матриц вида $f(t + e_n) + e_n$, где $f \in F$, есть подгруппа в G. Каково её строение?

19.37. Пусть F – поле характеристики, отличной от 2, и G – подгруппа из $GL_n(F)$, состоящая из всех мономиальневых матриц с вхождениями 0, 1, –1.

1) $G = D \lambda S$, где D – подгруппа из $Diag_n(F)$, изоморфная E_{2^n}, и $S \simeq S_n$.

2) Определить строение подгруппы $\langle D, a\rangle$, где

$$a=\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & & \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix} \quad (a \in S)$$

(a получается из единичной матрицы перестаиовкой первой строки на последнее место).

19.38. Пусть K – коммутативное кольцо с единицей. Для любой матрицы $a \in M_n(K)$ в группе $GL_n(K)$ положим

$$G(a) := \{g \in GL_n(K) \mid gag^{\tau} = a\}.$$

(При необходимости указать кольцо K пишут $G(K, a)$ вместо $G(a)$.) Доказать, что $G(a)$ – подгруппа в $GL_n(K)$.

19.39. Описать подгруппы $A := G(a)$ и $B := G(b)$ группы $GL_2(F)$ (F – поле), где $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ и $b = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ (см. 19.38). Показать, в частности, что

1) $A = SL_2(F)$, если $char(F) = 2$, и $A \simeq D(F^*)$, если $char(F) \neq 2$;

2) $B \simeq F^+$, если $char(F) = 2$, и $B \simeq F^*$, если $char(F) \neq 2$.

19.40. Определить подгруппы $G(a)$ и $G(b)$ в группе $GL_2(F)$, где $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

19.41. Пусть K – коммутативное кольцо с единицей, $n \in \mathbf{N}$ и $a = \begin{pmatrix} 0 & e_n \\ -e_n & 0 \end{pmatrix}$. Подгруппа $G(a)$ группы $GL_{2n}(K)$ (см. 19.38) называется *симплектической группой* степени $2n$ над K и обозначается через $Sp_{2n}(K)$ или через $Sp_{2n}(q)$, если $K = \mathbf{F}_q$.

1) $Sp_2(2) \simeq S_3$.

2) $Sp_2(q) = SL_2(q)$.

3) $Sp_{2n}(K) \simeq \leq Sp_{2(n+1)}(K)$.

19.42. $Sp_4(2) \simeq S_6$.

19.43. Пусть f: $V \times V \to F$ – билинейная форма на $V = V(2n, F)$ такая, что $f(x, y) = \sum_{i=1}^{n}(x_i y_{n+i} - x_{n+i} y_i)$ для $x = (x_1, \ldots, x_{2n})$ и $y = (y_1, \ldots, y_{2n})$. Положим

$$G(f) := \{g \in GL(V) \mid f(x^g, y^g) = f(x, y)\}.$$

1) $G(f)$ – подгруппа в $GL(V)$ (*группа формы* f).

2) $G(f) \simeq Sp_{2n}(F)$.

19.44. На векторном пространстве $V = V(2, F)$ рассмотрим билинейную форму $f(x, y) = x_1y_1 + x_1y_2$ ($x = (x_1, x_2)$ и $y = (y_1, y_2)$ – переменные векторы из V).

1) Из $f(x, y) = 0$ не следует $f(y, x) = 0$.

2) Каково строение группы $G := \{g \in GL(V) \mid f(x^g, y^g) = f(x, y)\}$?

19.45. 1) Подмножество $U(n) := \{g \in GL_n(\mathbf{C}) \mid g^{-1} = \overline{g}^{\mathrm{T}}\}$ группы $GL_n(\mathbf{C})$ ($(\overline{g})_{ij} = \overline{g}_{ij}$) является в ней подгруппой, которая называется *комплексной унитарной группой* степени n).

2) $SU(n) := \{g \in U(n) \mid det(g) = 1\} \trianglelefteq U(n)$ и $U(n)/SU(n) \simeq T$, где T – одномерный тор (1.17).

19.46. Пусть α – автоморфизм поля F и $a \in M_n(F)$. Положим

$$G(a, \alpha) := \{g \in GL_n(F) \mid ga(g^{\alpha})^{\mathrm{T}} = a\}$$

(здесь g^{α} – матрица с $(g^{\alpha})_{ij} = (g_{ij})^{\alpha}$).

1) $G(a, \alpha)$ – подгруппа в $GL_n(F)$.

2) Пусть $F = \mathbf{F}_{q^2}$. Тогда отображение $^- : x \mapsto \bar{x} := x^q$ ($x \in F$) есть автоморфизм поля F и, следовательно,

$$GU_n(q) := \{g \in GL_n(\mathbf{F}_{q^2}) \mid g^{-1} = \overline{g}^{\mathrm{T}}\} = G(e_n, ^-)$$

– подгруппа в $GL_n(\mathbf{F}_{q^2})$ (которая называется *общей унитарной группой* степени n над $\mathbf{F}_q$) (другое её обозначение: $GU(n, q^2)$).

19.47. *Аффинным преобразованием* пространства $V = V(n, F)$ называется отображение вида $\tau_{g,v} : x \mapsto xg + v (x \in V)$, где $g \in GL(V)$ и $v \in V$.

1) Множество $AGL_n(F) := \{\tau_{g,v} \mid g \in GL(V), v \in V\}$ образует подгруппу в S_V (*аффинная группа* пространства V).

2) $AGL_n(F) = T \lambda G$, где $T \simeq V^+$ и $G \simeq GL(V)$.

19.48. 1) Пусть $H := \{(a_{ij}) \in GL_n(F) \mid a_{11} = 1, a_{12} = a_{13} = \ldots = a_{1n} = 0\}$. Тогда $H \leq GL_n(F)$ и $H \simeq AGL_{n-1}(F)$.

2) Найти подгруппу, изоморфную $AGL_{n-1}(F)$, в группе $SL_n(F)$.

19.49. Группу $AGL_n(F)$ при $F = \mathbf{F}_q$ обозначают через $AGL_n(q)$.

1) $AGL(1, 2) \simeq S_2$.

2) $AGL(1, 3) \simeq S_3$.

3) $AGL(1, 4) \simeq A_4$.

4) $AGL(2, 2) \simeq S_4$.

19.50. Пусть $G = GL_n(F)$ и $g \in G$.

1) Если поле F алгебраически замкнуто, то g сопряжена в G с матрицей вида

$$a = \begin{pmatrix} f_1 & & O \\ & \ddots & \\ * & & f_n \end{pmatrix}, \text{ где } f_1, \ldots, f_n \in F,$$

причём $f_i^{o(g)} = 1$ для всех i, если $o(g)$ конечен; в частиости, $G = \bigcup_{g \in G} T^g$, где $T = T_n(F)$ (сравните с 5.26).

2) Если F – любое поле характеристики p, то элемент вида a из 1) является p-элементом если и только если $f_1 = \ldots = f_n = 1$.

19.51. Пусть F – алгебраически замкнутое поле, g – элемент конечного порядка m группы $G = GL_n(F)$ и $char(F)$ не делит m.

1) g сопряжён в G с диагональной матрицей.

2) $\langle g \rangle$ содержит представителей по крайней мере $\left[\frac{\varphi(m)}{n}\right]$ классов сопряжённых элементов порядка m группы G.

19.52. Если a – матрица конечного порядка из $GL_n(\mathbf{R})$, то $det(a) = \pm 1$.

19.53. 1) $PGL_n(\mathbf{C}) = PSL_n(\mathbf{C})$.

2) $PGL_n(\mathbf{R}) \simeq PSL_n(\mathbf{R}) \Leftrightarrow n$ нечётно.

3) При $n > 1$ $PGL_n(\mathbf{Q}) \neq PSL_n(\mathbf{Q})$.

19.54. Пусть $G = \langle a, b \rangle \leq GL_2(\mathbf{C})$, где $a = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 \\ 2 & -1 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 0 \\ 0 & \omega \end{pmatrix}$, $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Тогда G изоморфна центральному произведению $SL_2(3) * Z_4$ с объединёнными подгруппами порядка 2.

19.55. 1) Если g – элемент конечного порядка в $GL_2(\mathbf{Z})$, то $o(g) \in \{1, 2, 3, 4, 6\}$.

2) Для каждого $m \in \{1, 2, 3, 4, 6\}$ указать элемент порядка m в $GL_2(\mathbf{Z})$.

19.56. 1) $SL_2(\mathbf{Z}) = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

2) $GL_2(\mathbf{Z}) = \left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$.

§ 20. π-разрешимые и π-скованные группы. Теорема Шура–Цассенхауза

В этом параграфе буква G обозначает конечную группу, p – простое число, а π – некоторое множество простых чисел за единственным исключением: $\pi(H)$ обозначает множество всех простых делителей порядка конечной группы H;

π' – множество всех простых чисел, не входящих в π;

$O_\pi(G)$ – наибольшая нормальная π-подгруппа из G;

$O_{\pi,\pi'}(G)$ – полный прообраз в G подгруппы $O_{\pi'}(G/O_\pi(G))$;

$O^\pi(G)$ – наибольшая нормальная подгруппа из G, фактор-группа по которой есть π-группа (равносильно: подгруппа, порождённая всеми π'-элементами из G).

Группа G называется:

π-отделимой (соответственно, *π-разрешимой*), если она имеет нормальный ряд, каждый фактор которого есть либо π-группа (соответственно, разрешимая π-группа), либо π'-группа;

π-разложимой, если она является прямым произведением π-группы и π'-группы;

π-скованной, если в группе $\overline{G} := G/O_\pi(G)$ выполнено условие: $C_{\overline{G}}(O_\pi(\overline{G})) \subseteq O_\pi(\overline{G})$.

Для π-отделимой группы G строится *π-ряд*

$$1 = P_0(G) \trianglelefteq M_0(G) \lhd P_1(G) \lhd M_1(G) \lhd \ldots \lhd P_l(G) \trianglelefteq M_l(G) = G$$

следующим образом: $M_i(G)/P_i(G) = O_{\pi'}(G/P_i(G))$ $(i = 0, 1, \ldots, l)$, а $P_i(G)/M_{i-1}(G) = O_\pi(G/M_{i-1}(G))$ $(i = 1, \ldots, l)$. Число l называется *π-длиной* группы G и обозначается через $l_\pi(G)$.

В случае, когда $\pi = \{p\}$, во всех этих терминах ставится p вместо π.

Пусть $H \leq G$. Говорят, что

H есть *подгруппа Картера* группы G, если H нильпотентна и $N_G(H) = H$;

H *абнормальна* в G, если $\langle H, H^g\rangle \ni g$ для любого $g \in G$;

H *пронормальна* в G, если H и H^g сопряжены в $\langle H, H^g\rangle$ для любого $g \in G$;

H есть *TI-подгруппа* в G, если $H \cap H^g = 1$ для всех $g \in G \setminus N_G(H)$.

Отметим, что из теоремы Фейта–Томпсона о разрешимости групп нечётного порядка (см. § 13) вытекает следующий факт:

каждая конечная π-отделимая группа является π-разрешимой или π'-разрешимой.

20.1. (Теорема Шура–Цассенхауза) Пусть G имеет нормальную холлову подгруппу N.

1) В G существует дополнение к N (т. е. $G = N \lambda H$, где $H \leq G$).

2) Если хотя бы одна из групп N и G/N разрешима, то все дополнения к N в G сопряжены в G.

(По теореме Фейта–Томпсона о разрешимости групп нечётного порядка одна из групп N и G/N всегда разрешима.)

20.2. (Т) 1) Конечная π-отделимая группа имеет π-холлову и π'-холлову подгруппы.

2) Если G – конечная π-разрешимая группа, то

а) все π-холловы подгруппы из G сопряжены в G;

б) все π'-холловы подгруппы из G сопряжены в G;

в) каждая π-подгруппа группы G содержится в некоторой π-холловой подгруппе из G;

г) каждая π'-подгруппа группы G содержится в некоторой π'-холловой подгруппе из G.

20.3. Конечная π-отделимая группа имеет $\{p, q\}$-холлову подгруппу при любых $p \in \pi$ и $q \in \pi'$.

20.4. Пусть $N \trianglelefteq G$ и $\pi := \pi(N)$.

1) Любые два π'-элемента из G, лежащие в одном смежном классе по N, сопряжены элементом из N.

2) Число классов сопряжённых π'-элементов в G равно числу классов сопряжённых π'-элементов в G/N.

3) Если x – π'-элемент из G, то $C_{G/N}(xN) = C_G(x)\, N/N$.

20.5. Пусть G – конечная группа, $H \leq G$ и φ – гомоморфизм группы G такой, что $(|H|, |Ker(\varphi)|) = 1$ и хотя бы одна из групп H и $Ker(\varphi)$ разрешима. Тогда

1) $N_{G^\varphi}(H^\varphi) = N_G(H)^\varphi$,

2) $C_{G^\varphi}(H^\varphi) = C_G(H)^\varphi$.

20.6. Пусть A и B – подгруппы группы G такие, что $\langle A, B\rangle = A \lambda B$ и $(|A|, |B|) = 1$. Тогда $C_G(AB/A) = C_G(B)A$.

20.7. (Т) Конечная π-отделимая группа π-скованна. В частности, конечная p-разрешимая группа p-скованна.

20.8. Равносильны условия:

(1) группа G p-скованна,

(2) группа $G/O_{p'}(G)$ p-скованна,

(3) $C_G(S) \subseteq O_{p',p}(G)$ для некоторой p-силовской подгруппы S из $O_{p',p}(G)$,

(4) $C_G(S) \subseteq O_{p',p}(G)$ для каждой p-силовской подгруппы S из $O_{p',p}(G)$.

20.9. Пусть α – какое-либо из следующих свойств группы: π-замкнутость, π-отделимость, π-разрешимость.

1) Свойство α наследуется подгруппами и фактор-группами (т. е. все подгруппы и фактор-группы группы, обладающей свойством α, обладают свойством α).

2) Свойство π-скованности (даже при $\pi = \{p\}$) не наследуется ни подгруппами, ни фактор-группами.

20.10. Пусть $G = H \lambda A$, $(|H|, |A|) = 1$ и хотя бы одна из подгрупп H, A разрешима. Тогда $H = [H, A]C_H(A)$. Если, кроме того, H абелева, то $H = [H, A] \times C_H(A)$.

20.11. (Т) Пусть A – π'-группа автоморфизмов π-группы G и одна из групп A и G разрешима. Пусть $p \in \pi(G)$.

1) G имеет A-инвариантную силовскую p-подгруппу.

2) Любые две A-инвариантные силовские p-подгруппы группы G сопряжены элементом из $C_G(A)$.

3) Каждая A-инвариантная p-подгруппа группы G содержится в некоторой A-инвариантной силовской p-подгруппе группы G.

20.12. Пусть A – π'-группа автоморфизмов π-группы G, причём A или G разрешима. Пусть P – A-инвариантная силовская p-подгруппа из G. Тогда $C_P(A)$ – силовская p-подгруппа в $C_G(A)$.

20.13. Пусть $G = H \lambda A$, $(|H|, |A|) = 1$ и хотя бы одна из подгрупп H и A разрешима.

1) Если A оставляет на месте смежный класс из H по некоторой её A-инвариантной подгруппе, то A оставляет на месте некоторый элемент из этого смежного класса.

2) Если A оставляет неподвижным некоторый класс сопряжённых элементов группы H, то A оставляет на месте некоторый элемент этого класса.

20.14. Если $N \trianglelefteq G$ и G/N разрешима, то в G существует разрешимая подгруппа A такая, что $G = AN$.

20.15. Если $P \in Syl(G)$, то $P \not\subseteq \Phi(G)$ и, значит, $\pi(G/\Phi(G)) = \pi(G)$.

20.16. Обобщить пункт 1) теоремы Шура–Цассенхауза (20.1), доказав следующее утверждение.

Если $N \trianglelefteq G$, то G имеет подгруппу H такую, что

$$G = HN, \ \pi(H) = \pi(G/N) \ \text{ и } \ H \cap N \subseteq \Phi(H)$$

(в частности, $H \cap N$ нильпотентна).

20.17. Пусть $N \trianglelefteq G$ и N содержится в подгруппах A и B из G. Равносильны условия:

(1) $(|A/N|, |B/N|) = 1$;

(2) существуют подгруппы A_1 и B_1 такие, что $A = A_1N$, $B = B_1N$ и $(|A_1|, |B_1|) = 1$.

20.18. 1) Если $G/\Phi(G)$ π-замкнута, то и G π-замкнута.

2) Если $G/\Phi(G)$ π-разложима, то и G π-разложима.

20.19. Пусть $N \trianglelefteq G$ и G/N – π_1-замкнутая π-группа, где $\pi_1 \subseteq \pi$. Тогда существует π_1-замкнутая π-подгруппа K в G такая, что $G = KN$.

20.20. Пусть $N \trianglelefteq G$, N – π-разрешима и H – π-холлова или π'-холлова подгруппа в N.

1) H пронормальна в G.

2) $G = N\,N_G(H)$.

20.21. Если подгруппа H пронормальна в группе G, то $G = \langle H^G \rangle N_G(H)$ и $N_G(H)$ абнормальна в G.

20.22. Для подгруппы A группы G равносильны условия:

(1) A абнормальна в G;

(2) Если $A \le H \le G$, то $N_G(H) = H$ и A не содержится в двух подгруппах, сопряжённых с H.

20.23. Пусть $N \trianglelefteq G$ и $H \le G$.

1) Если $N \le H$, то: H/N абнормальна в $G/N \Leftrightarrow H$ абнормальна в G.

2) Если H абнормальна в HN и HN абнормальна в G, то H абнормальна в G.

20.24. Пусть $N \trianglelefteq G$ и N – p-группа. Если K/N – подгруппа Картера группы G/N, то $K = NK_1$, где K_1 – подгруппа Картера группы G.

20.25. (Т) Пусть G – разрешимая группа.

1) G имеет подгруппу Картера и все её подгруппы Картера сопряжены в ней.

2) Если C – подгруппа Картера группы G, то:

а) C абнормальна в G;

б) если $N \trianglelefteq G$ и G/N нильпотентна, то $G = NC$.

20.26. Для каждой из групп S_4, $GL_2(3)$, D_{2n} и D_∞ найти 2-длину и подгруппы Картера.

20.27. Если H – холлова подгруппа конечной разрешимой группы G, то $G = N_G(H)G'$.

20.28. Пусть G – разрешимая группа, $H < G$ и $|G:H| = p$ – простое число. Тогда $G/H_G \simeq \leq Hol(Z_p)$ (в частности, G/H_G – сверхразрешимая группа).

20.29. В конечной разрешимой неединичной группе G существует истинная нормальная подгруппа, индекс которой не превосходит индекса любой истинной подгруппы из G.

20.30. В конечной разрешимой группе две максимальные подгруппы H и K сопряжены тогда и только тогда, когда $H_G = K_G$.

20.31. Пусть G – конечная разрешимая группа и $N \lhd G$. Тогда G имеет максимальную подгруппу M с $M_G = N$ тогда и только тогда, когда выполнены следующие два условия:

1) G/N имеет единственную минимальную нормальную подгруппу K/N,

2) $K/N = O_p(G/N)$ для некоторого $p \in \pi(G/N)$.

20.32. Пусть G – конечная разрешимая подгруппа и пусть силовская 2-подгруппа в G является обобщённо диэдральной группой. Какова 2-длина G?

20.33. Пусть $G = (T \lambda K) \lambda \langle a \rangle_2$, где T – 2-группа, K – 2′-группа и $t^a = t^{-1}$ для всех $t \in T$. Тогда $G/O(G)$ – 2-замкнута.

20.34. В разрешимой группе G для любой её истинной нормальной подгруппы N произведение $G'N$ – также истинная нормальная подгруппа в G.

20.35. Пусть G – конечная разрешимая группа и $O_2(G)$ – циклическая группа. Тогда либо G – 2-группа, либо $O(G) \neq 1$.

20.36. Пусть G – конечная π-скованная (в частности, π-разрешимая) группа и $O_{\pi'}(G) = 1$. Тогда

$$G/O_\pi(G) \simeq H/O_\pi(H), \quad \text{где} \quad H \leq Aut(O_\pi(G)).$$

20.37. Пусть G – p-скованная группа, $P \in Syl_p(G)$ и P нециклическая. Тогда $P \cap O_{p',p}(G)$ нециклическая.

20.38. Пусть G – конечная p-разрешимая группа и пусть любые две различные силовские p-подгруппы из G порождают группу p-длины 1. Тогда G имеет p-длину 1.

20.39. Пусть G – конечная p-разрешимая группа, у которой каждая бипримарная подгруппа имеет p-длину ≤ 1. Тогда p-длина группы $G \leq 1$.

20.40. Если p-разрешимая группа G имеет абелевы силовские p-подгруппы, то её p-длина ≤ 1.

20.41. 1) Произведение всех π-замкнутых нормальных подгрупп группы G есть $O_{\pi,\pi'}(G)$.

2) Чему равно произведение всех π-разложимых нормальных подгрупп из группы G?

20.42. 1) Если $O_{\pi,\pi'}(G) \leq H \leq G$, то $O_{\pi,\pi'}(G) \leq O_{\pi,\pi'}(H)$.

2) Если $H \trianglelefteq G$, то $O_{\pi,\pi'}(H) \leq O_{\pi,\pi'}(G)$.

20.43. Пусть P – силовская p-подгруппа из $O_{p',p}(G)$. Если подгруппа $H := O_{p',p}(G)C_G(P)$ p-скованна, то и G p-скованна (и $H = O_{p',p}(G)$).

20.44. Пусть $C_G(O_p(G)) \subseteq O_p(G)$ (т. е. группа G p-скованна и $O_{p'}(G) = 1$), $P \in Syl_p(G)$ и A – абелева подгруппа из P, сильно замкнутая в P относительно G (т. е. $A^G \cap P \subseteq A$). Тогда $A \trianglelefteq G$.

20.45. Пусть P – p-подгруппа из G и $P_1 \in Syl_p(PC_G(P))$. Тогда $N_G(P_1)$ – p-скованная группа. Более того, если P_2 – произвольная p-подгруппа из G, содержащая P_1, то $N_G(P_2)$ p-скованна.

20.46. Пусть G – p-скованная группа и P – её p-подгруппа. Тогда $O_{p'}(N_G(P)) \subseteq O_{p'}(G)$.

20.47. 1) Если G – π-отделимая группа и $K := O_\pi(G) \times O_{\pi'}(G)$, то $C_G(K) \subseteq K$.

2) Привести пример π-отделимой группы G, в которой ни одна из подгрупп $C_G(O_\pi(G))$ и $C_G(O_{\pi'}(G))$ не содержится в $O_\pi(G) \times O_{\pi'}(G)$.

20.48. Пусть $N \trianglelefteq G$, $N \subseteq \Phi(G)$ и $O_{\pi'}(G) = 1$, то $O_{\pi'}(G/N) = 1$.

20.49. Если в конечной p-разрешимой группе G p-силовская подгруппа максимальна и неединична, то G бипримарна.

20.50. Пусть группа G π-разрешима и некоторая её максимальная подгруппа является π-группой. Тогда G разрешима.

20.51. Если конечная группа G π-разрешима и её π-холлова подгруппа H является прямым множителем некоторой максимальной подгруппы M группы G, то либо G π'-замкнута, либо $M = H \times O_{\pi'}(G)$ и индекс $|G : M|$ примарен.

20.52. Следующие условия конечной группы G равносильны:

(1) каждая максимальная подгруппа группы G содержит одну из подгрупп $O^{\pi}(G)$ и $O^{\pi'}(G)$;

(2) $G = O_{\pi}(G) \times O_{\pi'}(G)$.

20.53. Пусть $G = P \lambda H$, где $P \in Syl(G)$.

1) $\Phi(G) = \Phi(P) \times (\Phi(H) \cap H_G)$. В частности, $\Phi(P) = \Phi(G) \cap P$;

2) Если $H \leq M < G$, то $M \trianglelefteq G \Leftrightarrow N_G(H) \subseteq M$;

3) $\bigcap\limits_{M}\{M \mid H \leq M < G,\ M \trianglelefteq G\} = \Phi(P)N_G(H)$.

20.54. Пусть группа G имеет подгруппы A и B такие, что $G = ABA$, и пусть $p \in \pi(A)\setminus\pi(B)$. Если G p-разрешима, то $Syl_p(A) \subseteq Syl_p(G)$.

20.55. Пусть H – TI-подгруппа конечной группы G, $N \trianglelefteq G$, $(|H|, |N|) = 1$ и H или N разрешима. Тогда HN/N – TI-подгруппа в G/N.

20.56. Пусть $G = AB$, где $A \leq G$ и $B \trianglelefteq G$. Тогда для любого $a \in A$ такого, что $(o(a), |B|) = 1$, $C_G(a) = C_A(a)C_B(a)$.

20.57. Пусть G – конечная π-разрешимая или π'-разрешимая группа и H – её ненормальная π-холлова TI-подгруппа. Тогда в G имеется секция, являющаяся группой Фробениуса с дополнительным множителем, изоморфным H.

§ 21. Перенос и нормальные p-дополнения. Слияние p-элементов

Рассмотрим разложение группы G по подгруппе H конечного индекса n:

$$G = Hy_1 \dot{\cup} Hy_2 \dot{\cup} \ldots \dot{\cup} Hy_n. \qquad (1)$$

Каждый элемент x группы G можно тогда записать в виде $x = hy_i$, где $h \in H$, и элементы h и y_i определяются элементом x однозначно. Элемент h ("H-часть элемента x") обозначим через $\eta(x)$. Пусть K – некоторая подгруппа из H, содержащая коммутант H. Отображение из G в абелеву группу G/K, заданное формулой

$$g \mapsto K \prod_{i=1}^{n} \eta(x_i g) \quad (g \in G),$$

называется *переносом* G *в* H/K и обозначается через $V_{G \to H/K}$, а при $K = H'$ – просто через $V_{G \to H}$.

Обозначение вида $V_{X \to Y/Z}$ всегда предполагает, что X – группа, Y – её подгруппа конечного индекса и $Y' \le Z \le Y$.

Пусть $A \subseteq P \le G$. Говорят, что

A слабо замкнуто в P относительно G, если при любом $g \in G$ из $A^g \subseteq P$ следует, что $A^g = A$; и

A сильно замкнуто в P относительно G, если $A^G \cap P \subseteq A$. Эти понятия используются, главным образом, в случае, когда P – силовская подгруппа конечной группы G.

Если $x \in P \in Syl_p(G)$, где G – конечная группа, то элемент x называется *экстремальным* в P (относительно G), если $|C_P(x)| = |C_G(x)|_p$ (т. е. если $C_P(x) \in Syl_p(C_G(x))$).

Конечная группа называется:

p-нильпотентной, если она p'-замкнута (т. е. имеет нормальное p-дополнение);

p-нормальной, если центр любой её силовской p-подгруппы является центром любой другой силовской p-подгруппы, его содержащей;

группой Шмидта; если она не нильпотентна, но все её истинные подгруппы нильпотентны.

В этом параграфе:

p – простое число,

$Cl(X)$ – множество всех классов сопряжённых элементов группы X,

G – конечная группа в тех задачах, в которых встречается выражение "$Syl_p(G)$".

21.1. (Т) Пусть H – подгруппа конечного индекса группы G и $H' \le K \le H$.

1) Отображение $V_{G\to H/K}$, определённое во введении, не зависит от выбора представителей y_i смежных классов в (1).

2) $V_{G\to H/K}$ есть гомоморфизм из G в H/K.

21.2. (Т) Пусть H – подгруппа конечного индекса группы G и $g \in G$.

1) Существуют элементы $x_1, \dots, x_t$ в G такие, что

а) $G = \dot{\bigcup}_{i=1}^{t} (Hx_i \cup Hx_ig \cup \dots \cup Hx_ig^{n_i-1})$;

б) $n_i = o(x_ig x_i^{-1};\ H)$ (т. е. $x_ig^{n_i}x_i^{-1}$ – наименьшая натуральная степень элемента $x_ig x_i^{-1}$, входящая в H);

в) $n_1 + \dots + n_t = |G : H|$.

(В частности, при любом i множество $\{Hx_i,\ Hx_ig, \dots, Hx_ig^{n_i-1}\}$ есть орбита элемента g при его действии умножениями справа на множестве $G : H$ правых смежных классов по H. Назовём его *g-орбитой* на $G : H$. t – число g-орбит.)

2) Если $x_1, \dots, x_t$ – элементы со свойством пункта 1) и $H' \le K \le H$, то

$$V_{G\to H/K}(g) = K \prod_{i=1}^{t} x_ig^{n_i}x_i^{-1}.$$

21.3. Пусть H – холлова подгруппа конечной группы G. Через $F_G(H)$ обозначим подгруппу, порождённую всеми коммутаторами вида $[h, g]$, где $h \in H$ и $g \in G$, содержащимися в H.

1) Если $V = V_{G\to H/K}(H)$ $(H' \le K \le H)$, то

$$G = Ker(V)H \quad \text{и} \quad V(G) = V(H).$$

2) $Ker(V_{G\to H}) \cap H = G' \cap H = F_G(H)$.

3) $Ker(V_{G\to H}) = \cap\{K \trianglelefteq H \mid G/K$ – абелева $\pi(H)$-группа$\}$.

21.4. Пусть G – конечная группа, $P \in Syl_2(G)$ и $M \lessdot P$. Тогда

а) либо каждая инволюция из P сопряжена с некоторой инволюцией из M,

б) либо G имеет нормальную подгруппу индекса 2.

21.5. Пусть $P \in Syl_p(G)$, $P = B \lambda \langle a\rangle$ $(B \le G,\ a \in G)$ и $a^G \cap P \subseteq Ba$. Тогда в G существует нормальное дополнение N к $\langle a\rangle$: $G = N \lambda \langle a\rangle$.

21.6. Ядро переноса $V_{G\to H/K}$ всегда содержит H', но не всегда содержит K.

21.7. Пусть $P \in Syl_p(G)$ и A, B – нормальные подмножества из P, сопряжённые в группе G. Тогда A и B сопряжены в $N_G(P)$.

21.8. (Теорема Бернсайда о нормальном p-дополнении) Если силовская подгруппа P конечной группы G лежит в центре $N_G(P)$, то G имеет нормальную подгруппу N такую, что $G = N \lambda H$.

21.9. Группа порядка $2^3 \cdot p^2$ при любом простом $p > 3$ имеет нормальную силовскую подгруппу.

21.10. Доказать следующее обобщение теоремы Бернсайда. Если холлова подгруппа H конечной группы G входит в центр $N_G(H)$, то G имеет нормальную подгруппу N такую, что $G = N \lambda H$.

21.11. Пусть $P \in Syl_2(G)$. Тогда группа G имеет нормальное 2-дополнение в каждом из следующих случаев:

1) P – циклическая группа,

2) $P \simeq Z_{2^m} \times Z_2$, где $m > 1$.

21.12. Если $P = \langle a \rangle \in Syl_p(G)$ $(a \in P)$ и $(p - 1, |N_G(P)|) = 1$, то G имеет нормальное p-дополнение.

21.13. Если все силовские подгруппы конечной группы G циклические, то G разрешима, причём $F(G)$ и $G/F(G)$ циклические.

21.14. Пусть $P \in Syl_p(G)$, P абелева и $P \cap Z(N_G(P)) \neq 1$, то G имеет нормальную подгруппу индекса p.

21.15. Если конечная группа G имеет абелеву силовскую p-подгруппу типа $(n_1, n_2, \ldots, n_k)$, где $n_1 > n_2 \geq \ldots \geq n_k$ $(k \geq 2)$, и если $(p - 1, |N_G(P)|) = 1$, то G имеет нормальную подгруппу индекса p.

21.16. Пусть $P \in Syl_p(G)$, P – абелева и $\langle a \rangle$ – неединичная характеристическая подгруппа в P такая, что a не сопряжён в G ни с какой своей степенью, отличной от a. Тогда в G существует нормальная подгруппа индекса p. Если при этом P циклическая, то G имеет нормальное p-дополнение.

21.17. Пусть H – подгруппа конечной группы G такая, что $H \cap H^g = 1$ для всех $g \in G \setminus H$. Пусть $V := V_{G \to H}$.

1) H – холлова подгруппа в G.

2) $V(h) = H'h$ для всех $h \in H$ и, следовательно, $G = Ker(V)H$ и $Ker(V) \cap H = H'$.

3) Если H разрешима, то G имеет нормальную подгруппу N такую, что $G = N \lambda H$. (Частный случай теоремы Фробениуса из § 22.)

21.18. Пусть H – разрешимая холлова подгруппа конечной группы G. Если H взаимно проста со своими сопряжёнными, отличными от неё, и является прямым множителем в своём нормализаторе, то G имеет нормальную подгруппу N такую, что $G = N \lambda H$.

21.19. Пусть G – конечная группа, имеющая абелеву максимальную подгруппу A.

1) В G существует нормальная подгруппа N такая, что

$$G = AN \quad \text{и} \quad A \cap N = A_G.$$

2) G разрешима.

21.20. Пусть G – конечная группа с абелевой силовской p-подгруппой P, где $p > 2$, и $K \trianglelefteq G$. Если $\Omega_1(P) \le P \cap K \le \Phi(P)$, то G p-разрешима.

21.21. Пусть G – конечная группа с циклической силовской p-подгруппой. Тогда если G имеет нормальную подгруппу K такую, что p делит $|K|$ и $|G/K|$, то G p-разрешима.

21.22. (Т) Пусть $P \in Syl_p(G)$.

1) (1-я теорема Грюна)

$$P \cap Ker(V_{G \to P}) = P \cap G' = \langle P \cap N_G(P)',\ P \cap (P^g)' \mid g \in G \rangle.$$

2) (2-я теорема Грюна) Если конечная группа G p-нормальна, то наибольшие p-фактор-группы групп G и $N_G(Z(P))$ изоморфны.

21.23. Пусть $P \in Syl_2(G)$ и $P \simeq M_{2^m}$, $m \ge 4$ (т. е. $P = \langle a \rangle_{2^{m-1}} \lambda \langle b \rangle_2$, где $b^{-1}ab = a^{1+2^{m-2}}$). Тогда группа G имеет нормальное 2-дополнение.

21.24. Пусть $P \in Syl_p(G)$, P абелева и $N := N_G(P)$.

1) $P \cap G' = P \cap N'$ и $P = (P \cap N') \times (P \cap Z(N))$.

2) Наибольшая p-фактор-группа группы G изоморфна $P \cap Z(N)$.

21.25. Пусть P – неединичная p-подгруппа конечной группы G. Если $P \in Syl_p(G)$, то равносильны условия:

(1) $N_G(P)/C_G(P)$ – p-группа,

(2) $N_G(P)$ p-нильпотентна.

Сохранится ли равносильность этих условий, если P не является силовской подгруппой?

21.26. (Теорема Фробениуса о нормальном p-дополнении) Пусть $P \in Syl_p(G)$. Равносильны условия:

(1) для любой подгруппы A из P $N_G(A)/C_G(A)$ есть p-группа,

(2) для любой неединичной подгруппы A из P $N_G(A)$ p-нильпотентна,

(3) G p-нильпотентна.

21.27. Пусть G – группа Шмидта.

1) G p-нильпотентна для некоторого $p \in \pi(G)$.

2) G имеет примарное нормальное p-дополнение и, следовательно, $G = P \lambda Q$, где $|P| = p^{\alpha}$, $|Q| = q^{\beta}$, p, q – различные простые числа, $\alpha, \beta \in \mathbb{N}$.

3) $P = \langle a \rangle$ – циклическая группа.

21.28. Конечная группа, все максимальные подгруппы которой p-нильпотентны, либо сама p-нильпотентна, либо является группой Шмидта.

21.29. Конечная группа, все максимальные подгруппы которой p-разложимы, либо сама p-разложима, либо является группой Шмидта.

21.30. Пусть G – конечная группа, имеющая нильпотентную π-холлову подгруппу H. Тогда каждая π-подгруппа группы G содержится в некоторой подгруппе, сопряжённой с H. (H. Wielandt, 1954)

21.31. Если силовская p-подгруппа конечной группы G содержится в нормальной подгруппе N группы G такой, что все максимальные подгруппы группы G, не содержащие N, p-нильпотентны, то группа $G/O_p(G)$ p-нильпотентна.

21.32. (Теорема Томпсона о нормальном p-дополнении) Пусть $P \in Syl_p(G)$, где $p > 2$. Равносильны условия:

(1) для любой характеристической подгруппы A в P $N_G(A)/C_G(A)$ есть p-группа;

(2) для любой неединичной характеристической подгруппы A из P $N_G(A)$ p-нильпотентна;

(3) группа G p-нильпотентна.

21.33. Пусть p – нечётное простое число и G – конечная группа. Если в G любая максимальная подгруппа p-нильпотентна или нормальна в G, то G – p-разрешимая группа p-длины ≤ 2.

21.34. Пусть G имеет минимальную нормальную подгруппу N такую, что $N \not\subseteq \Phi(G)$ и все максимальные подгруппы из G, не содержащие N, p-нильпотентны. Предположим, что либо $p > 2$, либо $p = 2$ и силовские 2-подгруппы из N дедекиндовы. Тогда N нильпотентна и G – p-разрешимая группа p-длины ≤ 2.

21.35. Пусть $K \trianglelefteq H \leq G$ и V – перенос G в H/K. Пусть $g \in G$ и

$$G = \dot{\bigcup_{i=1}^{k}} Hy_i C_G(g)$$

($y_i \in G, k \in \mathbb{N}$). Тогда

$$V(g) = K \prod_{i=1}^{k} y_i g^{m_i} y_i^{-1}, \quad \text{где} \quad m_i = |C_G(g) : C_G(g) \cap H^{y_i}|.$$

21.36. Пусть $H' \leq K \leq H \leq G$ и $g \in G$. Пусть $X = \{x_1, \ldots, x_t\}$ – множество элементов $x_i \in G$ со свойством 1) задачи 21.2. Для $x \in X$ положим $x[g] := xg^{n_x}x^{-1}$, где $n_x = o(xgx^{-1}; H)$, и для $C \in Cl(H)$

$$X_C := \{x \in X \mid x[g] \in C\},$$

$$con(C) := K \prod_{x \in X_C} x[g] \quad (con(C) = K \quad \text{при} \quad X_C = \varnothing).$$

Тогда по пункту 2) задачи 21.2

$$V_{G \to H/K(g)} = K \prod_{x \in X} x[g] = \prod_{C \in Cl(H)} con(C).$$

Пусть $C = a^H \in Cl(H)$ $(a \in H)$.

1) $con(C) = Ka^{|X_C|}$.

2) Если $o(g)$ конечен, то для любого $x \in X_C$:

а) $n_x = q := \dfrac{o(g)}{o(a)}$;

б) $X_C = X \cap HxC_G(g^q)$;

в) $HxC_G(g^q)$ есть объединенне некоторого числа r g-орбит на $G : H$, каждая из которых имеет мощность q;

г) $|X_C| = r = \dfrac{|C_G(a)|}{|C_H(a)|q}$.

(Schiefelbusch, 1975)

21.37. Если $P \in Syl_p(G)$, то каждый элемент из P сопряжён в G с некоторым экстремальным элементом из P (т. е. с элементом b таким, что $C_P(b) \in Syl_p(C_G(b))$).

21.38. Пусть $P \in Syl_p(G)$, $P' \leq K \leq P$ и V – перенос G в P/K. Пусть a – элемент порядка p из $P \setminus K$ и $a^G \cap P = a_1^P \dot{\cup} \ldots \dot{\cup} a_k^P$. Пусть $a_1, \ldots, a_r$ – все экстремальные элементы среди $a_1, \ldots, a_k$. Тогда

$$V(a) = K \prod_{i=1}^{r}{}' a_i^m, \quad \text{где} \quad m = |C_G(a)|_{p'}.$$

(D. Goldschmidt)

21.39. Пусть $P \in Syl_p(G)$, $P' \leq K \leq P$ и a – элемент порядка p из $P \setminus K$. Предположим, что $a^G \cup K$ содержит все элементы b порядка p из P такие, что $C_p(b) \simeq C_p(a)$. Тогда G имеет нормальную подгруппу индекса p.

21.40. Если $A \subseteq B \leq G$, то подгруппа $\langle A^G \cap B \rangle$ слабо замкнута в B относительно G.

21.41. Пусть $A \subseteq B \leq G$ и $H \leq G$.

1) Если A сильно замкнуто в B относительно G, то $A \cap H$ сильно замкнуто в $B \cap H$ относительно H.

2) Привести пример, в котором A слабо замкнуто в B относительно G, но $A \cap H$ не является слабо замкнутым в $B \cap H$ относительно H.

21.42. Пусть $A \subseteq B \leq G$.

1) Если A слабо замкнуто в B относительно G, то $\langle A \rangle$ слабо замкнута в B относительно G.

2) Привести пример, в котором A сильно замкнуто в B относительно G, но $\langle A \rangle$ не является сильно замкнутой в B относительно G.

21.43. Пусть G – конечная группа, $P_1 \leq P \in Syl_p(G)$ и A – характеристическая подгруппа в P_1. Если любые два элемента из P сопряжены элементом из $N_G(P_1)$ (в этом случае говорят, что $N_G(P_1)$ *контролирует слияние элементов в* P), то A сильно замкнута в P относительно G.

21.44. Пусть $P \in Syl_p(G)$ и A – слабо замкнутая подгруппа в P относительно G.

1) A слабо замкнута в любой силовской p-подгруппе из G, в которой она содержится.

2) Любые два A-инвариантных подмножества из P сопряжены в $N_G(A)$.

3) Если $A \subseteq Z(P)$, то A сильно замкнута в P относительно G.

21.45. Пусть G – конечная группа, $x \in P \in Syl_p(G)$ и пусть x лежит в центре любой силовской p-подгруппы из G, в которой он содержится. Тогда $\langle x^G \cap P \rangle$ сильно замкнута в P относительно G.

§ 22. Представления и характеры конечных групп

Всюду в этом параграфе G – конечная группа, F – поле и p – простое число.

Представлением **группы G над полем F называется гомоморфизм этой группы в группу $GL_n(F)$ или в группу $GL(V)$, где V – векторное пространство размерности n над F, $n \geq 1$. Число n называется *степенью* этого представления и обозначается через $deg(\mathcal{A})$. Представления в группу $GL_n(F)$ называются *матричными*, а представления в $GL(V)$ – *операторными*. Представления обозначаются далее рукописными прописными буквами латинского алфавита. Представление $\mathcal{A}$ называется *точным*, если его ядро $Ker(\mathcal{A})$ – единичная подгруппа.**

Пусть $V \simeq V(n, F)$ и i_B – естественный изоморфизм $GL(V)$ на $GL_n(F)$, определённый в §6 (B – упорядоченная база в V и $i_B : a \mapsto a_B$, где a_B – матрица оператора a в базе B). Если $\mathcal{A}$ – операторное представление $G \to GL(V)$, то композиция $\mathcal{M} = \mathcal{A} i_B$ есть матричное представление $G \to GL_n(F)$ ($\mathcal{M}(g) = \mathcal{A}(g)_B$ для всех $g \in G$). Оно называется *матричной интерпретацией* представления $\mathcal{A}$, а $\mathcal{A}$ $(= \mathcal{M} i_B^{-1})$ – *операторной интерпретацией* представления $\mathcal{M}$. Прилагательные "матричная" и "операторная" здесь могут быть опущены.

Представления $\mathcal{A}$ и $\mathcal{B}$ группы G над полем F называются *эквивалентными* (запись: $\mathcal{A} \approx \mathcal{B}$), если либо $\mathcal{A}$ есть интерпретация (матричная или операторная) представления $\mathcal{B}$, либо $\mathcal{A}$ и $\mathcal{B}$ – интерпретации одного представления. Все представления G над F разбиваются на непересекающиеся *классы эквивалентных представлений* (22.3).

Прилагательные, относящиеся к представлениям, – неприводимое, разложимое, регулярное, индуцированное и некоторые другие – определяются ниже лишь для матричных или лишь для операторных представлений; считается, что они относятся и к их интерпретациям.

Представление $\mathcal{A} : G \to GL(V)$ называется *приводимым*, если V имеет собственное (т. е. отличное от $\{0\}$ и V) $\mathcal{A}(G)$-инвариантное подпространство, и *разложимым*, если $V = V_1 \oplus V_2$, где V_1 и V_2 – собственные $\mathcal{A}(G)$-инвариантные подпространства в V. Если U и V – $\mathcal{A}(G)$-инвариантные подпространства в V и $U \supset W$, то можно определить *фактор* $\mathcal{A}_{U/W} : G \to GL(U/W)$ представления $\mathcal{A}$, положив

$\mathcal{A}_{U/W}(g) : u + W \mapsto u^{\mathcal{A}(g)} + W$ ($g \in G$, $u \in U$) (см. 22.9). Разложимое представление является *прямой суммой* некоторых представлений меньшей степени; см. определение в задаче 22.6. Конструкция *тензорного произведения* двух представлений приводится в 22.7.

Характером представления $\mathcal{A}$ группы G над полем F называется функция $\chi_{\mathcal{A}}$ из G в F с $\chi_{\mathcal{A}}(g) = \text{след}(\mathcal{A}(g))$ при $g \in G$. ($\chi_{\mathcal{A}}(g) = \chi_{\mathcal{M}}(g) = \sum_{i=1}^{deg\mathcal{M}} \mathcal{M}(g)_{ii}$ для любой матричной интерпретации $\mathcal{M}$ представления $\mathcal{A}$.)

Единичное представление G над F есть представление группы G в $GL(1, F)$ или в $GL(V)$, где $V \simeq V(1, F)$, при котором каждому $g \in G$ ставится в соответствие единичная матрица или, соответственно, единичный оператор.

Пусть FG – групповая алгебра группы G над полем F (см. §6).

$Z(FG) := \{z \in FG \mid zx = xz$ для всех $x \in FG\}$ называется *центром* FG. Для $X \subseteq G$ положим $\tilde{X} := \sum_{x \in X} x \in FG$.

Регулярным представлением группы G над F называется представление, эквивалентное представлению $Reg_{G,F} : G \to GL(F[G])$ с

$$Reg_{G,F}(x) : \sum_{g \in G} f_g g \mapsto \sum_{g \in G} f_g gx = \sum_{g \in G} f_{g^{-1}x} g.$$

Пусть $\mathcal{M}$ – матричное представление $G \to GL_n(F)$. *Координатными функциями* представления $\mathcal{M}$ называются функции

$$\mathcal{M}_{ij} : g \mapsto \mathcal{M}(g)_{ij} \ (g \in G), \quad \text{где } i, j \in \{1, \ldots, n\}.$$

Множество всех функций из G в F с операциями $\varphi_1 + \varphi_2 : g \mapsto \varphi_1(g) + \varphi_2(g)$, $f\varphi : g \mapsto f\varphi(g)$ ($\varphi, \varphi_1, \varphi_2$ – функции, $f \in F$) есть векторное F-пространство над F (размерности $|G|$). Обозначим его через $(G \to F)$. Пусть $GF(G \to F)$ – подпространство в $(G \to F)$, состоящее из всех *классовых функций*, т. е. функций, постоянных на каждом классе сопряжённых элементов группы G.

Представление конечной группы G над полем F называется *обыкновенным*, если $char\ (F)$ не делит $|G|$, и *модулярным* в противном случае.

Характером группы G называется характер любого представления G над $\mathbf{C}$. Характер неприводимого представления G над $\mathbf{C}$ называется *неприводимым характером группы* G. Степень и ядро представления, имеющего характер χ, называются соответственно *степенью* (обозначение: $deg(\chi)$) и *ядром* ($Ker(\chi)$) характера χ. Классовые функции из G в $\mathbf{C}$ называется *классовыми функциями группы* G. Разность двух характеров группы G называется *обобщенным характером* группы G.

Характер единичного представления G над $\mathbf{C}$ называется *главным характером* группы G и обозначается через 1_G. Пусть

$Irr(G)$ – множество всех неприводимых характеров группы G;

$CF(G) := CF(G \to \mathbf{C})$. Для $\alpha, \beta \in CF(G)$ определяются *скалярное произведение*

$$(\alpha,\beta)_G := \frac{1}{|G|}\sum_{g\in G}\alpha(g)\overline{\beta(g)}$$

и *произведение*

$$\alpha\beta : g \mapsto \alpha(g)\beta(g) \quad (g \in G),$$

$Irr(\alpha) := \{\chi \in Irr(G) \mid (\alpha, \chi)_G \neq 0\}$ и $Irr(\Xi) := \{Irr(\xi) \mid \xi \in \Xi\}$.

Если $\{C_1, \ldots, C_k\}$ – миожество всех классов сопряжённых элементов группы G, $g_i \in C_i$ и $Irr(G) = \{\chi_1, \ldots, \chi_k\}$, то $(k \times k)$-матрица X с $X_{ij} = \chi_i(g_j)$ называется *таблицей характеров* группы G.

Запись $D \trianglelefteq G$ означает, что D есть нормальное подмножество группы G.

Пусть $D \trianglelefteq G$, $\Phi \subseteq Irr(G)$ и $\psi \in CF(G)$. *D-срезкой* функции ψ называется классовая функция

$$\psi|_D^0 : g \mapsto \begin{cases} 0 & \text{при} \quad g \in G \setminus D, \\ \psi(g) & \text{при} \quad g \in G \end{cases} \quad (g \in G);$$

$\Phi|_D^0 := \{\varphi|_D^0 \mid \varphi \in \Phi\}$. Очевидно, $|_D^0$ – линейный оператор пространства $CF(G)$, $CF(G)|_D^0$ – подпространство в $CF(G)$, состоящее из всех классовых функций, исчезающих на $G \setminus D$, и $CF(G) = CF(G)|_D^0 \oplus CF(G)|_{G\setminus D}^0$.

Говорят, что D и Φ *взаимодействуют* (запись $D \longleftrightarrow \Phi$), если D-срезка $\varphi|_D^0$ любого характера φ из Φ является линейной комбинацией характеров из Φ: $\varphi|_D^0 = \sum_{\psi\in\Phi} a_{\varphi,\psi}\psi$, $a_{\varphi,\psi} \in \mathbf{C}$.

D-блоком группы G называется минимальное (по включению) непустое подмножество из $Irr(G)$, взаимодействующее с D, а *Ф-блоком* группы G – минимальное непустое нормальное подмножество из G, взаимодействующее с Φ.

Если X – таблица характеров группы G, $\Phi \subseteq Irr(G)$ и $D \trianglelefteq G$, то $X(\Phi, D)$ обозначает подматрицу из X, лежащую на пересечении строк, соответствующих характерам из Φ, и столбцов, соответствующих элементам из D. В случае, когда D и Φ взаимодействуют, матрица $X(\Phi, D)$ называется *активным фрагментом таблицы характеров* X группы G, или, для краткости, *активным фрагментом группы* G.

Важные понятия *индуцированного представления* и *индуцированной классовой функции* группы (связанные с некоторой её подгруппой) вводятся в задачах 22.77 и 22.78.

22.1. Пусть $\mathcal{M}_1$ и $\mathcal{M}_2$ – матричные представления группы G над F. Равносильны условия:

(1) $\mathcal{M}_1$ и $\mathcal{M}_2$ – матричные интерпретации одного операторного представления (т. е. $\mathcal{M}_1 \approx \mathcal{M}_2$);

(2) существует обратимая матрица S над F такая, что

$$S^{-1}\mathcal{M}_1(g)S = \mathcal{M}_2(g) \quad \text{для всех } g \in G.$$

22.2. Пусть $\mathcal{A}_1 : G \to GL(V_1)$ и $\mathcal{A}_2 : G \to GL(V_2)$ – операторные представления группы G. Равносильны условия:

(1) $\mathcal{A}_1$ и $\mathcal{A}_2$ – операторные интерпретации одного матричного представления (т.е. $\mathcal{A}_1 \approx \mathcal{A}_2$);

(2) существует изоморфизм σ из V_1 на V_2 такой, что

$$\sigma^{-1}\mathcal{A}_1(g)\,\sigma = \mathcal{A}_2(g) \text{ для всех } g \in G.$$

22.3. Все представления группы G над данным полем F разбиваются на непересекающиеся классы эквивалентных представлений ($\mathcal{A} \approx \mathcal{B} \Leftrightarrow \mathcal{A}$ и $\mathcal{B}$ лежат в одном классе).

22.4. Если $\mathcal{A}$ и $\mathcal{B}$ – эквивалентные представления группы G, то

1) $Ker(\mathcal{A}) = Ker(\mathcal{B})$;

2) $\mathcal{A}(G) \approx \mathcal{B}(G)$.

22.5. 1) Эквивалентные представления группы G имеют равные характеры.

2) Характер любого представления группы G является классовой функцией.

22.6. Пусть $\mathcal{A}_1, \ldots, \mathcal{A}_n$ – операторные и $\mathcal{M}_1, \ldots, \mathcal{M}_n$ – матричные представления группы G над полем F.

1) Если $\mathcal{A}_i : G \to GL(V_i)$ $(i = 1, \ldots, n)$ и V – внешняя прямая сумма пространств $V_1, \ldots, V_n$, то функция $\mathcal{A} : G \to GL(V)$ с

$$(v_1, \ldots, v_n)^{\mathcal{A}(g)} = (v_1^{\mathcal{A}(g)}, \ldots, v_1^{\mathcal{A}(g)}) \text{ для всех } g \in G$$

есть представление G над F ($\mathcal{A} = \mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n$ – *прямая сумма* представлений $\mathcal{A}_1, \ldots, \mathcal{A}_n$).

2) Функция $\mathcal{M}$ такая, что

$$\mathcal{M}(g) = \begin{pmatrix} \mathcal{M}_1(g) & & O \\ & \ddots & \\ O & & \mathcal{M}_n(g) \end{pmatrix} \text{ для всех } g \in G,$$

есть представление G над F ($\mathcal{M} = \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_n$).

3) Если $\mathcal{A}_i \approx \mathcal{M}_i (1 \le i \le n)$, то $\mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n \approx \mathcal{M}_1 \oplus \ldots \oplus \mathcal{M}_n$.

4) $\chi_{\mathcal{A}_1 \oplus \ldots \oplus \mathcal{A}_n} = \chi_{\mathcal{A}_1} + \ldots + \chi_{\mathcal{A}_n}$.

22.7. (Т) Для матриц $a \in M_m(F)$ и $b \in M_n(F)$ через $a \otimes b$ обозначается их кронекерово произведение, т.е. матрица, получающаяся из матрицы a заменой элементов a_{ij} клетками $a_{ij}b$.

Пусть $\mathcal{A}$ и $\mathcal{B}$ – матричные представления группы G степеней m и n над F. Определим функцию

$$\mathcal{A} \otimes \mathcal{B} : g \mapsto \mathcal{A}(g) \otimes \mathcal{B}(g) \ (g \in G).$$

1) $\mathcal{A} \otimes \mathcal{B}$ – представление группы G над F степени mn (называемое *тензором* (или *прямым*) *произведением* представлений $\mathcal{A}$ и $\mathcal{B}$).

2) Если $\mathcal{A}_1, \mathcal{B}_1$ – матричные представления G над F, $\mathcal{A} \approx \mathcal{A}_1$ и $\mathcal{B} \approx \mathcal{B}_1$, то $\mathcal{A} \otimes \mathcal{B} \approx \mathcal{A}_1 \otimes \mathcal{B}_1$.

22.8. Для представлений $\mathcal{A}$ и $\mathcal{B}$ из 22.7 $\chi_{\mathcal{A}\otimes\mathcal{B}} = \chi_{\mathcal{A}}\chi_{\mathcal{B}}$.

22.9. Пусть $\mathcal{A}$ – представление $G \to GL(V)$, а U и W – $\mathcal{A}(G)$-допустимые подпространства в V.

1) Отображение $\mathcal{A}_{U/W}$ (см. введение к § 22) правильно определено и действительно является представлением группы G.

2) $\mathcal{A}_{U+W/W} \approx \mathcal{A}_{U/U\cap W}$.

22.10. Представление $\mathcal{A}$ группы G приводимо тогда и только тогда, когда оно эквивалентно матричному представлению $\mathcal{M}$ такому, что для некоторого натурального $m < deg(\mathcal{A})$

$$\mathcal{M}(g) = \begin{pmatrix} A(g)_{m\times m} & O \\ B(g) & C(g) \end{pmatrix} \text{ для всех } g \in G.$$

22.11. Пусть $\mathcal{A}$ и $\mathcal{B}$ – представления группы G и $H \le G$. Тогда

1) если $\mathcal{A} \approx \mathcal{B}$, то $\mathcal{A}|_H \approx \mathcal{B}|_H$;

2) если $\mathcal{A}$ приводимо, то $\mathcal{A}|_H$ приводимо;

3) если $\mathcal{A}$ разложимо, то $\mathcal{A}|_H$ разложимо.

22.12. Пусть $\mathcal{M}$ – матричное представление $G \to GL_n(F)$. Определим функцию $\mathcal{M}^\dagger$ по правилу

$$\mathcal{M}^\dagger(g) = \mathcal{M}(g^{-1})^\tau (g \in G)$$

(т – транспортирование). Тогда

1) $\mathcal{M}^\dagger$ – представление группы G;

2) $\chi_{\mathcal{M}^\dagger}(g) = \chi_{\mathcal{M}}(g^{-1})$ $(g \in G)$;

3) $\mathcal{M}^\dagger$ неприводимо $\Leftrightarrow$ $\mathcal{M}$ неприводимо.

(Представление $\mathcal{M}^\dagger$ называется *контрградиентным* к $\mathcal{M}$.)

22.13. (Лемма Шура) Пусть $\mathcal{A} : G \to GL(V)$ и $\mathcal{B} : G \to GL(W)$ – неприводимые операторные представления группы G над полем F и пусть σ – гомоморфизм из V в W такой, что

$$\mathcal{A}(g)\sigma = \sigma\mathcal{B}(g) \text{ для всех } g \in G.$$

Тогда либо $\sigma = 0$ (т. е. $\sigma(V) = \{0\}$), либо σ – изоморфизм и, следовательно, $\mathcal{A} \approx \mathcal{B}$.

22.14. Показать, что матричная формулировка леммы Шура (22.13) такова: если $\mathcal{M} : G \to GL_m(F)$ и $\mathcal{N} : G \to GL_n(F)$ – неприводимые матричные представления группы G над полем F, $s \in M_{m\times n}(F)$ и

$$\mathcal{M}(g)s = s\mathcal{N}(g) \text{ для всех } g \in G,$$

то либо $s = o$ (нулевая матрица), либо $m = n$ и s обратима.

22.15. (Т) Если $\mathcal{X}$ – неприводимое представление группы G над полем, то центр группы $\mathcal{X}(G)$ – циклический.

22.16. Пусть $\mathcal{X}$ – неприводнмое представление $G \to GL_n(F)$, где F – алгебраически замкнутое поле. Тогда всякая матрица из $M_n(F)$, перестановочная с каждой матрицей из $\mathcal{X}(G)$, является скалярной.

22.17. Пусть F – алгебраически замкнутое поле.

1) Все неприводимые представления абелевой группы над F имеют степень 1.

2) Если $\mathcal{X}$ – неприводимое представление G над F, то

$$deg(\mathcal{X}) = 1 \Leftrightarrow Ker(\mathcal{X}) \supseteq G'.$$

22.18. Подпространство $S(\mathcal{M})$ пространства $(G \to F)$ всех функций из G в F, порождённое всеми координатными функциями матричного представления $\mathcal{M}$, называется *пространством координатных функций* представления $\mathcal{M}$.

1) Пространства координатных функций эквивалентных матричных представлений совпадают.

2) Если $\mathcal{R}$ – матричное регулярное представление группы G над полем F, то $S(\mathcal{R}) = (G \to F)$.

22.19. (Критерий неприводимости Бернсайда) Пусть G – конечная группа и $\mathcal{M}$ – представление $G \to GL(n, F)$ над алгебраически замкнутым полем F. Равносильны условия:

(1) $\mathcal{M}$ непрнводимо;

(2) множество всех координатных функций $\mathcal{M}_{ij}$ представления $\mathcal{M}$ состоит нз n^2 элементов и линейно независимо;

(3) $F[\mathcal{M}(G)] = M(n, F)$, т.е. $\mathcal{M}(G)$ содержит n^2 линейно незавнсимых (над F) матриц.

22.20. Пусть F – алгебраически замкнутое поле и $G = G_1 \times G_2$. Если при $i = 1, 2$ $\mathcal{X}_i$ – неприводимое матричное представление группы G над F такое, что $G_i \subseteq Ker\,(\mathcal{X}_i)$, то представление $\mathcal{X}_1 \otimes \mathcal{X}_2$ группы G неприводимо.

22.21. (Теорема Фробениуса–Шура) Пусть $\mathcal{X}_1, \ldots, \mathcal{X}_k$ – попарно не эквивалентные неприводимые представления группы G над алгебраически замкнутым полем F.

1) Если представления $\mathcal{X}_1, \ldots, \mathcal{X}_k$ матричные, то множество $T = \{(\mathcal{X}_i)_{s_i,t_i} \mid i \in \{1, \ldots, k\};\ s_i, t_i \in \{1, \ldots, deg\mathcal{X}_i\}\}$ всех координатных функций этих представлений линейно независимо над F, причём $|T| = \sum_{i=1}^{k} (deg\,\mathcal{X}_i)^2 \le |G|$.

2) Характеры представлений $\mathcal{X}_1, \ldots, \mathcal{X}_k$ попарно различны и линейно независимы.

22.22. (Т) Пусть $\mathcal{X}$ и $\mathcal{Y}$ – неприводимые матричные представления группы G над полем F.

1) Если $\mathcal{X}$ не эквивалентно $\mathcal{Y}$, то

$$\sum_{g \in G} \mathcal{X}(g)_{ij} \mathcal{Y}(g^{-1})_{kl} = 0 \quad \text{для любых возможных } i, j, k, l.$$

2) Если поле F алгебраически замкнуто, то

$$deg(\mathcal{X}) \sum_{g \in G} \mathcal{X}(g)_{ij} \mathcal{X}(g^{-1})_{kl} = |G| \delta_{il} \delta_{jk} \quad \text{для любых возможных } i, j, k, l.$$

22.23. Всякое обыкновенное представление конечной группы G эквивалентно прямой сумме неприводимых представлений группы G над тем же полем.

22.24. (Т) Пусть G – конечная группа и F – алгебраически замкнутое поле такое, что $char\,(F)$ не делит $|G|$.

1) Число классов неприводимых представлений группы G над F равно числу k классов сопряжённых элементов группы G.

2) Пусть $\chi_1, \ldots, \chi_k$ – все различные характеры неприводимых представлений G над F (число их равно k по 22.21(2)) и $g_1, \ldots, g_k$ – представители всех классов сопряжённых элементов в G. Тогда

$$\sum_{g \in G} \chi_i(g) \chi_j(g^{-1}) = |G|\, \delta_{ij}$$

(*первое соотношение ортогональности*) и

$$\sum_{i=1}^{k} \mathcal{X}_i(g_m) \chi_i(g_n^{-1}) = |C_G(g_m)| \delta_{mn}$$

(*второе соотношение ортогональности*).

22.25. Пусть F – алгебраически замкнутое поле характеристики 0.

1) Два представления G над полем F эквивалентны если и только если их характеры равны.

2) Конечные подгруппы A и B из $GL_n(F)$ сопряжены в $GL_n(F)$ если и только если существует изоморфизм γ из A на B такой, что след a = след $\gamma(a)$ для всех $a \in A$.

22.26. (Т) Пусть χ – характер группы G (т. е. характер некоторого представления G над $\mathbf{C}$) и $g \in G$.

1) Существует представление $\mathscr{X}$ группы G над $\mathbf{C}$ с характером χ такое, что $\mathscr{X}(g) = diag(\varepsilon_1, \ldots, \varepsilon_{\chi(1)})$, где $\varepsilon_i^{o(g)} = 1$. В частности $\chi(g) = \varepsilon_1 + \ldots + \varepsilon_{\chi(1)}$.

2) $|\chi(g)| \leq \chi(1)$.

3) $\chi(g^{-1}) = \overline{\chi(g)}$.

4) $Ker(\chi) = \{g \in G \mid \chi(g) = \chi(1)\}$.

5) $Z_\chi := \{g \in G \mid |\chi(g)| = \chi(1)\} \trianglelefteq G$ и $Z_\chi / Ker(\chi) \leq Z(G / Ker(\chi))$.

Если $\chi \in Irr(G)$, то $Z_\chi / Ker(\chi) = Z(G / Ker(\chi))$.

22.27. Характер χ группы G является гомоморфизмом если и только если $\chi(1) = 1$. (Характер степени 1 называется *линейным характером*.)

2) Число линейных характеров группы G равно индексу $|G : G'|$ коммутанта G' группы G.

22.28. 1) Построить таблицы характеров групп Z_3, S_3, D_8 и Q_8.

2) Заметить, что (неизоморфные) группы D_8 и Q_8 имеют одинаковые таблицы характеров (при подходящем упорядочении классов сопряжённых элементов и неприводимых характеров).

22.29. $\sum_{g \in G} \chi(xg)\overline{\chi(g)} = |G| \dfrac{\chi(x)}{\chi(1)}$ для любых $x \in G$ и $\chi \in Irr(G)$.

22.30. Если X – таблица характеров группы G и $g_1, \ldots, g_k$ – представители всех классов сопряжённых элементов G, то

$$|det(X)|^2 = \prod_{i=1}^{k} |C_G(g_i)|.$$

22.31. Скалярное произведение $(\alpha, \beta)_G := \dfrac{1}{|G|} \sum_{g \in G} \alpha(g)\overline{\beta(g)}$ в пространстве $CF(G)$ обладает следующими свойствами:

$$(\alpha, \beta)_G = \overline{(\beta, \alpha)_G}, \quad (\alpha + \beta, \gamma)_G = (\alpha, \gamma)_G + (\beta, \gamma)_G,$$
$$(c\alpha, \beta)_G = c(\alpha, \beta)_G, \quad (\alpha, c\beta)_G = \bar{c}(\alpha, \beta)_G$$

($\alpha, \beta, \gamma \in CF(G)$; $c \in \mathbf{C}$).

22.32. 1) $Irr(G)$ – ортонормированная база пространства $CF(G)$, т. е. $CF(G) = \oplus_{\chi \in Irr(G)} \mathbf{C}\chi$ и $(\chi, \psi)_G = \delta_{\chi,\psi}$ для всех $\chi, \psi \in Irr(G)$.

2) Если $\alpha \in CF(G)$, то $\alpha = \sum_{\chi \in Irr(G)} (\alpha, \chi)_G \chi$.

22.33. 1) Функция $\alpha \in CF(G)$ является характером группы G если и только если $\alpha = \sum_{\chi \in Irr(G)} a_\chi \chi$, где $a_\chi \in \mathbf{N} \cup \{0\}$ и не все a_χ равны 0.

2) Характер χ группы G неприводим если и только если $(\chi, \chi)_G = 1$.

3) Если χ и ψ – характеры группы G, то $Ker(\chi + \psi) = Ker(\chi) \cap Ker(\psi)$.

22.34. Пусть χ – характер группы G.

1) $(\chi, \chi)_G \leq \chi(1)^2$.

2) Когда $(\chi, \chi)_G = \chi(1)^2$?

22.35. 1) Произведение нескольких характеров группы также есть характер этой группы.

2) Если $\chi, \lambda \in Irr(G)$ и $\lambda(1) = 1$, то $\chi\lambda \in Irr(G)$.

3) Условие $\lambda(1) = 1$ в предыдущем утверждении не может быть опущено.

22.36. Пусть ρ – характер регулярного представления группы G над $\mathbf{C}$ (*регулярный характер* G).

1) $\rho(1) = |G|$ и $\rho(g) = 0$ при $g \in G \setminus \{1\}$.

2) $\rho = \sum_{\chi \in Irr(G)} \chi(1)\chi$.

3) $\bigcap_{\chi \in Irr(G)} Ker(\chi) = 1$.

22.37. 1) Элементы x и y группы G сопряжены в G если и только если $\chi(x) = \chi(y)$ для всех $\chi \in Irr(G)$.

2) Элемент x группы G сопряжён в G со своим обратным (такой элемент называется *вещественным* в G) если и только если $\chi(x) \in \mathbf{R}$ для всех $\chi \in Irr(G)$.

22.38. Пусть $\theta \in CF(G)$. Классовая функция $\overline{\theta}: g \mapsto \overline{\theta(g)}$ $(g \in G)$ называется *комплексно сопряжённой с* θ.

1) Если χ – характер группы G, то $\overline{\chi}$ – характер G.

2) Если $\theta \in Irr(G)$, то $\overline{\chi} \in Irr(G)$.

22.39. По таблице характеров группы G можно определить: $|G|$, порядки централизаторов элементов, порядки классов сопряжённых элементов, а также $Z(G)$ и G' как объединения определенных классов сопряжённых элементов.

22.40. (Т) *Алгебраическим числом (целым алгебраическим числом)* называется элемент из $\mathbf{C}$, являющийся корнем уравнения вида $x^n + a_1 x^{n-1} + \ldots + a_n = 0$, где $n \in \mathbf{N}$ и все a_i – рациональные (соответственно, целые) числа. Пусть $\hat{\mathbf{Q}}$ – множество всех алгебраических чисел, $\hat{\mathbf{Z}}$ – множество всех целых алгебраических чисел.

1) $\hat{\mathbf{Q}}$ – подполе в $\mathbf{C}$.

2) $\hat{\mathbf{Z}}$ – подкольцо в $\hat{\mathbf{Q}}$.

3) $\hat{\mathbf{Z}} \cap \mathbf{Q} = \mathbf{Z}$.

22.41. (Т) Пусть $\chi \in Irr(G)$, $\mathfrak{X}$ – (неприводимое) представление группы G над $\mathbf{C}$ с характером χ и ω_χ – отображение из $Z(\mathbf{C}G)$ в $\mathbf{C}$ такое, что $\omega_\chi\left(\tilde{g}^G\right) = \dfrac{\left|g^G\right|\chi(g)}{\chi(1)}$ при $g \in G$.

1) $\sum\limits_{x \in g^G} \mathfrak{X}(x) = \omega_\chi\left(\tilde{g}^G\right)E$, где E – единичная матрица или единичный оператор.

2) ω_χ – алгебраический гомоморфизм из $Z(\mathbf{C}G)$ в $\mathbf{C}$, т. е. такое линейное отображение, что $\omega_\chi(z_1 z_2) = \omega_\chi(z_1)\omega_\chi(z_2)$ для любых z_1, $z_2 \in Z(\mathbf{C}G)$.

3) $\omega_\chi\left(\tilde{g}^G\right)$ – целое алгебраическое число при любом $g \in G$.

4) $\chi(1) \| G|$.

22.42. Если $\chi \in Irr(G)$ и $\chi(1) = 2$, то группа G непроста.

22.43. Пусть $\chi \in Irr(G)$.

1) $\chi(zg) = \dfrac{\chi(z)\chi(g)}{\chi(1)}$ для всех $z \in Z(G)$ и $g \in G$, причём $\dfrac{\chi(z)}{\chi(1)}$ – корень степени $o(z)$ из единицы.

2) $\chi|_{Z(G)} = \chi(1)\lambda$, где $\lambda \in Irr(Z(G))$.

3) $\chi(1)^2 \le |G : Z(G)|$.

22.44. 1) $Z(FG)$ – подалгебра в FG.

2) $Z(FG) = F\tilde{C}_1 \oplus \ldots \oplus F\tilde{C}_k$, где $C_1, \ldots, C_k$ – все классы сопряжённых элементов группы G.

3) Существуют целые неотрицательные числа h_{ijm} такие, что для всех $i, j \in \{1, \ldots, k\}$

$$\tilde{C}_i \tilde{C}_j = \sum_{m=1}^{k} h_{ijm} \tilde{C}_m.$$

4) Пусть $char(F) = 0$. Если $g \in C_m$, то h_{ijm} есть число всех записей вида $g = g_i g_j$, где $g_i \in C_i$ и $g_j \in C_j$.

5) При $F = \mathbf{C}$ числа h_{ijm} могут быть определены по таблице характеров группы G:

$$h_{ijm} = \frac{|g_i^G||g_j^G|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_m)}}{\chi(1)}.$$

22.45. В групповой алгебре FG в случае, когда $char(F) \mid |G|$, найти элемент x такой, что $x \neq 0$ и $x^2 = 0$.

22.46. Пусть χ – характер группы G и $H \leq G$. Если $\chi|_H \in Irr(H)$, то $\chi \in Irr(G)$.

22.47. Пусть χ – точный характер группы G и $H \leq G$. Тогда H абелева если и только если каждая неприводимая часть характера $\chi|_H$ линейна.

22.48. Пусть $H \leq G$, $\chi \in Irr(G)$ и $\chi|_H = \chi(1)\lambda$, где λ – (линейный) характер H. Тогда $[G, H] \subseteq Ker(\chi)$.

22.49. Пусть $H \leq G$. Равносильны условия:

1) $H \subseteq Z(G)$;

2) для любого $\chi \in Irr(G)$ существует $\lambda \in Irr(G)$ такой, что $\chi|_H = \chi(1)\lambda$.

22.50. Пусть χ и ψ – характеры группы G.

1) $(\chi\psi, \chi\psi)_G \geq (\chi, \chi)_G$.

2) Когда в 1) имеет место равенство?

22.51. Пусть χ – характер группы G и $\mathfrak{X}$ – представление группы G над $\mathbf{C}$ с характером χ. Определим функцию $det\,\chi$ равенством $(det\,\chi)(g) = det(\mathfrak{X}(g))$. Тогда $det\,\chi$ есть (правильно определённый) линейный характер группы G.

22.52. Пусть χ – характер группы G и g – инволюция из G.

1) $\chi(g) \in \mathbf{Z}$ и $\chi(g) \equiv \chi(1) \pmod 2$.

2) Либо $\chi(g) \equiv \chi(1) \pmod 4$, либо G имеет нормальную подгруппу индекса 2.

22.53. Пусть G – конечная группа, в которой все элементы простого порядка p сопряжены, E – некоторая элементарная абелева p-подгруппа в G и $\chi \in Irr(G)$. Тогда

1) если $g \in G$ и $o(g) = p$, то $\chi(g) \equiv \chi(1) \pmod{|E|}$;

2) если $\chi \neq 1_G$ и $\chi(1) \leq \frac{|E|}{2}$, то G непроста или $|G| = p = 2$.

22.54. Пусть $\chi \in Irr(G)$.

1) $|\chi(G)| = 1$ (т. е. все значения характера χ равны) $\Leftrightarrow \chi = 1_G$.

2) $|\chi(G)| = 2 \Leftrightarrow |G : Ker(\chi)| = 2$ $(\text{и } \chi(G) = \{1, -1\})$.

22.55. Пусть $H \leq G$, $n \in \mathbf{N}$ и $\varphi(1) \geq n$ для всех $\varphi \in Irr(H) \setminus \{1_H\}$. Тогда для любого $\chi \in Irr(G)$ либо $\chi(1) \geq n$, либо $Ker(\chi) \supseteq H$.

22.56. Пусть χ – характер группы G.

1) Если $H \leq G$, то $\sum\limits_{h \in H} \chi(h) \in \mathbf{Z}$.

2) Если H – объединение нескольких подгрупп группы G, то $\sum\limits_{h \in H} \chi(h) \in \mathbf{Z}$.

3) Если $g \in G$ и $H = \left\{ g^m \,\middle|\, 1 \leq m \leq o(g),\ (m, o(g)) = 1 \right\}$, то $\sum\limits_{h \in H} \chi(h) \in \mathbf{Z}$.

22.57. Если $|G|$ нечётен, то любой неглавный неприводимый характер χ группы G не является вещественно значимым (т. е. $\chi \neq \overline{\chi}$). (W. Burnside)

22.58. Если G – группа нечётного порядка и k – число классов сопряжённых элементов в G, то $|G| \equiv k \pmod{16}$. (W. Burnside)

22.59. (Т) Пусть χ – характер группы G и $a \in Aut(\mathbf{Q}(\omega))$, где ω – первообразный корень степени $|G|$ из единицы.

1) Функция $\chi^a : g \mapsto \chi(g)^a$ $(g \in G)$ – также характер G.

2) $\chi^a \in Irr(G) \Leftrightarrow \chi \in Irr(G)$.

(Характер χ^a называется *алгебраически сопряжённым* с χ.)

3) Если $x \in \mathbf{Q}(\omega)$ и $x^a = x$ для всех $a \in Aut(\mathbf{Q}(\omega))$, то $x \in \mathbf{Q}$.

22.60. Пусть G, χ и ω – как в 22.59.

1) $Aut(\mathbf{Q}(\omega)) = \{\alpha_n \mid n \in \{1, \ldots, |G|\}, \ (n, |G|) = 1\}$, где автоморфизм α_n определяется равенством $\omega^{\alpha_n} = \omega^n$. В частности, $|Aut(\mathbf{Q}(\omega))| = \varphi(|G|)$.

2) $\chi^{\alpha_n}(g) = \chi(g^n)$ для всех $g \in G$ и всех α_n из 1).

22.61. Пусть $g \in G$. Равносильны условия:

(1) $\chi(g) \in \mathbf{Q}$ для всех $\chi \in Irr(G)$;

(2) g сопряжён в G с любым элементом вида g^m, где $m \in \mathbf{N}$ и $(m, |G| = 1)$.

22.62. Все элементы таблицы характеров симметричной группы S_n – целые числа.

22.63. Пусть $\chi \in Irr(G)$. Если χ – единственный характер из $Irr(G)$ степени $\chi(1)$, то $\chi(G) \subseteq \mathbf{Z}$.

22.64. 1) Пусть $g \in G$ и r – число пар (x, y) элементов из G таких, что $g = [x, y]$. Тогда $r = |G| \sum\limits_{\chi \in Irr(G)} \dfrac{\chi(g)}{\chi(1)}$.

2) Если g – коммутатор в G, $n \in \mathbf{N}$ и $(n, o(g)) = 1$, то g^n – коммутатор в G.

22.65. Пусть $g \in G$, $X := \{x \in G \mid \langle x \rangle = \langle g \rangle\}$ и χ – характер группы G. Предположим, что $\chi(g) \neq 0$. Тогда

$$\prod_{x \in X} |\chi(x)|^2 \geq 1 \text{ и } \sum_{x \in X} |\chi(x)|^2 \geq |X|,$$

причём левые части этих неравенств – целые числа.

22.66. Пусть G – конечная группа, $\chi \in Irr(G)$ и l – число элементов g из G таких, что $\chi(g) = 0$.

1) $l \geq \chi(1)^2 - 1$.

2) $l = 0 \Leftrightarrow \chi(1) = 1$.

22.67. (Теорема Бернсайда) Если $g \in G$ и $|g^G| = p^a$, где p – простое число и $a \in \mathbf{N}$, то группа G непроста.

22.68. (*$p^\alpha p^\beta$-теорема Бернсайда*) Каждая группа порядка $p^a q^b$, где p, q – различные простые числа и $a, b \in \mathbf{N}$, разрешима.

22.69. (Т) Пусть $N \trianglelefteq G$. Положим,

$$Irr(G \mid N) := \{\chi \in Irr(G) \mid Ker\,\chi \supseteq N\}.$$

1) Существует взаимно однозначное отображение $\chi \mapsto \chi'$ из $Irr(G \mid N)$ на $Irr(G/N)$ такое, что $\chi'(gN) = \chi(g) = \chi(gn) = \chi(ng)$ для все $g \in G$ и $n \in G$.

2) $N = \bigcap\limits_{x \in Irr(G \mid N)} Ker\,\chi$.

22.70. Пусть $N \trianglelefteq G$ и $g \in G$. Положим $\Phi := Irr(G) \setminus Irr(G \mid N)$.

1) $\left|C_G(g)\right| - \left|G_{G/N}(gN)\right| = \sum\limits_{\chi \in \Phi} \left|\chi(g)\right|^2$.

2) Если $C_N(g) = 1$, то $\left|C_G(g)\right| = \left|G_{G/N}(gN)\right|$ и $\chi(g) = 0$ для всех $\chi \in \Phi$.

22.71. Пусть $G = A \times B$. Для классовых функций α и β групп A и B соответственно через $\alpha \times \beta$ обозначим (классовую) функцию из G в $\mathbf{C}$ такую, что $(\alpha \times \beta)(ab) = \alpha(a)\beta(b)$ для всех $a \in A$ и $b \in B$.

1) $Irr(G) = \{\alpha \times \beta \mid \alpha \in Irr(A),\ \beta \in Irr(B)\}$.

2) Если α и β – обобщённые характеры A и B соответственно, то $\alpha \times \beta$ – обобщённый характер G.

22.72. Пусть $A = \langle a_1 \rangle \times \ldots \times \langle a_n \rangle$ – конечная абелева группа.

1) Множество $Irr(A)$ с операцией умножения классовых функций есть группа. (Она обозначается через $\hat{A}$ и называется *группой характеров* группы A.)

2) Пусть ε_i – некоторый первообразный корень степени $o(a_i)$ из единицы в поле $\mathbf{C}$. Каждому элементу $a = a_1^{s_1} \ldots a_n^{s_n}$ группы A поставим в соответствие функцию $\chi_a : A \to \mathbf{C}$ с $\chi_a(a_1^{t_1} \ldots a_n^{t_n}) = \varepsilon_1^{s_1 t_1} \ldots \varepsilon_n^{s_n t_n}$ $(s_i, t_i \in \mathbf{Z})$. Тогда

$$Irr(A) = \{\chi_a \mid a \in A\}.$$

3) Отображение $a \mapsto \chi_\alpha$ $(a \in A)$ есть изоморфизм группы A на группу $\hat{A}$.

4) Если $B \le A$, то отображение $\alpha \mapsto \alpha|_B$ $\left(a \in \hat{A}\right)$ есть гомоморфизм $\hat{A}$ на $\hat{B}$ с ядром

$$B^{\perp} := Irr(A|B) \quad \left(= \left\{\alpha \in \hat{A} \middle| \alpha(B) = 1\right\}\right).$$

5) Отображение $B \to B^{\perp}$ $(B \le A)$ есть взаимно однозначное отображение множества всех подгрупп группы A на множество всех подгрупп группы $\hat{A}$.

22.73. Построить таблицы характеров групп Z_4, E_4, A_4 и S_4.

22.74. Пусть $\mathcal{P}: G \mapsto S_\Omega$ – представление группы G перестановками конечного множества Ω. *Характером* представления $\mathcal{P}$ называется функция

$$\chi_{\mathcal{P}} : g \mapsto \left|\left\{i \in \Omega \middle| i^{\mathcal{P}(g)} = i\right\}\right| \quad (g \in G).$$

1) $\chi_{\mathcal{P}}$ – характер группы G.

2) $\left(\chi_{\mathcal{P}}, 1_G\right)_G = m$, где m – число орбит группы $\mathcal{P}(G)$.

22.75. Пусть $G = \{g_1, \ldots, g_n\}$ – группа порядка n. Рассмотрим представление

$$\mathcal{P}: g \mapsto \begin{pmatrix} g_1 & \cdots & g_n \\ g^{-1}g_1 g & \cdots & g^{-1}g_n g \end{pmatrix} \quad (g \in G)$$

группы G перестановками множества G. По 22.74, $\chi_{\mathcal{P}} = \sum\limits_{\chi \in Irr(G)} \alpha_\chi \chi$, где $\alpha_\chi \in \mathbb{N} \cup \{0\}$. Выразить α_χ через значения характера χ. Полученный результат сформулировать как свойство таблицы характеров группы G.

22.76. Пусть $H \le G$, $\{Hx_1, \ldots, Hx_n\}$ – множество всех смежных классов G по H и $\{H_1, \ldots, H_m\}$ – множество всех подгрупп, сопряжённых с H в G. Тогда отображения

$$\mathcal{P}: g \mapsto \begin{pmatrix} Hx_1 & \cdots & Hx_n \\ Hx_1 g & \cdots & Hx_n g \end{pmatrix} \quad (g \in G),$$

$$\mathcal{Q}: g \mapsto \begin{pmatrix} H_1 & \cdots & H_m \\ g^{-1}H_1 g & \cdots & g^{-1}H_m g \end{pmatrix} \quad (g \in G)$$

являются представлениями группы G перестановками, причём

$$\chi_{\mathcal{P}}(g) = \frac{|g^G \cap H| \, |C_G(g)|}{|H|} \quad \text{и} \quad \chi_{\mathcal{Q}}(g) = \frac{|g^G \cap N_G(H)| \, |C_G(g)|}{|N_G(H)|}.$$

22.77. (Т) Пусть $H \le G$ и $T = (t_1, \ldots, t_m)$ – система вычетов G по H, т. е. такая последовательность элементов группы G, что $G = Ht_1 \cup \ldots \cup Ht_m$. Для любого представления $\mathcal{A}: H \to GL_n(F)$ определим функцию $\mathcal{A}_T^G: G \to GL_{nm}(F)$ такую, что $\mathcal{A}_T^G(g)$ состоит из m^2 клеток степени n и клетка с координатами (i, j) есть $\mathcal{A}'(t_i g t_j^{-1})$, где $\mathcal{A}'(x) = \mathcal{A}(x)$ при $x \in H$ и $\mathcal{A}'(x) = O_{n \times n}$ при $x \in G \setminus H$.

1) $\mathcal{A}_T^G$ есть (правильно определённое) представление G над F.

Говорят, что $\mathcal{A}_T^G$ *индуцировано* представлением $\mathcal{A}$ (относительно T), а также что $\mathcal{A}_T^G$ – *индуцированное представление* группы G. (Если T ясно из контекста, то слова "относительно T" здесь опускают и пишут $\mathcal{A}^G$ вместо $\mathcal{A}_T^G$).

2) $\mathcal{A}_T^G \approx \mathcal{A}_R^G$ для любой системы вычетов R группы G по H.

22.78. (Т) Пусть $H \le G$ и $T = (t_1, \ldots, t_m)$ – система вычетов G по H. Для любой классовой функции $\xi \in CF(H \to F)$ определим функцию

$$\xi^G : g \mapsto \sum_{i=1}^{m} \xi'(t_i g t_i^{-1}),$$

где $\xi'(x) = \xi(x)$ при $x \in H$ и $\xi'(x) = 0$ при $x \in G \setminus H$.

1) ξ^G есть классовая функция из G в F и не зависит от выбора системы вычетов T.

Говорят, что функция ξ^G *индуцирована* функцией ξ, а также что ξ^G – *индуцированная классовая функция* группы G.

2) $\xi^G(g) = 0$, если $g^G \cap H = \varnothing$.

3) Если $H \le K \le G$, то $(\xi^K)^G = \xi^G$.

4) $\left(\sum_{i=1}^{n} f_i \xi_i\right)^G = \sum_{i=1}^{n} f_i \xi_i^G$ для любых $f_1, \ldots, f_n$ из F и $\xi_1, \ldots, \xi_n$ из $CF(H \to F)$.

5) Если $char(F)$ не делит $|H|$, то

$$\xi^G(g) = \frac{1}{|H|} \sum_{x \in G} \xi'(xgx^{-1}) = \frac{|C_G(g)|}{|H|} \sum_{x \in g^G \cap H} \xi(x).$$

22.79. 1) Если $\mathcal{A}$ – представление подгруппы H группы G, то $\chi_{\mathcal{A}_T^G} = (\chi_{\mathcal{A}})^G$.

2) Если ξ – характер подгруппы H группы G, то ξ^G – характер группы G (*индуцированный характер группы G*).

22.80. Пусть $H \le G$, T – система вычетов G по H и $\mathcal{A}$ – матричное представление H над полем F.

1) Как связаны ядра представлений $\mathcal{A}$ и $\mathcal{A}_T^G$?

2) Если $\mathcal{A}$ – регулярное представление H над F, то $\mathcal{A}_T^G$ – регулярное представление G над F.

3) Если $\mathcal{A} \approx \mathcal{B} \oplus \mathcal{C}$, то $\mathcal{A}_T^G \approx \mathcal{B}_T^G \oplus \mathcal{C}_T^G$.

4) Если $\xi \in CF(H \to F)$ и $\psi \in CF(G \to F)$, то $\xi^G \psi = \left(\xi\psi\big|_H\right)^G$.

22.81. Пусть $H \le G$ и ρ_H – регулярный характер H. Тогда $\left(\rho_H\right)^G = \rho_G$ – регулярный характер группы G. В частности $1_{\{1\}}^G = \rho_G$.

22.82. (Закон взаимности Фробениуса) Пусть $H \le G$, $\xi \in CF(H)$ и $\psi \in CF(G)$. Тогда

$$\left(\xi^G, \psi\right)_G = \left(\xi, \psi\big|_H\right)_H.$$

22.83. Пусть G – абелева группа и $H \le G$. Тогда каждый неприводимый характер H является ограничением на H некоторого неприводимого характера G.

22.84. Пусть $A \le B \le G$. Тогда $\left(1_A\right)^G - \left(1_B\right)^G$ – характер группы G.

22.85. Пусть $H \le G$ и ξ – классовая функция из G в $\mathbf{C}$ с $\xi(g) = \left|\left\{(h, x) \in H \times G \;\middle|\; h = g^x\right\}\right|$. Тогда $\xi = |H| 1_H^G$.

22.86. (Т) Пусть T – TI-подмножество конечной группы G и $H = N_G(T)$. Тогда G имеет точно одну нормальную подгруппу N такую, что

$$G = NH \text{ и } H \cap N = \langle H \setminus T \rangle.$$

При этом $N = G \setminus \left(H \setminus \langle H \setminus T \rangle\right)^G$. (В. А. Белоногов, 1978)

22.87. Из 22.86 вывести следующую *теорему Фробениуса*. Пусть $H \le G$ и $H \cap H^g = 1$ для всех $g \in G \setminus H$. Тогда G имеет точно одну нормальную подгруппу N такую, что $G = H \lambda N$. Более того, $N = G \setminus (H \setminus 1)^G$.

22.88. Пусть $H_0 \trianglelefteq H \leq G$ и

$$H \cap H^g \subseteq H_0 \cup H_0^g \quad \text{для всех} \quad g \in G \setminus H.$$

Тогда G имеет точно одну нормальную подгруппу N такую, что $G = HN$ и $H \cap N = H_0$. При этом $N = G \setminus \left(H \setminus H_0\right)^G$.

22.89. Пусть $G \neq 1$, $g \in G$ и $\chi \in Irr(G)$. Тогда

$$g^G \not\hookrightarrow \{\chi\} \Leftrightarrow \chi(g) = 0.$$

22.90. Пусть $D \subseteq \big| G$ и $\Phi \subseteq Irr(G)$.

1) Если Φ – D-блок группы G, то либо $Irr\left(\Phi|_D^0\right) = \varnothing$ (и тогда $|\Phi| = 1$), либо $Irr\left(\Phi|_D^0\right) = \Phi$.

2) Если $\Phi|_D^0 \subseteq \mathbf{C}[\Phi] + \mathbf{C}\psi$, где $\psi \in Irr(G)$, то либо $D \not\hookrightarrow \Phi$, либо $D \not\hookrightarrow \Phi \cup \{\psi\}$.

22.91. (Т) Пусть G – конечная группа $D \subseteq \big| G$ и $\Phi \subseteq Irr(G)$. Положим $D^- := G \setminus D$ и $\Phi^- := Irr(G) \setminus \Phi$. Следующие условия равносильны:

(1) $D \not\hookrightarrow \Phi$;

(2) $\sum\limits_{d \in D} \varphi(d)\,\overline{\chi(d)} = 0$ для всех $(\varphi, \chi) \in \Phi \times \Phi^-$;

(3) $\sum\limits_{\varphi \in \Phi} \varphi(d)\,\overline{\varphi(g)} = 0$ для всех $(d, g) \in D \times D^-$;

(4) $\dfrac{1}{|G|} \sum\limits_{d \in D} \sum\limits_{\varphi \in \Phi} \varphi_0(d)\,\overline{\varphi(d)}\,\varphi(d_0) = \varphi_0(d_0)$ для всех $(\varphi_0, d_0) \in \Phi \times D$.

(В. А. Белоногов, 1984)

22.92. Пусть G, D и Φ – как в предыдущей задаче. Равносильны условия:

(1) $D \not\hookrightarrow \Phi$;

(2) $D^- \not\hookrightarrow \Phi$;

(3) $D \not\hookrightarrow \Phi^-$;

(4) $D^{-1} := \left\{d^{-1} \,\middle|\, d \in D\right\} \not\hookrightarrow \Phi$;

(5) $D \not\hookrightarrow \overline{\Phi} := \left\{\overline{\varphi} \,\middle|\, \varphi \in \Phi\right\}$.

22.93. Пусть D, D_1, D_2 – нормальные подмножества из G, а Φ, Φ_1, Φ_2 – подмножества из $Irr(G)$.

1) Если $D_1 \not\hookrightarrow \Phi$ и $D_2 \not\hookrightarrow \Phi$, то $D_1 \cap D_2 \not\hookrightarrow \Phi$, $D_1 \cup D_2 \not\hookrightarrow \Phi$ и $D_1 \setminus D_2 \not\hookrightarrow \Phi$.

2) Если $D \leftarrow\!\!\!\rightarrow \Phi_1$ и $D \leftarrow\!\!\!\rightarrow \Phi_2$, то $D \leftarrow\!\!\!\rightarrow \Phi_1 \cap \Phi_2$, $D \leftarrow\!\!\!\rightarrow \Phi_1 \cup \Phi_2$ и $D \leftarrow\!\!\!\rightarrow \Phi_1 \setminus \Phi_2$.

22.94. Пусть $A = X(\Phi, D)$ – активный фрагмент группы G $\left(\Phi \subseteq Irr(G), D \subseteq\!\!\mid G\right)$.

1) $1_G \in \Phi \Leftrightarrow A$ имеет строку $(1, \ldots, 1)$.

2) $1 \in D \Leftrightarrow A$ имеет ненулевой столбец, состоящий из вещественных неотрицательных чисел (тогда A имеет столбец, состоящий из степеней характеров из Φ).

3) Если в A вычеркнуть нулевую строку или нулевой столбец, то получится снова активный фрагмент группы G.

22.95. Пусть $D \leftarrow\!\!\!\rightarrow \Phi$ и

$$X(\Phi, D) = \begin{pmatrix} 1 & 1 & 1 \\ 4 & 0 & 1 \\ 3 & -1 & 0 \\ 3 & -1 & 0 \end{pmatrix}.$$

1) Показать, что $1 \in D$ и найти порядки централизаторов всех элементов из D в группе G.

2) Доказать, что $G \simeq A_5$.

22.96. Пусть X – таблица характеров группы G, $D \subseteq\!\!\mid G$ и $\Phi \subseteq Irr(G)$; $D^- := G \setminus D$ и $\Phi^- := Irr(G) \setminus \Phi$. Пусть $X(\Phi, D)$ имеет t столбцов, которым соответствуют элементы $d_1, \ldots, d_t$ соответственно, и

$$T = diag\left(\left|C_G(d_1)\right|, \ldots, \left|C_G(d_t)\right|\right)^{-1}.$$

Равносильны условия:

(1) $D \leftarrow\!\!\!\rightarrow \Phi$ и ранг $X(\Phi, D) = t$;

(2) $X(\Phi, D)^* X(\Phi, D) = T^{-1}$;

(3) $X\left(\Phi^-, D\right) = O$.

22.97. Пусть выполнено условие предыдущей задачи. Равносильны условия:

1) $D \leftarrow\!\!\!\rightarrow \Phi$ и ранг $X(\Phi, D) = \left|\Phi\right|$;

2) $X(\Phi, D) T X(\Phi, D)^* = E$;

3) $X\left(\Phi, D^-\right) = O$.

22.98. Если $D \leftarrow\!\!\!\rightarrow \Phi$ и матрица $X(\Phi, D)$ – квадратная невырожденная $\left(D \subseteq\!\!\mid G, \Phi \subseteq Irr(G)\right)$, то $D = G$ и $\Phi = Irr(G)$.

22.99. Равносильны условия:

(1) G имеет активный фрагмент

$$\begin{pmatrix} 1 & \dots & 1 \\ \vdots & & \vdots \\ 1 & \dots & 1 \end{pmatrix}$$ размеров $s \times t$;

(2) G имеет нормальную подгруппу H такую, что $|G:H| = s$, $H \supseteq G'$ и H состоит из t классов сопряжённых элеметов группы G.

22.100. Равносильны условия:

(1) G имеет активный фрагмент, состоящий из t равных положительных вещественных столбцов;

(2) G имеет нормальную подгруппу, состоящую из t классов сопряжённых элементов группы G.

§ 23. Разные задачи

В этом параграфе
p – простое число и
π – множество простых чисел.

pd-группой **называется группа, содержащая неединичный p-элемент.**

πd-группа **– это группа, содержащая неединичный π-элемент. Очевидно, конечная группа является πd-группой если и только если её порядок делится на простое число из π.**

Группы равных порядков называются *изоордными*. Если $H \le G$, то множество всех подгрупп из G, изоордных H, называется *классом изоордных подгрупп* группы G (с представителем H). Классы сопряжённых подгрупп называются посто *классами подгрупп*. Максимальная подгруппа максимальной подгруппы группы G называется 2-*максимальной* подгруппой в G.

Группой типа A **называется ненильпотентная q-замкнутая группа порядка pq^{δ}, где p и q – различные простые числа и δ – показатель q по модулю p (т. е. δ – наименьшее из натуральных чисел m таких, что $q^m \equiv 1 \pmod{p}$).**

Напомним, что *группа Шмидта* – это ненильпотентная группа, все собственные подгруппы которой нильпотентны, а *группа Миллера–Морено* – это неабелева группа, все собственные подгруппы которой абелевы.

23.1. Пусть P – минимальная нормальная подгруппа группы G порядка p^{α} (p – простое число, а $\alpha \in \mathbf{N}$) и $P \not\subseteq Z(G)$. Тогда $\alpha < |G:P|$; более точно: $\alpha < \min\limits_{x \in P \setminus \{1\}} |x^G|$.

23.2. Пусть P – минимальная нормальная подгруппа порядка p^{α} (p – простое число, $\alpha > 1$) группы G. Если существует простое число $q \neq p$, не делящее α и делящее $\left|G:N_N\left(\tilde{P}\right)\right|$ для любой собственной подгруппы $\tilde{P}$ из P, то α есть показатель числа p по модулю q.

23.3. Конечная группа, имеющая максимальную подгруппу простого порядка p, есть или группа порядка pq, где q – простое число, или группа типа A.

23.4. Конечная непростая группа имеет пару максимальных подгрупп взаимно простых порядков тогда и только тогда, когда она имеет порядок pq, где p и q – различные простые числа, или есть группа типа A.

23.5. Если G – группа Шмидта, то:

1) $G = \langle a \rangle_{p^\alpha} \leftthreetimes Q$, где $|Q| = q^\beta$, p и q – различные простые числа, $\alpha, \beta \in \mathbf{N}$;

2) каждая максимальная подгруппа группы G либо совпадает с $\langle a^p \rangle \times Q$, либо сопряжена с $\langle a \rangle \times \Phi(Q)$.

3) $\Phi(Q) = Z(G) = \langle a^p \rangle \times \Phi(Q)$;

4) $|Q/\Phi(Q)| = q^\delta$, где δ – показатель q по модулю p;

5) $G' = Q$;

6) $Q' = \Phi(Q)$. (О. Ю. Шмидт, 1924)

23.6. Группа Шмидта является группой Миллера–Морено если и только если её ненормальная силовская подгруппа максимальна в ней.

23.7. Следующие условия конечной группы G равносильны:

(1) G есть группа Шмидта и одновременно группа Фробениуса;

(2) G – группа типа A.

23.8. Пусть G – конечная группа и p – простое число.

1) G нильпотентна $\Leftrightarrow$ G не имеет подгрупп Шмидта $\Leftrightarrow$ все бипримарные подгруппы в G нильпотентны.

2) G p-нильпотентна $\Leftrightarrow$ G не имеет p-замкнутых pd-подгрупп Шмидта $\Leftrightarrow$ все бипримарные подгруппы в G p-нильпотентны.

3) G p-разложима $\Leftrightarrow$ G не имеет pd-подгрупп Шмидта $\Leftrightarrow$ все бипримарные подгруппы в G p-разложимы.

23.9. Пусть G – конечная группа, каждая собственная подгруппа которой, порождённая двумя элементами, p-нильпотентна. Тогда G p-нильпотентна.

23.10. Конечная непримарная группа имеет бипримарную pd-подгруппу для любого простого числа p, делящего её порядок.

23.11. Для конечной непримарной группы G равносильны условия:

(1) G не имеет собственных бипримарных подгрупп;

(2) все собственные подгруппы группы G примарны;

(3) G есть группа типа A или группа порядка pq, где p и q – различные простые числа.

23.12. Описать конечные ненильпотентные pd-группы, в которых все собственные pd-подгруппы нильпотентны (группы типа S_p по С. А. Чунихину, 1938).

23.13. Пусть G – конечная группа, все бипримарные подгруппы (чётного порядка) которой 2-замкнуты. Тогда G 2-замкнута.

23.14. Пусть G – конечная группа и нормализатор в G любой подгруппы нечётного порядка имеет нечётный порядок. Тогда группа G 2-замкнута.

23.15. Пусть G – бипримарная pd-группа, все собственные подгруппы которой p-замкнуты. Определить строение G.

23.16. Пусть G – конечная группа, все подгруппы которой, порождённые двумя элементами, 2-замкнуты. Тогда G 2-замкнута.

23.17. Всякая конечная группа, порядок которой делится более чем на два различных простых числа, порождается своими бипримарными подгруппами. Описать конечные группы, не порождающиеся своими собственными бипримарными подгруппами.

23.18. Для конечной не π-замкнутой группы G равносильны условия:

(1) все максимальные подгруппы группы G π-замкнуты и $G/\Phi(G)$ непроста;

(2) G – группа Шмидта.

23.19. Каковы конечные непростые группы с единственным классом непримарных собственных подгрупп?

23.20. Пусть A, B и C – подгруппы конечной группы G.

1) Если A субнормальна в B, то $A \cap C$ субнормальна в $B \cap C$.

2) Если A и B субнормальны в G, то и $\langle A, B\rangle$ субнормальна в G.

23.21. Следующие условия конечной группы G равносильны:

(1) все циклические подгруппы группы G субнормальны в ней;

(2) все подгруппы группы G субнормальны в ней;

(3) G нильпотентна.

23.22. Для конечной нильпотентной группы G равносильны условия:

(1) все 2-максимальные подгруппы из G субнормальны в G;

(2) G – группа Миллера–Морено.

23.23. Следующие условия конечной группы G равносильны:

(1) G имеет точно один класс несубнормальных изоордных подгрупп;

(2) G – непримарная группа Миллера–Морено.

23.24. Пусть G – конечная группа и p – простое число. Если G имеет лишь один класс несубиормальных изоордных pd-подгрупп, то G разрешима.

23.25. Пусть G – конечная группа, имеющая точно два класса изоордных несубнормальных подгрупп. Тогда каждая максимальная подгруппа группы G является нильпотентной группой или группой Миллера–Морено.

23.26. Пусть G – конечная группа и π – множество простых чисел. Следующие условия равносильны:

(1) каждая π-подгруппа из G субнормальна в G;

(2) G имеет нормальную нильпотентную π-холлову подгруппу.

23.27. Пусть G конечная группа и π – множество простых чисел. Следующие условия равносильны:

(1) G имеет точно один класс изоордных несубнормальных π-подгрупп;

(2) G – группа одного из следующих двух типов:

а) $\pi(G) \cap \pi = \{p\}$, G имеет ненормальную циклическую силовскую подгруппу p-подгруппу $\langle a\rangle$ и $\langle a^p\rangle \lhd G$.

б) $\pi(G) \cap \pi = \{p, q\}$, $p \neq q$ и G имеет нормальную π-холлову подгруппу H, являющейся группой Миллера–Морено.

23.28. Описать конечные группы, у которых всякая собственная подгруппа, содержащая центр группы, нильпотентна.

23.29. Найти все конечные группы G такие, что для любых трех её собственных подгрупп A, B и C из $AC = BC$ и $C \not\trianglelefteq \langle A, B\rangle$ следует, что $A = B$.

23.30. Найти все конечные группы, в которых для любых трёх её подгрупп A, B, C будет $AC \cap BC = (A \cap B)C$.

23.31. Если в конечной группе G любые два примарных элемента одинаковых порядков перестановочны, то группа G абелева.

23.32. Если в конечной группе все подгруппы Шмидта иормальны, то она разрешима.

23.33. Пусть N – нормальная подгруппа конечной группы G.

1) Каждая бипримарная подгруппа группы G/N является образом (при естественном гомоморфизме G на G/N) некоторой бипримарной подгруппы группы G.

2) Подгруппа Шмидта группы G/N может не быть образом подгруппы Шмидта группы G (построить такие G и N).

23.34. Следующие условия конечной ненильпотентной группы G равносильны:

(1) каждая подгруппа группы G либо субнормальна в G, либо совпадает со своим нормализатором;

(2) $G = N \lambda \langle a \rangle_{p^\alpha}$, где $N_G(\langle a \rangle) = \langle a \rangle$ и $a^p \in Z(G)$.

23.35. Описать конечные группы, в которых

а) нормализатор любой неединичной циклической подгруппы циклический,

б) нормализатор любой неединичной абелевой подгруппы абелев,

в) нормализатор любой неединичной нильпотентной подгруппы нильпотентен.

23.36. Конечная группа, в которой нормализатор любой ненормальной нильпотентной подгруппы нильпотентен, является расширением нильпотентной группы с помощью нильпотентной группы.

23.37. В конечной непримарной группе G любая непримарная подгруппа нормальна тогда и только тогда, когда выполнено одно из следующих условий:

(1) G дедекиндова,

(2) $G = P \leftthreetimes Q$, P – дедекиндова p-группа, $|Q| = q^\beta$, где p и q – различные простые числа, и

либо $\beta = 1$,

либо G – группа Фробениуса с ядром Q и β – показатель q по модулю p.

23.38. Конечная группа, в которой любые два сопряжённых элемента перестановочны, нильпотентна.

23.39. Описать строение конечной группы G, в которой любые два элемента порождают подгруппу, порядок которой либо – простое число, либо – произведение двух простых множителей (одинаковых или различных).

23.40. Определить все конечные группы G, в которых для любого истинного делителя n порядка G в G существует элемент порядка n.

23.41. Пусть G – конечная группа, $H < G$ и любые два элемента из $G \setminus H$ сопряжены в G. Показать, что группа G разрешима и описать её строение.

23.42. Пусть G – конечная группа, $P \in Syl_p(G)$ и $O_p(G) = 1$. Если

а) ни один собственный делитель числа $n := |G : P|$ не сравним с 1 по модулю p, и

б) $n \not\equiv 1 \pmod{p^2}$,

то G – группа типа A.

23.43. Конечная группа, в которой каждая истинная иенильпотентная подгруппа отлична от своего нормализатора, разрешима.

23.44. Пусть силовская подгруппа P группы G перестаиовочна с каждой максимальной подгруппой из G. Тогда $P \trianglelefteq G$.

23.45. Пусть силовская подгруппа P группы G перестановочиа с каждой 2-максимальной подгруппой группы G. Тогда либо $P \trianglelefteq G$, либо G – группа Миллера–Морено.

23.46. Пусть G имеет максимальную подгруппу с единичной сердцевиной и все такие подгруппы

а) p-разложимы или

б) p-нильпотентны и $p > 2$.

Доказать, что G p-разрешима и найти её p-длину.

(G. Pazdersky, 1964)

23.47. Пусть G имеет максимальную подгруппу с единичной сердцевиной и все такие подгруппы 2-нильпотентны. Если силовская 2-подгруппа в G есть дедекиндова группа или группа Миллера–Морено, то G 2-разрешима. Найти её 2-длину.

23.48. Описать конечные группы, в которых пересечение любых двух неинцидентных собственных подгрупп является максимальной подгруппой каждой из них. (Две подгруппы называются *инцидентными*, если одна из них содержится в другой).

23.49. Определить все конечные группы, имеющие

а) точно 3 класса сопряжённых элементов,

б) точно 4 класса сопряжённых элементов.

23.50. Пусть G – конечная группа, в которой не все инволюции сопряжены. Тогда существует инволюция t в G такая, что $|G| < |C_G(t)|^3$ (R. Brauer)

23.51. В конечной группе чётного порядка число классов сопряжённых 2-центральных инволюций нечётно. (2-центральный элемент группы – это элемент из центра некоторой 2-силовской подгруппы этой группы.)

23.52. Пусть $G = AB$, где G – конечная группа. A и B – её абелевы подгруппы и $(|A|,|B|) = 1$. Тогда $N_G(A)$ и $N_G(B)$ имеют нормальные дополнения в G. А именно, $G = [A, B_G] \lambda N_G(A) = [B, A_G] \lambda N_G(B)$.

(Н. А. Романовская, 1989)

23.53. Пусть $P \in Syl_p(G)$, $x \in P$, и $X := x^G \not\subseteq P$.

1) Существует $Q \in Syl_p(G)$ такая, что $X \cap P \neq X \cap Q$.

2) Среди всех Q со свойством пункта 1) зафиксируем такую, для которой $|X \cap P \cap Q|$ максимален, и положим $D = \langle X \cap P \cap Q \rangle$. Тогда

а) $N_{X\cap P}(D) \not\subseteq D$, $N_{X\cap Q}(D) \not\subseteq D$;

б) $\langle x, y \rangle$ не является p-группой для любых $x \in N_{X\cap P}(D) \setminus D$ и $y \in N_{X\cap Q}(D) \setminus D$.

23.54. (Теорема Бэра–Судзуки) Для p-элемента x группы G равносильны условия:

(1) $x \in O_p(G)$;

(2) $\langle x, x^g \rangle$ есть p-группа для любого $g \in G$.

23.55. Пусть $G = AB$, где G – конечная группа и A, B – её подгруппы. Пусть p – простое число. Тогда $O_p(A) \cap O_p(B) \leq O_p(G)$ и $\langle O_p(A), O_p(B) \rangle$ – p-группа. (Л. С. Казарин)

23.56. Пусть G – конечная группа и $K \leq G$.

1) Если $N_G(K) = K$, то $H(G) \subseteq K$. ($H(G)$ – гиперцентр G.)

2) $G' \cap H(G) \subseteq \Phi(G)$.

23.57. Пусть $G = A \lambda B \neq A \times B$ и $|B| = 3$. Тогда

1) если $A \simeq E_4$, то $G \simeq A_4$;

2) если $A \simeq Q_8$, то $G \simeq SL_2(3)$.

В обонх случаях $[A, B] = A$.

23.58. Пусть A и B – различные нормальные подгруппы группы G, каждая из которых изоморфна A_4 или $SL_2(3)$. Тогда

либо $O_2(A) = O_2(B)$ и $\langle A, B \rangle \simeq A \times Z_3 \simeq B \times Z_3$,

либо $[A, B] = 1$.

23.59. Пусть A и B – нормальные π-подгруппы группы G, где $\pi = \{p, q\}$, и каждая из них есть q-замкнутая группа Шмидта. Тогда
либо $A \cap B$ является силовской q-подгруппой и в A, и в B,
либо $[A, B] \subseteq O_p(Z(AB))$.

23.60. Пусть T – примарная Tl-подгруппа конечной группы G и $N \trianglelefteq G$. Тогда
либо $[N, T] \subseteq N \cap T$,
либо $|N| > |T|$.

23.61. Пусть $t(G)$ – наибольший общий делитель порядков классов сопряжённых ненормальных подгрупп конечной группы G (число П. И. Трофимова).
1) Если $t(G) > 1$ и G не нильпотентна, то $t(G)$ – простое число.
2) Если $t(G) > 1$ и G нильпотентна, то точно одна силовская подгруппа в G не дедекиндова (и $t(G)$ делит её порядок).
3) Найти $t(G)$ для группы $G = D_{16}$.

23.62. Пусть G – конечная группа и $\tau(G)$ – наибольший общий делитель чисел $|H / H_G|$ для всех ненормальных подгрупп H из G.
1) Если $\tau(G) > 1$, то $\tau(G)$ – простое число.
2) $t(G) = p \Leftrightarrow G = P \leftthreetimes D$, где $P \in Syl_p(G)$, D – дедекиндова, и P не дедекиндова, если $P \trianglelefteq G$.

Ответы и подсказки

Здесь
m, n – натуральные числа,
p – простое число и, за исключением § 19,
q – простое число, отличное от p.

§ 1

1.1. (См. [11], § 1 и § 2; [16], I.1.3.) 1): Будем использовать мультипликативное обозначение операции. Пусть e и e_1 – нейтральные элементы в G и $a \in G$. Тогда (используйте аксиомы группы) существуют $x, y \in G$ с $xa = e$ и $yx = e$, и тогда $a = ea = (yx)a = y(xa) = ye$, откуда $ax = (ye)x = y(ex) = yx = e$. Таким образом,

$$\text{из } xa = e \text{ следует } ax = e \text{ для всех } a, x \in G. \qquad (a)$$

Так как e, e_1 – нейтральные элементы, то $ee_1 = e_1$ и $e_1e = e$. Но из последнего равенства по (a) $ee_1 = e$. Следовательно, $e = e_1$.

Наконец, $a = ea = (xa)e =_{(a)} (ax)a = a(xa) = ae$.

2): Если $xa = e = za$, то по (a) $ax = e = az$. Следовательно, $x = ex = (xa)x = x(ax) = x(az) = (xa)z = ez = z$.

1.9. 2): Не зная операцию $\cdot$, но зная Φ, можно отметить в нём все "групповые" функции, т. е. функции φ такие, что (M, φ) – группа. Это можно сделать проверкой условий:

1) $\varphi(\varphi(x, y), z) = \varphi(x, \varphi(y, z))$ для всех $x, y, z \in M$,

2) существует $e \in M$ такой, что $\varphi(e, x) = x$ для всех $x \in M$,

3) для каждого $x \in M$ существует $y \in M$ такой, что $\varphi(x, y) = e$.

Такие функции в Φ есть: такова, например, функция $\varphi(x, y) = xy$ (хотя сейчас она нам не известна). Но для любой такой функции φ согласно 1) $(M, \varphi) \simeq G$.

1.11. Нет.

1.15. а): да, б): да, в): нет, г): нет, д): нет, е): да, ё): да.

1.44. 2): $X = A \Delta B$.

1.45. Не являются.

1.47. 2): $\{(a, 1) \mid a \in \mathbf{R}\}$ и $\{(0, b) \mid b \in \mathbf{R}\backslash\{0\}\}$.

3): $\{(a, -1) \mid a \in \mathbf{R}\}$ – множество всех инволюций в G. G не имеет элементов конечного порядка, большего двух.

1.50. M_λ – группа $\Leftrightarrow \lambda < 0$.

1.51. Нет.

1.52. 2): Да.

1.54. 4.

§ 2

2.6. Нет.

2.8. 4): M – максимальная подгруппа в $G \Leftrightarrow M = \langle a^p \rangle$, где p – простое число.

2.13. В Z_4 – 3 подгруппы, в $Z_2 \times Z_2$ – 5 подгрупп, в Z_6 – 4 подгруппы, в S_3 – 5 подгрупп.

2.14. Нет.

2.15. $\{\langle n \rangle \mid n \in \mathbf{N}\}$ – множество всех подгрупп в $\mathbf{Z}^+$, $|\mathbf{Z}^+ : \langle n \rangle| = n$. M – максимальная подгруппа в $\mathbf{Z}^+ \Leftrightarrow M = \langle p \rangle$, где p – простое число.

2.16. Каждая группа с указанным свойством изоморфна $\mathbf{Z}^+$.

2.17. 2): Системой вычетов является множество $\{1, g, \ldots, g^{d-1}\}$, где $d = |m|$, если $o(g) = \infty$, и $d = (|m|, o(g))$, если $o(g) < \infty$.

2.18. 3): а): $G = S_3$, $|H| = 2$; б): $G = S_3$, $|H| = 3$.

2.23. Нет.

2.25. 3): При $k = 1$ G изоморфна Z_2 (если $A \subseteq B$ или $A \supseteq B$) или $Z_2 \times Z_2$. При $k = 2$ G либо изоморфна Z_3, Z_4, $Z_2 \times Z_2$, Z_6 или S_3, либо есть нециклическая группа порядка 8.

2.26. а): $G = 1$ или $G \simeq Z_p$; б): $G \simeq Z_{p^2}$;

в): $G \simeq Z_{p^3}$ или $G \simeq Z_{pq}$;

г): $G \simeq Z_{p^4}$ или $Z_2 \times Z_2$.

2.27. а): $G \simeq Z_{p^m}$; б): $G \simeq Z_{p^m q^n}$.

2.30. 2): $o(-1) = 2$, $o(i) = o(j) = o(k) = 4$. Все подгруппы: $\{1\}$, $\langle i \rangle$, $\langle j \rangle$, $\langle k \rangle$, Q_8.

2.39. Примените индукцию по n.

2.50. G и T обладают указанным свойством $\Leftrightarrow$ в G все неединичные элементы – инволюции и $|T| = 2$.

2.52. Нет.

2.56. Нет.

2.58. Вторая, третья и четвёртая группы.

2.60. $\mathbf{Q}^+$ не имеет максимальных подгрупп.

§ 3

3.4. 3): Элементы a и a^{-1} при $o(a) = \infty$; элементы a^k с $(k, o(a)) = 1$ при $o(a) < \infty$.

5): При $o(a) = \infty$ – это все нечётные степени a; при нечётном $o(a)$ в $\langle a \rangle$ нет неквадратов; при $o(a) = 2k$ все неквадраты составляют множество $\{a, a^3, \ldots, a^{2k-1}\}$.

3.8. 3): $Z_{30} = Z_2 Z_3 Z_5$; $Z_{61} = Z_{61}$; $Z_{10} \times Z_{60} = ABC$, где $A \simeq Z_2 \times Z_4$, $B \simeq Z_3$, $C \simeq Z_5 \times Z_5$.

3.11. 2): $\left\{1, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\right\}$.

3.12. Взаимно однозначные отображения: 1), 3), 4). а): 4), б): 1), 4).

3.16.

$$\frac{(p^n-1)(p^{n-1}-1)\ldots(p^{n-m+1}-1)}{(p^m-1)(p^{m-1}-1)\ldots(p-1)}.$$

3.19. Нет.

3.21.

$$C_G(x) = \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbf{C} \setminus \{0\}\right\} \simeq \mathbf{C}^* \times \mathbf{C}^*.$$

$$C_G(y) = \left\{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbf{C}^*,\ b \in \mathbf{C}\right\}.$$

$$C_G(z) = \left\{\begin{pmatrix} a & 0 & 0 \\ b & c & 0 \\ d & e & a \end{pmatrix} \in M_{3\times 3}(\mathbf{C}) \mid ac \neq 0\right\}.$$

3.24. 2):

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ c & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ c & 1 \end{pmatrix}, \begin{pmatrix} a & b \\ \dfrac{1-a^2}{b} & -a \end{pmatrix},$$

где $a, b, c \in \mathbf{C}$, $b \neq 0$.

3.38. G – циклическая π-группа с $|\pi| = 2$.

3.46. $|Z(D_{2(2n-1)})| = 1$, $|Z(D_{4n})| = 2$ при $n > 1$, $Z(D_\infty) = 1$.

3.47. 8; 6.

3.53. $G \simeq Z_p$ или $|G| = 4$.

3.54. G – циклическая группа.

3.55. G – циклическая, диэдральная или элементарная абелева 2-группа.

3.56. Решение. Пусть $G = \langle a_1, \ldots, a_n\rangle$ и $G = \langle M\rangle$, где $M \subseteq G$. Тогда для любого $i \in \{1, \ldots, n\}$ a_i есть произведение конечного числа элементов из $M \cup M^{-1}$, т. е. $a_i \in \langle M_i\rangle$, где $M_i \subseteq M$ и $|M_i| < \infty$. Поэтому $G \subseteq \langle\langle M_1\rangle, \ldots, \langle M_n\rangle\rangle = \langle M_1 \cup \ldots \cup M_n\rangle$.

3.57. В абелевой группе произведение двух элементов имеет конечный порядок $\Leftrightarrow$ порядки множителей конечны.

3.61. 4): $|\mathbf{Q}(p) : k\mathbf{Q}(p)| = k$. 5): M – максимальная подгруппа в $\mathbf{Q}(p) \Leftrightarrow M = q\mathbf{Q}(p)$, где q – простое число и $q \neq p$.

3.68. $o((a, b)) = [o(a), o(b)]$.

§ 4

4.7. Пусть $ab \in N$. Тогда последовательно получаем: $ba = (ab)^a \in N$, $a^2b^2 = (ab \cdot ba)^{a^{-1}} \in N$, $b^2a^2 = (a^2b^2)^{a^2} \in N$ и т. д., откуда a^nb^n и b^na^n принадлежат N для всех $n > 0$. Если же $m = -n$, где $n > 0$, то $a^mb^m = (b^na^n)^{-1} \in N$ и $b^ma^m = (a^nb^n)^{-1} \in N$.

4.13. $G = D_6 \supsetneq M = \{a, b\}$, где $o(a) = 2$ и $o(b) = 3$.

4.21. Нет.

4.25. Покажите, что отображение $(A / A \cap N \to AN/N \mid a(A \cap N) \mapsto aN)$ правильно определено и является изоморфизмом.

4.29. Обратное утверждение не верно.

4.35. Рассмотрите группы E_4 и D_8.

4.39. 2): $1, Z_2$ и D_{2m}, где $m \mid n$.

4.40. Все гомоморфные образы: $1, Z_2, D_{2m}$ при $m > 1$ и D_∞.

4.43. 1): Q_{16}, D_{16}.

4.45. $D(Z_{2^\infty})$.

4.46. 1): Нет. 2): Нет. 3): Нет.

4.55. $SL_n(\mathbf{C})$.

4.65. 2): 0 и $\mathbf{Q}^+$.

§ 5

5.6. Число классов сопряжённых элементов равно 4, 5, 5 соответственно.

5.8. Группы порядка 2.

5.9. $|G| = 2$.

5.14. 1): p, 2): $p^2 + p - 1$.

5.15. Да, это число равно $r/|G|$.

5.19. Используйте классовое равенство (см. введение к § 5) и 5.5(1).

5.20. G – циклическая группа.

5.29. $|G|$ равен p^2 или pq.

5.30. G имеет точно 4 класса сопряжённых подгрупп $\Leftrightarrow G \simeq Z_{p^3}$ или $|G| = pq$.

5.31. G изоморфна E_4 или Z_{pqr}, где p, q, r – различные простые числа.

5.32. 2) : $G \simeq D(H)$.

5.40. 1): Возьмите $G = S_3$.

5.41. Индекс ≤ 2.

5.49. Решение. $C_G(t) = \langle b \rangle \lambda Q$, где $H = \langle b \rangle \lambda \langle a \rangle$. Пусть $x \in N_G(Q)$. Тогда $t^x \in t^{N_G(Q)} \subseteq \{t, a, ta\}$ и по 5.5(1) $m := |t^{N_G(Q)}| = |N_G(Q) : C_{N_G(Q)}(t)| = |N_G(Q) : N_G(Q) \cap C_G(t)| = |N_G(Q) : Q|$, откуда $|N_G(Q)| = |Q| m = 4m$.

5.58. 2): Возьмите $G = S_3$.

5.62. Да.

5.68. Нет: $G = GL_2(\mathbf{Q})$, $b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}^{-1}$, $A = \langle b^2 \rangle$, $B = \langle b \rangle$. Тогда $1 = |B : A^g| \neq |B : A^g| = 2$.

5.69. $G := \langle a, b \rangle$, где $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ и $b = \begin{pmatrix} -2 & 0 \\ 0 & 2 \end{pmatrix}$.

5.70. $C_G(t) = A_2 \times \langle t \rangle$, где $A_2 := \{a \in A \mid a^2 = 1\}$. $Z(G)$ равен A_2 при $A_2 < A$ и равен G при $A_2 = A$.

5.71. б): При $n = 2k+1$: $\{1\}$, $\{a, a^{-1}\}$, $\{a^k, a^{-k}\}$, $\langle a \rangle b$. При $n = 2k$: $\{1\}$, $\{a, a^{-1}\}$, $\{a^{(k-1)}, a^{-(k-1)}\}$, $\langle a^2 \rangle b$, $\langle a^2 \rangle ab$.

в): Представители всех классов сопряжённых подгрупп: 1) при нечётном n: $\langle a^m \rangle$ при $m \mid n$ и G (нормальные), $\langle a^m \rangle \lambda \langle b \rangle$ при $m \mid n$ и $m \neq 1$ (ненормальные); 2): при чётном n: $\langle a^m \rangle$ при $m \mid n$, $\langle a^2 \rangle \lambda \langle b \rangle$, $\langle a^2 \rangle \lambda \langle ab \rangle$ и G (нормальные), $\langle a^m \rangle \lambda \langle b \rangle$ и $\langle a^m \rangle \lambda \langle ab \rangle$ при $m \mid n$ и $m > 2$ (ненормальные).

5.73. а): См. 5.72. б): $G = D_{2p^n}$, где p – нечётное простое число.

5.74. а): $n = 2(2k-1)$, $k \in \mathbf{N}$. б), в): n нечётно.

5.75. 1) $\{1\}$, $\{a^m, a^{-m}\}$ при $m \in \mathbf{N}$, $\langle a^2 \rangle b$, $\langle a^2 \rangle ab$.

2) $\{1\}$, $\langle a^m \rangle$ $m \in \mathbf{N}$, $\langle a^2 \rangle \lambda \langle b \rangle$, $\langle a^2 \rangle \lambda \langle ab \rangle$ и G.

§ 6

6.3. 2): $k\mathbf{Z}$ с $k \in \mathbf{N} \cup \{0\}$. 3): $\{0\}$, $\{1\}$, $\{1, -1\}$ ($=\mathbf{Z}^*$).

6.13. $\mathbf{Z}_6[x] \ni x^2 + x = (x-0)(x+1) = (x-2)(x-3) \neq (x-0)(x-2)$.

6.15. Пусть K состоит из n элементов $a_1, \ldots, a_n$. Для $a \in K \setminus \{0\}$ следует рассмотреть последовательности $aa_1, \ldots, aa_n$. и $a_1a, \ldots, a_na$ и учесть наличие единицы в K.

6.20. Решение. Пусть $H \leq F^*$ и $|H| < \infty$. Так как H абелева, то, по 3.8(4), H имеет элемент h порядка n такого, что все элементы из H удовлетворяют уравнению $x^n = 1$. Следовательно, по 6.10, $|H| \leq n$. Но H имеет подгруппу $\langle h \rangle$ порядка n и, значит, $H = \langle h \rangle$.

6.22. Да.

6.41. а): $\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in K \right\}$.

б): $\left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \mid A, B, C, D \in C_{M_2(K)}(x) \right\}$.

6.45. $Diag_n(\mathbf{C})$.

6.46. $\left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & e \end{pmatrix} \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbf{C}), e \in \mathbf{C}^* \right\}$.

6.45. $Diag_n(K)$.

6.51. 3): $(\{0, 2\}, \circ)$ при $K = \mathbf{Z}$ и $(\mathbf{Q}) \setminus \{1\}, \circ)$ при $K = \mathbf{Q}$.

6.52. 2): Нет.

6.57. 2): $Ker(\tilde{\varphi}) = R^{\cdot} \cap (1 + Ker(\varphi))$.

6.58. Да.

6.59. $Ker(\varphi) = m\mathbf{Z}_n = \{[0]_n, [m]_n, [2m]_n, \ldots, [(k-1)m]_n\}$, где $k = n/m$.

6.61. Ядро равно $GL_n(R) \cap (e + M_n(I))$, где e – единичная матрица.

6.62. $N = e + M_2(I)$, где e – единичная матрица и $I = p\mathbf{Z}_p{}^2$.

6.65. Это кольцо K состоит из элементов $\tilde{0} := (0, 0)$, $a := (0, 1)$, $b := (1, 0)$ и $\tilde{1} := (1, 1)$. Подкольца: $\{\tilde{0}\}$, $\{\tilde{0}, a\}$, $\{\tilde{0}, b\}$, $\{\tilde{0}, \tilde{1}\}$, K. Идеалы: $\{\tilde{0}\}$, $\{\tilde{0}, a\}$, $\{\tilde{0}, b\}$, K.

§ 7

7.2. Число циклических подгрупп порядка 2, 3 и 4 равно 9, 4 и 5, соответственно.

7.3. 6 при $n \in \{5, 6\}$, 12 при $n = 7$, 15 при $n = 8$, 20 при $n = 9$, 30 при $n = 10$.

7.6. $(n-1)!$.

7.7. a^k есть произведение (m, k) циклов равной длины.

7.14. $(a, \ldots a_k b_1 \ldots b_l)$.

7.28. $2k - 3$.

7.39. 2): $(n/2)!2^{n/2}$.

7.49. 1): 5 классов сопряжённых элементов (элементы порядка 5 образуют 2 класса).

2): В A_5 – 3 класса сопряжённых максимальных подгрупп: 4 подгруппы, изоморфных A_4; 10 подгрупп, изоморфных D_6; 6 подгрупп, изоморфных D_{10}.

7.51. $4 \leq n \leq 7$.

7.52. $\langle (1234)\,(56), (12)\,(56), (567) \rangle$.

§ 8

8.11. По условию X есть объединение t орбит $x_1^G, \ldots, x_t^G$. Пусть $M := \{(x, g) \mid x \in X, g \in G \text{ и } x^g = x\}$. Тогда $\sum\limits_{g \in G} |Fix(g)| = |M| = \sum\limits_{x \in X} |G_x| =$

$$= \sum_{x \in X} \frac{|G|}{|x^G|} = \sum_{i=1}^{t} |x_i^G| \frac{|G|}{|x_t^G|} = t|G|.$$

8.17. Нетранзитивные: подгруппы порядков 1, 2, 3, ненормальные четверные подгруппы и стабилизаторы точек ($\simeq S_3$); регулярные: циклические группы порядка 4 и нормальная четверная подгруппа; примитивные: A_4; импримитивные: силовские 2-подгруппы и нормальная четверная подгруппа.

8.18. 3): S_4.

8.21. S_n и A_n.

8.41. Расссмотрите представление группы G на смежных классах по B. Как выглядит образ инволюции из A при этом представлении?

8.46. 1): $\{1, \alpha\} \simeq Z_2$, где α – инверсия относительно данной точки. 2): $\{1, \beta\} \simeq Z_2$, где β – инверсия относительно середины отрезка $[a, b]$. 3): 1.

8.48. 1): Z_2. 2): Орбиты – окружности.

8.52. Группы симметрии изоморфны соответственно: S_3, Z_2, D_8, E_4, E_4, 1, E_4, $Z_2 \times D(T)$, $Z_2 \times D(T)$ (T – одномерный тор), Z_2.

§ 9

9.1. а): Z_{p^n}, $n \in \mathbf{N}$. б): Z_6. в): E_4.

9.2. Число бинарных факторизаций в $Q_8 - 3$, в $D_8 - 11$.

9.3. 1): $\{Z_k, Z_l\}$, где k, l – собственные делители n и $[k, l] = n$. 2): Z_k, где $k \| n$ и $(k, n/k) = 1$.

9.5. $D_6 = \langle a \rangle_3 \langle b \rangle_2$; $D_{10} = \langle a \rangle_5 \langle b \rangle_2$; $D_{30} = \langle a \rangle_{15} \langle b \rangle_2 = \langle a^3 \rangle (\langle a^5 \rangle \langle b \rangle) =$ $= \langle a^5 \rangle (\langle a^3 \rangle \langle b \rangle)(\langle a^5 \rangle \langle b \rangle \simeq D_6$, $(\langle a^3 \rangle \langle b \rangle \simeq D_{10})$; $A_4 = E\langle a \rangle$, где $E \simeq E_4$.

9.12. Нет: $G = E_4$.

9.13. $G = D_6$.

9.40. Возьмите $G = E_4$.

9.51. n нечётно.

9.52. D_∞.

§ 10

10.6. 1): Рассмотрите группу S_3. 2): Нет.

10.9. Рассмотрите действие группы S сопряжениями на множестве $Syl_p(G)$.

10.12. 48.

10.13. 4): 2, если G – циклическая, и $1 + q$, если G – нециклическая.

10.19. G изоморфна одной из групп: Z_p, Z_4, Z_6, Z_9, E_4, E_9, S_3.

10.33. а): 6, б): 21.

10.39. $n_1 n_2$.

10.45. 2): Рассмотрите группу $D_8 \times Z_2$.

§ 11

11.1. 1) – 3) и 5) – 6): φ – эндоморфизм. (φ – автоморфизм только в 3) и 6)) 4): φ – эндоморфизм $\Leftrightarrow x = 1$.

11.2. 1), 2), 4), 5): φ – эндоморфизм. (φ – автоморфизм только в 1), 4) и в 5) при $x \neq 0$).

11.7. По 11.6 $End(K^+)$ имеет подкольцо $A = \{\alpha_x \mid x \in K\}$, изоморфное кольцу K, а по 11.5 $Aut(K^+) = End(K^+)^*$. Следовательно, для указанных колец достаточно показать, что $End(K^+) \subseteq A$.

а): Пусть $K = \mathbf{Z}$. Тогда $K^+ = \langle g \rangle$ – бесконечная циклическая группа. Если $\varphi \in End(K^+)$, то $\varphi(g) = mg$ для некоторого $m \in \mathbf{Z}$. Следовательно, $\varphi : x \mapsto mx$ $(x \in K^+)$, т. е. $\varphi = \alpha_m$. Таким образом, $End(K^+) \subseteq A$.

11.8. 2): 1, Z_2, Z_2, Z_4, Z_2, Z_6, E_4, Z_6, Z_4.

11.12. 2): 6.

11.20. $|G| \leq 2$.

11.24. Пусть $D_{2n} = \langle a \rangle_n \langle b \rangle_2$. Тогда для любого автоморфизма α этой группы будет $\alpha(a) = ab^i$, где $0 \leq i \leq n-1$, и $\alpha(b) = b^j$, где $0 \leq j \leq n-1$ и $(j, n) = 1$. Отсюда легко следуют 1) и 2).

11.26. S_4.

11.37. 1): Рассмотрите группу $G = Z_2 \times A_4$.

2): Рассмотрите группу $G = D_8$.

11.44. Используйте 1.43.

§ 12

12.18. $|S_3'| = 3$, $|Q_8'| = 2$, $D_{4n}' \simeq Z_n$, $D_{2(2n+1)}' \simeq Z_{2n+1}$, $|D_\infty : D_\infty'| = 4$ и $D_\infty' \simeq \mathbf{Z}^+$. В любой из этих групп каждый элемент коммутанта является коммутатором.

12.20. $A_4' \simeq E_4$, $S_4' = A_4$.

12.25. $SL_2(\mathbf{Z}_2)' \simeq Z_3$, $SL_2(\mathbf{Z}_3)' \simeq Q_8$.

12.26. Решение. Определение μ некорректно, так как представление элемента g в виде $g = \varphi(g_1, \ldots, g_n)$ неоднозначно.

12.27. 2): Нет. Рассмотрите группу D_{16}.

12.32. 2): Нет. Рассмотрите группу Q_8.

§ 13

13.15. $G = A_4 : L_i(G) = G' \simeq E_4$ для всех $i \geq 2$, $G'' = 1$, $Z_i(G) = 1$ для всех $i \geq 1$; G не нильпотентна; $1 < G' < G$ – единственный композиционный ряд и единственный главный ряд группы G.

$G = S_4 : G' = A_4$, $G'' \simeq E_4$, $G''' = 1$, $Z_i(G) = 1$ для всех $i \geq 1$, $L_i(G) = G'$ для всех $i \geq 2$; G не нильпотентна; $1 < G'' < G' < G$ – единственный композиционный ряд и единственный главный ряд.

Q_8 имеет 3 композиционных ряда, которые все – главные.

D_8 имеет 7 композиционных рядов, из них 3 – главные.

13.16. Пусть $G = \langle a \rangle_\gamma \lambda \langle b \rangle_2$, где $\gamma \in \mathbf{N} \cup \{\infty\}$, $a^b = a^{-1}$. Во всех случаях $G' = \langle a^2 \rangle$, $G'' = 1$.

1) Если γ – нечётное число, то $Z_i(G) = 1$ для всех $i \geq 1$, $L_i(G) = G' = \langle a \rangle$ для всех $i \geq 2$.

2) Если $\gamma = 2^k$ ($k \in \mathbb{N}$), то $Z_i(G) = \langle a^{2^{k-i}} \rangle$ при $1 \leq i \leq k-1$, $Z_k(G) = G$; $L_i(G) = \langle a^{2^{i-1}} \rangle$ для всех $i \geq 2$ (= 1 при $i \geq k+1$).

3) Если $\gamma = 2^k m$, $k \geq 1$, m нечётно, $m > 1$, то $Z_i(G) = \langle a^{2^{k-i}m} \rangle$ при $1 \leq i \leq k$, $Z_i = \langle a^m \rangle = H(G)$ при $i \geq k$; $L_i(G) = \langle a^{2^{i-1}} \rangle$ при $2 \leq i \leq k+1$, $L_i(G) = \langle a^{2^k} \rangle$ при $i \geq k+1$.

Если $\gamma = \infty$, т. е. $G \simeq D_\infty$, то $Z_i(G) = 1$ при $i \geq 1$; $L_i(G) = \langle a^{2^{i-1}} \rangle$ для всех $i \geq 2$.

13.17. $G' = A$, $G'' = 1$, $Z_i(G) = \langle a_i \rangle$ для всех $i \geq 1$, $H(A) = L_i(G) = A$ для всех $i \geq 2$.

13.18. Следует из 7.46.

§ 14

14.5. 1): Пусть $n_i := n_i(G)$. Для $G = Z_2 \times Z_4$ $n_2 = 3, n_4 = 4$. Для $G = Z_2 \times Z_2 \times Z_4$ $n_2 = 7, n_4 = 8$. Для $G = Z_3 \times Z_4$ $n_2 = 1, n_4 = 2, n_3 = 2$, $n_6 = 2$, $n_{12} = 4$. Для $G = Z_p \times Z_{p^2} \times Z_{p^3}$ $n_p = p^3 - 1, n_{p^2} = p^3(p^2 - 1)$, $n_{p^3} = p^5(p-1)$. Для $G = Z_{p^m} \times Z_{p^n}$ с $m \leq n$ $n_{p^i} = p^{2i-2}(p^2 - 1)$ при $1 \leq i \leq m$ и (если $m < n$) $n_{p^{m+j}} = p^{2m+j-1}(p-1)$ при $1 \leq j \leq n-m$.

2): Число циклических подгрупп порядка i в G равно $n_i(G)/\varphi(i)$.

14.15. 2): Нет. Рассмотрите группу E_4.

14.22. 6): Рассмотрите группу E_4.

14.42. Пусть G – подпрямое произведение A и B, отличное от $A \times B$. а): При $A = \langle a \rangle$ и $B = \langle b \rangle$ $G = \{(1, 1), (a, b), (a^2, 1), a^3, b)\} \simeq Z_4$. б): $Z_4 \times Z_3$. в): G не существует. г): G не существует. д): Три группы, изоморфные $Z_4 \times Z_2$.

14.54. Пусть $G_1, \ldots, G_{n-m}$ неабелевы и $A = G_{n-m+1} \times \ldots \times G_n$ (абелева группа). Тогда любая нормальная подгруппа из G есть прямое произведение некоторых из подгрупп $G_1, \ldots, G_{n-m}$ и подгруппы из A (и обратно).

14.63. 2): Нет: первое произведение, в отличие от второго, – неупорядоченное.

§ 15

15.9. 1) $\mathbf{Z}^+ \times \mathbf{Z}^+$; 2) $G = \langle a \rangle \lambda \langle b \rangle$, $\langle a \rangle \times \langle b^2 \rangle \simeq \mathbf{Z}^+ \times \mathbf{Z}^+$ и $G/\langle b^2 \rangle \simeq D_\infty$.

15.10. 1): $\simeq Z_2$, 2): $\simeq D_6$, 3): $\simeq S_4$; 4): $\simeq D_\infty$.

15.26. 3): G абелева $\Leftrightarrow A$ и B абелевы и либо $A = 1$, либо $Ker(\mathcal{P}) = B$.

15.28. 2): $G = (\langle a_1\rangle_2 \times \langle a_2\rangle_2 \times \langle a_3\rangle_2) \lambda (\langle b\rangle_3 \lambda \langle c\rangle_2)$, где $\langle b\rangle\langle c\rangle \simeq S_3$. Силовская 2-подгруппа в G изоморфна $D_8 \times Z_2$.

15.29. 2): $G = (\langle a\rangle_4 \times \langle b\rangle_4) \lambda \langle c\rangle_2$, $a^c = b$. $Z(G) = \langle ab\rangle \simeq Z_4$.

15.40. $Z(G \wr S_n) = \left\{\left(\left(\underbrace{a,\ldots,a}_{n}\right),1\right) \mid a \in Z(G)\right\} \simeq Z(G)$.

§ 16

16.8. $\simeq Z_3$.

16.30. Нет. Рассмотрите гомоморфизм группы $G = Z_6$ на Z_2.

16.33. 2): Эта группа изоморфна $\langle a\rangle_4 \lambda_\varphi \langle b\rangle_4$, где $\varphi(b): a \mapsto a^{-1}$.

16.35. $\simeq Z_2$.

16.36. $G \simeq Z_p \wr S_2$.

16.45. $\simeq Z_5$.

16.49. $|G| = 12$, $|H| = 24$.

16.50. 2): 20.

16.51. 55.

16.52. 1): G/H изоморфна одной из следующих групп. а): E_4. б): D_{2m}, в): D_∞, г): D_∞.

§ 17

17.13. 1): $\langle a^4\rangle$, $\langle a^2\rangle$, $\langle a^2\rangle$. 2): Все элементы из $P \setminus \langle a\rangle$ имеют порядок 4. Классы сопряжённых элементов в P: $\{1\}$, $\{a^4\}$, $\{a^2, a^6\}$, $\{a, a^7\}$, $\{a^3, a^5\}$, $\langle a^2\rangle b$, $\langle a^2\rangle b^3$. 3): $\langle a\rangle, \langle a^2\rangle\langle b\rangle \simeq Q_8, \langle a^2\rangle\langle ab\rangle \simeq Q_8$. 4): 7 нормальных подгрупп. Гомоморфные образы: 1, Z_2, E_4, D_8, P. 5): 3, 1, 2.

17.14. 3): $\langle a\rangle \times \langle b^2\rangle$, $\langle a^2\rangle \times \langle b\rangle, \langle a^2\rangle \times \langle ab\rangle$.

17.15. $\Phi(P) = \Omega_1(P) = \langle a^p\rangle \times \langle b^p\rangle$.

17.18. а): P имеет точно $p + 1$ максимальных подгрупп: $\langle ab^i\rangle$ ($i \in \{1,\ldots,p-1\}$) и $\langle a^p\rangle \times \langle b\rangle$.

в): $\Omega_i(P) = \langle a^{p^{n-1-i}}\rangle \times \langle b\rangle$.

17.20. 11): 2, 2.

17.22. Следует из 1) и 17.20. 12): 2, 2.

17.23. Z_{p^n} при $n \geq 0$, E_{p^2}, Q_8.

17.24. $Z_{p^n} \times Z_p$ при $n \geq 2$, M_{p^n} при $p^n \neq 8$.

17.27. D_8, Q_8, M_{p^n} $(n \geq 3)$.

17.30. $\Omega_1(P) \subseteq Z(P) \Leftrightarrow m > 1$ и $n > 1$.

17.41. в): Группа $P = Q_8 * Z_4$ имеет точно 7 максимальных подгрупп: 3 подгруппы, изоморфных D_8, 3 подгруппы, изоморфных $Z_4 \times Z_2$, и подгруппу изоморфную Q_8. $m(P) = 2$, $r_s(P) = 3$.

17.47. Группа $P = D_8 * D_8$ имеет 10 максимальных подгрупп, изоморфных $D_8 * Z_4$ $(\simeq Q_8 * Z_4)$, и 5 максимальных подгрупп, изоморфных $Q_8 \times Z_2$; $m(P) = 2$, $r_s(P) = 4$.

Группа $P = D_8 * Q_8$ имеет 6 максимальных подгрупп, изоморфных $Q_8 * Z_4$ и 9 максимальных подгрупп, изоморфных $D_8 \times Z_2$; $m(P) = 3$, $r_s(P) = 4$.

§ 18

18.5. См. [15, 5.2.4].

18.8. 4): Если C – искомая подгруппа, то при $p = 2$ $C = Aut(P)$, а при $p > 2$ $C = \langle \alpha \rangle$, где α – автоморфизм порядка p^{n-1} такой, что $x^{\alpha} = x^{1+p}$.

18.12. $\simeq D_8$.

18.35. См. [15, 5.3.10].

18.40. 1): Доопределите P до векторного пространства над $\mathbf{Z}_p$.

§ 19

19.8. g – скалярная.

19.14. Порядки групп: 72, 36.

19.16. 3): G имеет точно 3 класса максимальных подгрупп: 5 2-замкнутых подгрупп порядка 24, 10 3-замкнутых подгрупп порядка 12, 6 5-замкнутых подгрупп порядка 20.

19.17. $Diag_2(q)$, $UT_2(q) \times Z(G)$.

19.19. 2): Число инволюций равно $q^2 - 1$ при чётном q и равно $q^2 + q + 1$ при нечётном q.

19.23. Число силовых p-подгрупп равно $p^m + 1$.

19.27. 2): $UT_3(q) \lambda D$, где $D \simeq Z_{q-1} \times Z_{q-1}$. 3): $\{t_{31}(a) \mid a \in \mathbf{F}_q\}$.

19.30. $C_G(H) = Diag_3(q)$, $C_G(H) \cap SL_3(q) \simeq Z_{q-1} \times Z_{q-1}$.

19.35. $\simeq GL_{n-1}(q)$.

19.36. $\simeq F^+$.

19.55. Используйте 19.51(1).

§ 20

20.1. См. [15, 6.2.1] или [16, I. 18.1 и I.18.2].

20.2. См. [15, гл. 6] или [16, гл. VI].

20.26. 2-длина равна 2, 2, 2, 1 соответственно. Подгруппы Картера: в первых трёх группах – силовские 2-подгруппы; в группе D_∞ – подгруппы порядка 2.

20.32. $l_2(G) \le 2$.

20.41. 2): $O_\pi(G) \times O_{\pi'}(G)$.

20.47. 2): $G = A_4 \times S_3$.

§ 21

21.6. Рассмотрите группу D_8.

21.25. Не сохранится: рассмотрите группу $Z_2 \times A_5$.

21.41. 2): $G = S_4$, $B = \langle a \rangle_4 \lambda \langle b \rangle_2 \in Syl_2(G)$, $A = \langle a \rangle$, $H = A_4$.

21.42. 2): $G = S_4$, $B = \langle a \rangle_4 \lambda \langle b \rangle_2 \in Syl_2(G)$, $A = \{a, a^{-1}\}$.

§ 22

22.28. $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \bar{\varepsilon} \\ 1 & \bar{\varepsilon} & \varepsilon \end{pmatrix}$ $\left(\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$, $\begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 2 & 0 & -1 \end{pmatrix}$,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 \\ 1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 \end{pmatrix}.$$

22.29. Примените 22.22.

22.34. $(\chi, \chi) = \chi(1)^2 \Leftrightarrow \chi(1) = 1$.

22.35. Рассмотрите таблицу характеров группы S_3 (22.28).

22.44. 5): К обеим частям равенства пункта 3) примените функцию ω_χ из 22.41. Обе части полученного равенства умножьте на $\chi(1)\overline{\chi(g_m)}$ и просуммируйте по $\chi \in Irr(G)$, используя 22.24.

22.50. 2): Равенство имеет место $\Leftrightarrow \psi \in Irr(G)$, $Irr(\chi)\psi \subseteq Irr(G)$ и $|Irr(\chi)\psi| = = Irr(\chi)$.

22.65. С помощью 22.59 докажите, что $\chi(X) = \{\chi(g)^\alpha | \alpha \in Aut(\mathbb{Q}(\omega))\}$ и что отсюда следует первое неравенство. Второе неравенство следует из первого и того факта, что среднее арифметическое нескольких вещественных чисел не меньше их среднего геометрического.

22.71. Примените 22.33 и 14.20.

22.75. $a_\chi = \sum_{i=1}^{k} \chi(g_i)$, где $g_1, \ldots, g_k$ – представители всех классов сопряжённых элементов группы G. Сумма всех элементов любой строки таблицы характеров – целое неотрицательное число.

22.80. 1): $Ker(\mathcal{A}_T^G) = Ker(\mathcal{A})_G$.

23.2. Используйте 3.16.

23.3. Используйте 23.1 и 23.2.

23.5. 1): Это – 21.28. 2): G имеет максимальную подгруппу вида $M = \langle a\rangle \times Q_1$, где $Q_1 \leq Q$, причём M – единственная максимальная подгруппа в G, содержащая $\langle a\rangle$. Следовательно, Q_1 содержит каждую $\langle a\rangle$-инвариантную подгруппу из Q и, в частности, $Q_1 \supseteq \Phi(Q)$. Обратное включение следует из теоремы Машке (18.40). 4): Используйте 23.3. 6): Достаточно рассмотреть случай, когда Q абелева. Предположим, что $\Phi(Q) \neq 1$. Тогда $\Omega(Q) \cup \mho(Q) \subseteq \Phi(Q) \subseteq Z(G)$. Покажите, что $t := [g, a]$ имеет порядок q и, следовательно, $t \in Z(G)$. Но тогда $g^2 = gt$, $g^{a^2} = gt^2, \ldots, g = g^{a^p} = gt^p$, откуда $t^p = 1$, что противоречиво.

23.8. Используйте 23.5 и 21.27.

23.12. Либо G – группа Шмидта, либо $G \simeq Z_p \times S$, где S – p'-группа Шмидта.

23.15. G либо p-замкнута, либо – p'-замкнутая группа Шмидта.

23.19. Если G не нильпотентна и не группа Шмидта, то либо $G = \langle a\rangle_{p^2} \leftthreetimes Q$, где $\langle a^p\rangle \leftthreetimes Q$ – группа типа A, либо $G = \langle a\rangle_p \leftthreetimes Q$, где $|Q| = pq^{2b}$ и $\langle a\rangle \leftthreetimes \Phi(Q)$ и $G/\Phi(G)$ – группы типа A порядка pq^b.

23.28. $G = Z(G)S$, где S – подгруппа Шмидта.

23.29. Циклические группы порядка p^n или pq.

23.30. Циклические группы.

23.33. 2): $G = D_{18}$, $N \simeq Z_3$.

23.35. а): Циклические группы. б): Абелевы группы. в): Нильпотентные группы.

23.39. Циклические группы порядка p^2 или pq, группа Фробениуса $\langle a\rangle_p \leftthreetimes Q$ с ядром Q, каждая неединичная подгруппа которого имеет простой порядок и нормальна в G.

23.40. Циклические группы, p-группы с циклической максимальной подгруппой, группы Миллера–Морено с нормальной силовской подгруппой простого порядка.

23.41. $G \simeq D(A)$, где $|A|$ нечётен.

23.46. Используйте 21.28, 21.34 и 21.34. $l_2(G) \leq 2$.

23.47. Используйте 21.22, 21.26 и 21.31(2). $l_2(G) \leq 2$.

23.48. Либо $|G| = pq$, либо G изоморфна Z_{p^n}, E_{p^2} или Q_8.

23.49. а): G изоморфна Z_3 или S_3. б): G изоморфна Z_4, E_4, A_4 или D_{10}.

23.50. См. [15, 9.1.6].

23.52. Используйте 13.64, 20.7 и 20.10.

23.54. Используйте 23.53.

Список обозначений и терминов

§ 1

бинарная операция 7
группа 7
нейтральный элемент 7
симметричный элемент 7
порядок группы 7
абелева или коммутативная группа 7
единичный элемент или единица группы 7
обратный элемент 7
нулевой элемент или нуль абелевой группы 8
противоположный элемент абелевой группы 8
степень элемента 8
периодический элемент 8
порядок или период элемента 8
инволюция 8
циклическая группа 8
изоморфизм групп 8
перестановка множества 8
группа перестановок 8
симметрическая группа S_X 8
полугруппа 9
квазигруппа 9
группы $\mathbf{C}^+$, $\mathbf{R}^+$, $\mathbf{Q}^+$ 11
группы $\mathbf{C}^*$, $\mathbf{R}^*$, $\mathbf{Q}^*$ 11
одномерный тор 12
группа Z_n 12
таблица умножения группы 12
теорема Кэли 13
(внешнее) прямое произведение групп 14
четверная группа 14
группа $D(A)$ 16
обобщённо диэдральная группа 16
группы $GL_n(\mathbf{R})$, $SL_n(\mathbf{R})$, $GL_n(\mathbf{C})$, $SL_n(\mathbf{C})$ 16
идемпотент 17

§ 2

подгруппа 18
единичная подгруппа 18
$\langle a \rangle$ 18
истинная подгруппа 18
собственная или нетривиальная подгруппа 18
максимальная подгруппа 18
взаимно простые подгруппы 18
Hg, правый смежный класс 18
$G : H$ 18
$|G : H|$ 18
индекс подгруппы 18
правая система вычетов группы по подгруппе 18
сопряжённые подгруппы 18
двойные смежные классы 18
$|A| \leq |B|$ 18
$|A|$ **делит** $|B|$ 18
подполугруппа 19
теорема Лагранжа 20
закон Дедекинда 21
группа кватернионов Q_8 22
точное произведение подмножеств группы 23
группа Z_{p^∞} 25
квазициклическая p**-группа** 25
группа типа p^∞ 25

§ 3

порождающее множество группы 26
$C_G(g)$ 26
централизатор элемента 26
$Z(G)$ 26
центр группы 26
π-элемент 26
π-группа 26
p-элемент 26
p-группа 26

примарный элемент 26
силовская p-подгруппа 26
элементарная абелева p-группа 26
сопряжённые элементы 26
D_{2n} 26
диэдрвльная группв 26
группа D_∞ 26
бесконечная диэдральная группа 26
группа p-ичных дробей $\mathbf{Q}(p)$ 26
порядок элемента относительно подгруппы 34
$o(a; H)$ 34

§ 4

нормальная подгруппа 36
$H \trianglelefteq G$ 36
минимальная нормальная подгруппа 36
простая группа 36
(внутреннее) прямое произведение 36
полупрямое произведение подгрупп
$N_G(M) := \{ g \in G \mid Mg = gM \}$ 36
нормализатор подмножествв в группе 36
G/H 36
фактор-группа 36
гомоморфизм группы 36
образ гомоморфизмв 37
$Ker(\varphi)$ 37
ядро гомоморфизма 37
собственный гомоморфный обрвз 37
эпиморфизм 37
мономорфизм 37
тривиальный гомоморфизм 37
секция группы 37
$Hom(G, H)$ 37
$\simeq \leq$ 37
теорема о гомоморфизмах 40
естественный гомоморфизм 40

§ 5

сопряжённые элементы 45
a^G 45
класс сопряжённых элементов 45
первая теорема Силовв 45
нормальное подмножество группы 45
сердцевина подгруппы 45
сопряжённые подмножества 45
X^a 45
класс сопряжённых подмножеств 45
$\{X\}^G$ 45
X^Y 45
сильно звмкнутое подмножество подгруппы 50

§ 6

кольцо 55
K^+ 55
аддитивная группа кольца 55
единица кольца 55
обратимый элемент кольца 55
K^* 55
мультипликативная группа кольца 55
делитель нуля 55
поле 55
характеристика поля 55
$char(K)$ 55
гомоморфизм кольцв 55
идеал кольца 55
фактор-кольцо 55
подкольцо 55
скалярнвя мвтрицв 56
векторное прострвнство 56
$dim(V)$ 56
линейный опервтор 56
эндоморфизм векторного прострвнствв 56
мвтрицв операторв 56
мвтрнцв α_B 56
$V(n, F)$ 56
алгебрв 57
поля $\mathbf{C}, \mathbf{R}, \mathbf{Q}$ 57
кольцо $\mathbf{Z}$ 57
кольцо p-целых рациональных чисел 57
кольцо $K[x]$ 57
кольцо $\mathbf{Z}_n$ 58
кольцо вычетов по модулю n 58
кольцо $M_n(K)$ 59
группв $GL_n(K)$ 59
группа $SL_n(K)$ 59
диагональная подгруппа 60
$Diag_n(K))$ 60
$T_n(K))$ 60
треугольная подгруппа 60
$UT_n(K))$ 60
уннтреугольная подгруппа 60
ортогональная подгруппа $O_n(K))$ 60
кольцо кватернионов 61

кольцо H 61
трансвекции 63
присоединённая группой кольца 63
прямая сумма колец 65
i_B 65
естественный изоморфизм $GL(V)$ на $GL_n(F)$ 65
теорема Машке 65
прямая сумма подпространств 66
FG 66
групповое кольцо 66
групповая алгебра 66

§ 7

цикл (длины m) 67
транспозиция 67
независимые циклы 67
цикл длины 1 67
циклические компоненты перестановки 67
(циклический) тип перестановки 67
нечётная перестановка 68
чётная перестановка 68
знак перестановки 68
$sign(g)$ 68
знакопеременная группа 68
A_X 68
A_n 68
инверсия перестановки 71
глобальный стабилизатор 71
поточечный стабилизатор 71
подгруппа Юнга 71
группа симметрий многочлена 73

§ 8

группа перестановок 75
степень группы перестановок 75
стабилизатор точки 75
поточечный стабилизатор 75
глобальный стабилизатор 75
орбита группы 75
$Fix(g)$ 75
стабилизатор двух точек 75
транзитивная группа 75
интранзитивная группа 75
группа действует на множестве 75
регулярная группа 75
k-транзитивная группа 75
k-кратно транзитивная группа 75
разбиение множества 75
система импримитивности 75
импримитивная группа 76
примитивная группа 76
представление группы перестановками 76
группа действует на множестве посредством гомоморфизма 76
степень представления перестановками 76
точное представление группы перестановками 76
транзитивное представление группы перестановками 76
представление группы сдвигами 76
группа действует сдвигами 76
группа действует сопряжениями 76
подобные группы перестановок 76
эквивалентные представления перестановками 76
движение пространства 76
изометрия пространства 76
эвклидова группа $E(n)$ 76
группа симметрий фигуры 77
(правое) регулярное представление группы 79
левое регулярное представление группы 79
представление группы перестановками смежных классов 79
аффинная группа прямой 82
группа вращений фигуры 83
n-угольный диэдр 83

§ 9

факторизация группы 84
бинарная факторизация группы 84
дополнение подгруппы 84
группа Фробениуса 84
ядро группы Фробениуса 84
дополнительный множитель группы Фробениуса 84
нормальный множитель группы Фробениуса 84
дедекиндова группа 89
лемма Кегеля 90

§ 10

p-силовская подгруппа 91
силовская подгруппа 91
$Syl_p(G)$ 91
максимальное p-силовское пересечение 91
$O_p(G)$ 91
примарная группа 91
бипримарная группа 91
π-число 91
π-замкнутая группа 91
p-замкнутая группа 91
холлова подгруппа 91
π-холлова подгруппа 91
теорема Силова 92
аргумент Фраттини 93
p-сигнализатор 98

§ 11

эндоморфизм группы 99
автоморфизм группы 99
$End(G)$ 99
группа $Aut(G)$ 99
внутренний автоморфизм группы 99
$Inn(G)$ 99
группа внутренних автоморфизмов группы 99
группа внешних автоморфизмов группы 99
$Out(G)$ 99
совершенная группа 99
регулярный автоморфизм 99
φ-инвариантная подгруппа 99
φ-допустимая подгруппа 99
индуцированный эндоморфизм 99
характеристическая подгруппа 99
характеристически простая группа 99
нормальный автоморфизм 99
кольцо $End(A)$ 100
автоморфизм кольца 100
операторная группа 100
Ω-группа 100
определяющее отображение Ω-группы 100
Ω-подгруппа 100
Ω-допустимая подгруппа 100
Ω-гомоморфизм 100
$Hom_\Omega(G, H)$ 100
$C_A(M/N)$ 100
индуцированный эндоморфизм фактор-группы 103
автомизатор подгруппы в группе 103
центральный автоморфизм 104
n-абелева группа 105

§ 12

коммутатор 107
коммутант 107
G' 107
взаимный коммутант 107
$[A, B]$ 107
лемма о трех подгруппах 107

§ 13

ряд подгрупп 113
субнормальный ряд 113
нормальный ряд 113
композиционный ряд 113
главный ряд 113
центральный ряд 113
факторы ряда 113
индексы ряда 113
субнормальная подгруппа 113
$H \trianglelefteq\trianglelefteq G$ 113
разрешимая группа 113
ступень разрешимости группы 113
сверхразрешимая группа 113
нильпотентная группа 114
класс нильпотентности группы 114
$G^{(n)}$ 114
n-й коммутант группы 114
$Z_n(G)$ 114
n-й центр группы 114
$L_n(G)$ 114
n-й централ группы 114
гиперцентр группы 114
$H(G)$ 114
$Z_\infty(G)$ 114
расширение группы 114
разрешимый радикал $S(G)$ группы 114
$S(G)$ 114
подгруппа Фиттинга 114
$F(G)$ 114
подгруппа Фраттини 114
$\Phi(G)$ 114
уплотнение ряда 114
изоморфные ряды 114
Θ-инвариантный ряд группы 114

Θ-допустимый ряд группы 114
автоморфизм стабилизирует ряд 114
автоморфизм централизует ряд 114
$exp\,(G)$ 114
теорема Фейта–Томпсона 115
теорема Шрайера 115
теорема Жордана–Гёльдера 115
ряд коммутантов 116
возрастающая центральная цепь 116
убывающая центральная цепь 116
силовский ряд группы 121

§ 14

прямое произведение подгрупп 122
$G_1 \times \ldots \times G_n$ 122
$\prod_{i=1}^{n} G_i$ 122
прямое произведение групп 122
внутреннее прямое произведение 122
внешнее прямое произведение 122
$G_1 \hat{\times} \ldots \hat{\times} G_n$ 122
прямое произведение бесконечного числа множителей 122
декартово произведение групп 122
прямая сумма 122
центральное произведение подгрупп 123
центральное пронзведенне групп 123
φ-центральное пронзведение групп 123
$A *_\varphi B$ 123
проектирование относительно данного прямого разложенння группы 123
проекция подгруппы 123
компонента подгруппы 123
подпрямое произведение групп 123
ψ-подпрямое произведение групп 129
подпрямое произведение групп с объединенными фактор-группами 129
цоколь группы 130
$Soc(G)$ 130
теорема Крулля–Ремака–Шмидта 132
условие минимальности 132
условне максимальности 132
$\times_{i \in I} G_i$ 133
$\overline{\times}_{i \in I} G_i$ 134
$SU(n)$ 134

§ 15

$A \lambda_\varphi B$ 135
декартово произведение групп 135
полупрямое произведение групп 135
канонические вложенння множителей полупрямого произведения 135
$Hol(G)$ 135
голоморф группы 135
сплетение групп 135
$\mathcal{P}$-сплетенне групп 135
$A \wr_\varphi B$ 135
декартово сплетение групп 135
$A \bar{\wr}_\varphi B$ 135
база сплетения 135
$A \wr B$ 136
сплетение подгрупп 136
$A \wr' B$ 136
полуцентральное произведение 138

§ 16

свободная группа 142
свободное порождающее множество группы 142
ранг свободной группы 142
слово над алфавнтом X 142
X-слово 142
длина слова 142
эквивалентные слова 143
$a \sim_W b$ 143
соотношение над X 143
X-соотношенне 143
выводнмость соотношения 143
следствие соотношенй 143
эквивалентность соотношений 143
значение слова в группе 143
соотношение выполнено в группе 143
соотношение справедливо в группе 143
определяющее множество соотношений 143
$G = \langle X \mid R \rangle$ 143
$\mathcal{W}(X)$ 143
$\mathcal{R}(X)$ 143
$\mathcal{W}_R$ 143
$[a]_W$ 143
$\langle X \parallel W \rangle$ 143
$\langle X \parallel R \rangle$ 143
$\sim_R$ 143
$[a]_R$ 143

$Grp(X : W)$ 144
$\sim$ 144
$[a]$ 144
сократимое слово 144
$F(X)$ 144
$\langle x_1, \ldots, x_m \| w_1, \ldots, w_n \rangle$ 144
порождающее представление группы 144
генетический код группы 144
теорема Дика 147

§ 17

$\langle g \rangle_n$ 151
$cl(P)$ 151
$d(P)$ 151
$m(P)$ 151
ранг p-группы 151
$r_s(P)$ 151
секционный ранг p-группы 151
$\Omega_i(J_i(P)$ 151
нижний слой p-группы 151
$\mho_i(P)$ 151
$\mathcal{A}(P)$ 151
$J(P)$ 151
подгруппа Томпсона 151
$SCN(P)$ 151
$SCN_m(P)$ 151
регулярная p-группа 151
специальная p-группа 151
экстраспециальная p-группа 151
p-группа максимального класса 151
M_{p^n} 152
полуабелева p-группа 152
модулярная p-группа 152
SD_{2^n} 152
полудиэдральная группа 152
Q_{2^n} 152
кватернионная группа 152
обобщённая группа кватернионов 152
$E(p)$ 152
группа Миллера–Морено 152
гамильтонова группа 152
$A * B$ 152

§ 18

гомоциклическая группа 162
$A \times B$-лемма Томпсона 164
теорема Гашютца 165
теорема Машке для групп 165

§ 19

$GL(V)$ 167
$det(\alpha)$ 167
$SL(V)$ 167
$PGL_n(F)$ 167
проективная общая линейная группа 167
$PSL_n(F)$ 167
проективная специальная линейная группа 167
прямая 167
гиперплоскость 167
$PGL(V)$ 167
$PSL(V)$ 167
$GL_n(q)$ 167
$SL_n(q)$ 167
$PGL_n(q)$ 167
$PSL_n(q)$ 167
$T_n(q)$ 167
$UT_n(q)$ 167
$Diag_n(q)$ 167
$L_n(q)$ 167
цикл Зингера 168
трансвекция 169
симплектическая группа 173
$Sp_{2n}(K)$ 173
группа формы f 174
комплексная унитарная группа 174
$U(n)$ 174
$SU(n)$ 174
$GU_n(q)$ 174
общая унитарная группа 174
$GU(n, q^2)$ 174
аффинное преобразование векторного пространства 174
$AGL_n(F)$ 174
аффинная группа 174
$AGL(n, q)$ 174

§ 20

$\pi(H)$ 176
π' 176
$O_\pi(G)$ 176
$O_{\pi,\pi'}(G)$ 176
$O^\pi(G)$ 176

π-отделимая группа 176
π-разрешимая группа 176
π-разложимая группа 176
π-скованная группа 176
π-длина группы 176
$l_\pi(G)$ 176
подгруппа Картера 176
абнормальная подгруппа 176
пронормальная подгруппа 176
TI-подгруппа 176
теорема Шура–Цассенхауза 177

§ 21

перенос G в H/K 183
$V_{X\to Y/Z}$ 183
слабо замкнутое подмножество 183
сильно замкнутое подмножество 183
экстремальный элемеит 183
p-нильпотентная группа 183
p-нормальная группа 183
группа Шмидта 183
$Cl(X)$ 184
теорема Бернсайда о нормальном p-дополнении 185
1-я теорема Грюна 186
2-я теорема Грюна 186
теорема Фробениуса о нормальном p-дополнении 186
теорема Томпсона о нормальном p-дополнении 187

§ 22

представление группы над полем 190
степень представления 190
матричное представление 190
операторное представлеиие 190
точное представление 190
матричная интерпретацня представления 190
операторная интерпретация представления 190
эквивалентные представления 190
$A \approx B$ 190
классы эквивалентных представлений 190
приводимое представление 190
разложимое представлеиие 190
фактор представлення 190
$A_{U/W}$ 190
характер представления 191
χ_A 191
единичное представление 191
$Z(FG)$ 191
регулярное представление 191
$Reg_{G,F}$ 191
координатные функции представления 191
классовые функции группы 191
обыкновеиное представление 191
модулярное представление 191
характер группы 191
неприводимый характер группы 191
степень характера 191
ядро характера 191
классовые функции группы 191
обобщенный характер группы 191
главный характер 192
$Irr(G)$ 192
$CF(G)$ 192
скалярное произведение 192
таблица характеров 192
D-срезка 192
$\psi|_D^0$ 192
взаимодействие 192
$D \leftarrow\!\!\rightarrow \Phi$ 192
D-блок группы 192
Ф-блок группы 192
вктивный фрвгмент таблицы харвктеров 192
актнвный фрагмент группы 192
индуцированное представление 192
индуцированная классовая функция 192
прямая сумма представлений 192
$A_1 \oplus \ldots \oplus A_n$ 193
тензорное произведение представлений 194
$A \otimes B$ 194
$M^\dagger$ 194
контрградиентное представление 194
лемма Шура 195
пространство координатных функций 195
критерий неприводимости Берисайда 195
теорема Фробениуса–Шура 196
первое соотношение ортогональности 196

второе соотношение ортогональности 196
линейный характер 197
регулярный характер группы 198
вещественный элемент группы 198
комплексно сопряжённые классовые функции 198
алгебраическое число 199
целое алгебранческое число 199
$\hat{\mathbf{Q}}$ 199
$\hat{\mathbf{Z}}$ 199
$det\chi$ 200
алгебранчески сопряжённые характеры 201
теорема Бернсайда 202
$p^{\alpha}q^{\beta}$-теорема Бернсайда 203
группа характеров 203
характер представления перестановками 204
индуцированное представление 205
индуцированная классовая функция 205
индуцированный характер 206
звкон взаимности Фробеннуса 206
теоремв Фробениуса 206

§ 23

pd-группа 210
πd-группа 210
изоордные группы 210
класс изоордных подгрупп 210
класс подгрупп 210
2-максимальная подгруппа 210
группа типа A 210
группа Миллера–Морено 210
инцидентные подгруппы 215
теорема Бэра–Судзуки 216

Литература

1. *Белоногов В. А., Фомин А. Н.* Матричные представления в теории конечных групп. М.: Наука, 1976. 126 с.

2. *Белоногов В. А.* Представления и характеры в теорни конечных групп. Свердловск: УрО РАН, 1990. 379 с.

3. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп. М.: Наука, 1977. 239 с.

4. *Кострикин А. И.* Введение в алгебру. М.: Наука, 1977. 495 с.

5. *Курош А. Г.* Теория групп. 3-е изд. М.: Наука, 1967. 648 с.

6. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр. М.: Наука, 1969. 668 с.

7. *Ляпин Е. С., Айзенштат А. Я., Лесохин М. М.* Упражнения по теории групп. М.: Наука, 1967. 264 с.

8. Сборнпк задач по алгебре / Под ред. А. И. Кострикнна. М.: Наука, 1987. 351 с.

9. *Супруненко Д. А.* Группы матрнц. М.: Наукв, 1972. 351 с.

10. *Холл М.* Теория групп. М.: Изд-во иностр. лит., 1963. 468 с.

11. *Шмидт О. Ю.* Абстрактная теория групп // Шмидт О.Ю. Избрвнные труды: Математнка. М.: Изд-во АН СССР, 1959. С. 17–175.

12. *Burn R. P.* Groups: A path to geometry. N.Y.: Cambridge Univ. Press, 1991. 249 с.

13. *Dixon J. D.* Problems in group theory. N.Y.: Braisdell, 1973. 176 с.

14. *Feit W., Thompson J. G.* Solvвbility of groups of odd order // Pвcif. J. Mвth. 1963. Vol. 13. P. 775–1029.

15. *Gorenstein D.* Finite groups. N.Y.: Harper and Row, 1968. 527 с.

16. *Huppert B.* Endliche Gruppen. I.B.: Springer, 1967. 793 с.

17. *Isaacs I. M.* Character theory of finite groups. N.Y.: Acad. press, 1976. 303 с.

18. *Neumann P. M., Stoy G. A., Thompson E. C.* Groups and geometry. Oxford: Oxford Univ. press, 1994. 254 с.

Белоногов Вячеслав Александрович

ЗАДАЧНИК ПО ТЕОРИИ ГРУПП

Учебное пособие

Зав. редакцией *А.А. Фролова*
Редактор *Т.А. Никитина*
Художественный редактор *Г.М. Коровина*
Технический редактор *О.В. Аредова*
Корректоры *Г.В. Дубовицкая*, *Т.И. Шеповалова*

Набор и верстка выполнены в издательстве на компьютерной технике

ЛР № 020297 от 23.06.1997

Подписано к печати 27.06.2000
Формат 60×90 1/16. Гарнитура Таймс
Печать офсетная
Усл. печ. л. 15,0. Усл. кр.-отт. 15,0. Уч.-изд. л. 14,82
Тираж 1000 экз. Тип. зак. 500

Издательство "Наука"
117864 ГСП-7, Москва В-485, Профсоюзная ул., 90

ППП "Типография "Наука"
121099, Москва, Шубинский пер., 6

ISBN 5-02-002533-X