

УДК 512 (075.8)

ББК 22.143

К 71

Кострикин А. И. Введение в алгебру. Часть III. Основные структуры: Учебник для вузов. — 3-е изд. — М.: ФИЗМАТЛИТ, 2004. — 272 с. — ISBN 5-9221-0489-6.

Алгебраические структуры, известные из первых двух частей учебника (группы, кольца, модули), изучаются на несколько более высоком уровне. Идеи и результаты теории представлений, подкрепленные многочисленными примерами, придают всему изложению общематематическое звучание. Особое место занимают конечно порожденные абелевы группы, теоремы Силлова, представления и характеристики конечных групп, алгебры над классическими полями. Имеются теоретико-числовые приложения. В заключительной главе изложены основы теории Галуа.

Второе издание — 2001 г.

Для студентов младших курсов университетов и вузов с повышенными требованиями по математике.

Ил. 6.

© ФИЗМАТЛИТ, 2000, 2001, 2004

© А. И. Кострикин, 2000, 2001

ISBN 5-9221-0489-6

# ОГЛАВЛЕНИЕ

ПРЕДИСЛОВИЕ . . . . .	7
-----------------------	---

## ГЛАВА 1 ТЕОРЕТИКО-ГРУППОВЫЕ КОНСТРУКЦИИ

§ 1. Классические группы малых размерностей . . . . .	9
1. Общие определения (9). 2. Параметризация групп $SU(2)$ , $SO(3)$ (10). 3. Эпиморфизм $SU(2) \rightarrow SO(3)$ (12). 4. Геометрическое изображение группы $SO(3)$ (14). 5. Кватернионы (14). Упражнения (18).	
§ 2. Смежные классы по подгруппе . . . . .	19
1. Элементарные свойства (19). 2. Строение циклических групп (22). Упражнения (23).	
§ 3. Действие групп на множествах . . . . .	23
1. Гомоморфизмы $G \rightarrow S(\Omega)$ (23). 2. Орбиты и стационарные подгруппы точек (24). 3. Примеры действий групп на множествах (26). 4. Однородные пространства (30). Упражнения (31).	
§ 4. Факторгруппы и гомоморфизмы . . . . .	32
1. Понятие о факторгруппе (32). 2. Теоремы о гомоморфизмах групп (33). 3. Коммутант (37). 4. Произведения групп (39). 5. Образующие и определяющие соотношения (41). Упражнения (45).	

## ГЛАВА 2 СТРОЕНИЕ ГРУПП

§ 1. Разрешимые и простые группы . . . . .	48
1. Разрешимые группы (48). 2. Простые группы (50). Упражнения (54).	
§ 2. Теоремы Силова . . . . .	54
Упражнения (59).	
§ 3. Конечно порождённые абелевы группы . . . . .	60
1. Примеры и предварительные результаты (60). 2. Абелевы группы без кручения (61). 3. Свободные абелевы группы конечного ранга (64). 4. Строение конечно порождённых абелевых групп (66). 5. Другие подходы к проблеме классификации (67). 6. Основная теорема о конечных абелевых группах (71). Упражнения (74).	

§ 4. Линейные группы Ли . . . . .	74
1. Определения и примеры (74). 2. Кривые в матричных группах (76). 3. Дифференциал гомоморфизма (78). 4. Алгебра Ли группы Ли (79). 5. Логарифм (81). Упражнения (82).	

## ГЛАВА 3

**ЭЛЕМЕНТЫ ТЕОРИИ ПРЕДСТАВЛЕНИЙ**

§ 1. Определения и примеры линейных представлений . . . . .	86
1. Основные понятия (86). 2. Примеры линейных представлений (91). Упражнения (95).	
§ 2. Унитарность и приводимость . . . . .	96
1. Унитарные представления (96). 2. Полная приводимость (99). Упражнения (102).	
§ 3. Конечные группы вращений . . . . .	102
1. Порядки конечных подгрупп в $\text{SO}(3)$ (103). 2. Группы правильных многогранников (105). Упражнения (108).	
§ 4. Характеры линейных представлений . . . . .	109
1. Лемма Шура и её следствие (109). 2. Характеры представлений (111). Упражнения (116).	
§ 5. Неприводимые представления конечных групп . . . . .	117
1. Число неприводимых представлений (117). 2. Степени неприводимых представлений (119). 3. Представления абелевых групп (121). 4. Представления некоторых специальных групп (123). Упражнения (125).	
§ 6. Представления групп $\text{SU}(2)$ и $\text{SO}(3)$ . . . . .	127
Упражнения (130).	
§ 7. Тензорное произведение представлений . . . . .	131
1. Контрагредиентное представление (131). 2. Тензорное произведение представлений (132). 3. Кольцо характеров (133). 4. Инварианты линейных групп (136). Упражнения (140).	

## ГЛАВА 4

**КОЛЬЦА И МОДУЛИ**

§ 1. Теоретико-кольцевые конструкции . . . . .	142
1. Идеалы колец и факторкольца (142). 2. Поле разложения многочлена (144). 3. Теоремы об изоморфизме колец (147). Упражнения (149).	
§ 2. Отдельные результаты о кольцах . . . . .	150
1. Целые гауссовые числа (150). 2. Каноническое разложение суммы двух квадратов (152). 3. Полиномиальные расширения факториальных колец (153). 4. Строение мультиплекативной группы $U(Z_n)$ (154). Упражнения (158).	

§ 3. Модули . . . . .	159
1. Первоначальные сведения о модулях (159). 2. Свободные модули (163). 3. Целые элементы кольца (166). Упражнения (167).	
§ 4. Алгебры над полем . . . . .	168
1. Определения и примеры алгебр (168). 2. Алгебры с делением (тела) (170). 3. Групповые алгебры и модули над ними (174). Упражнения (183).	
§ 5. Неприводимые модули над алгеброй Ли $\mathfrak{sl}(2)$ . . . . .	184
1. Исходный материал (184). 2. Веса и кратности (186). 3. Старший вектор (186). 4. Классификационный результат (187). Упражнения (188).	

## ГЛАВА 5

## НАЧАЛА ТЕОРИИ ГАЛУА

§ 1. Конечные расширения полей . . . . .	190
1. Примитивные элементы и степени расширений (190). 2. Изоморфизм полей разложения (194). 3. Существование примитивного элемента (196). Упражнения (198).	
§ 2. Конечные поля . . . . .	198
1. Существование и единственность (198). 2. Под поля и автоморфизмы конечного поля (200). 3. Формула обращения Мёбиуса и её применения (201). Упражнения (206).	
§ 3. Соответствие Галуа . . . . .	207
1. Предварительные результаты (207). 2. Фундаментальное соответствие Галуа (210). 3. Иллюстрации к соответствию Галуа (211). Упражнения (215).	
§ 4. Вычисление группы Галуа . . . . .	215
1. Действие группы $\text{Gal}(f)$ на корнях многочлена $f$ (215). 2. Многочлены и группы простой степени (217). 3. Метод приведения по модулю $p$ (219). 4. Нормальный базис (224). Упражнения (227).	
§ 5. Расширения Галуа и смежные вопросы . . . . .	228
1. Простые числа в арифметической прогрессии (228). 2. Расширения с абелевой группой Галуа (229). 3. Норма и след (230). 4. Циклические расширения (233). 5. Критерий разрешимости уравнений в радикалах (235). Упражнения (238).	
§ 6. Жёсткость и рациональность в конечных группах . . . . .	238
1. Определения и формулировка основной теоремы (239). 2. Подсчёт решений (240). 3. Примеры жёсткости (243). Упражнения (245).	
§ 7. Эпилог . . . . .	245

**ПРИЛОЖЕНИЕ  
НЕРЕШЁННЫЕ ЗАДАЧИ**

1. Классификация конечных простых групп . . . . .	248
2. Регулярный автоморфизм . . . . .	249
3. Странная алгебра Ли . . . . .	249
4. Проблема Бернсайда . . . . .	249
5. Конечные группы полиномиальных автоморфизмов . . . . .	250
6. Просто приводимые группы . . . . .	250
7. Обратная задача Галуа . . . . .	251
 ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ . . . . .	254
МЕТОДИЧЕСКИЕ ЗАМЕЧАНИЯ . . . . .	263
ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ . . . . .	268

Последнее время всё более распространённой становится точка зрения, что многие области математики являются не чем иным, как теорией инвариантов специальных групп.

*Софус Ли*

## ПРЕДИСЛОВИЕ

Содержание третьей части учебника “Введение в алгебру” можно квалифицировать как весьма серьёзное, но, надо надеяться, не слишком абстрактное продолжение первых двух частей. Новых понятий будет сравнительно немного, по крайней мере в первых четырёх главах. Читатель встретит своих старых “знакомых” по [ВА I, гл. 4] и [ВА II, гл. 7], которые введут его в область гораздо более содержательных понятий. Самое пристальное внимание рекомендуется уделить изучению примеров, которым отведена добрая четверть текста (скажем, материал § 1 гл. 1 и § 3 гл. 3 естественно отнести к примерам). Помимо всего прочего, подбор примеров рассчитан на то, чтобы перебросить мостик между алгеброй и другими разделами математики. Если в результате у читателя окрепнет чувство единства математики, то цель, поставленную автором в третьей части книги, следует считать достигнутой. Той же цели служит заключительная гл. 5, занимающая изолированное место и предназначенная почти целиком для освоения в рамках спецкурса.

Нет необходимости подчёркивать, что “Введение в алгебру” — учебник, рассчитанный на всех университетских студентов-математиков, а не только на будущих алгебраистов. Поэтому на подзаголовок “Основные структуры” надо смотреть снисходительно: это всё те же группы, кольца, поля, расширенные по ассортименту (с геометрическим уклоном), а главное — обогащённые важным понятием линейного представления. Именно модули и линейные представления дают те реализации алгебр и групп, которые постоянно возникают в анализе и геометрии.

*А.И. Кострикин*

## ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА

1. *Адамс Дж.* Лекции по группам Ли. — М.: Наука, 1979.
2. *Атья М., Макдональд И.* Введение в коммутативную алгебру. — М.: Мир, 1972.
3. *Барти Т., Биркгоф Г.* Современная прикладная алгебра. — М.: Мир, 1976.
4. *Белоногов В.А., Фомин А.Н.* Матричные представления в теории конечных групп. — М.: Наука, 1976.
5. *Боревич З.И., Шафаревич И.Р.* Теория чисел. — М.: Наука, 1972.

6. Бурбаки Н. Алгебра (модули, кольца, формы). — М.: Наука, 1966.
7. Вейль Г. Классические группы, их инварианты и представления. — М.: ИЛ, 1947.
8. Вейль Г. Симметрия. — М.: Наука, 1968.
9. Вейль А. Основы теории чисел. — М.: Мир, 1972.
10. Вингерг Э.Б. Курс алгебры. — М.: Факториал, 1999.
11. Джекобсон Н. Алгебры Ли. — М.: Мир, 1964.
12. Дьюдене Ж., Мамфорд Д., Керролл Дж. Геометрическая теория инвариантов. — М.: Мир, 1974.
13. Инфельд Л. Эварист Галуа. Избранный богов. — М.: Мол. гвардия, 1958.
14. Каргалолов М.И., Мерзляков Ю.И. Основы теории групп. — М.: Наука, 1972.
15. Клейн Ф. Лекции о развитии математики в XIX столетии. — М.: ГИТТЛ, 1937.
16. Клячко А.А. Теория Галуа: Уч. пособие. — Куйбышев: КГУ, 1982.
17. Кириллов А.А. Элементы теории представлений. — М.: Наука, 1972.
18. Кон П. Универсальная алгебра. — М.: Мир, 1968.
19. Кострикин А.И. Введение в алгебру. Ч. I. Основы алгебры. — М.: Физматлит, 2000.
20. Кострикин А.И. Введение в алгебру. Ч. II. Линейная алгебра. — М.: Физматлит, 2000.
21. Сборник задач по алгебре/ Под ред. А.И. Кострикина. — М.: Физматлит, 2000.
22. Курош А.Г. Лекции по общей алгебре. — М.: Наука, 1975.
23. Ленг С. Алгебра. — М.: Мир, 1968.
24. Лидл Р., Пильц Г. Прикладная абстрактная алгебра. — Изд-во Уральск. ун-та, 1996.
25. Мальцев А.И. Алгебраические системы. — М.: Наука, 1970.
26. Понtryagin L.S. Непрерывные группы. — М.: Наука, 1973.
27. Постников М.М. Теория Галуа. — М.: Физматгиз, 1963.
28. Сергеев Э.А. Элементы теории Галуа: Уч. пособие. — Краснодар: КГУ, 1987.
29. Серр Ж.-П. Линейные представления конечных групп. — М.: Мир,
30. Серр Ж.-П. Курс арифметики. — М.: Мир, 1972.
31. Херстейн И. Некоммутативные кольца. — М.: Мир, 1972.
32. Холл М. Теория групп. — М.: ИЛ, 1962.
33. Шафаревич И.Р. Основные понятия алгебры. — М.: ВИНИТИ, 1986.
34. Шевалле К. Теория групп Ли. — М.: ИЛ, 1948.
35. Edwards H.M. Galois Theory. — N.Y., B.: Springer-Verlag, 1984.
36. Jacobson N. Basic Algebra. I. — San Francisco: Freeman, 1974.
37. Malle G., Matzat B.H. Inverse Galois Theory. — N.Y., B.: Springer-Verlag, 1999.
38. Recent Developments in the Inverse Galois Problem, AMS, Contemporary Mathematics No. 186, 1995.
39. Serre J.-P. Topics in Galois Theory. — Boston: Jones and Bartlett, 1992.
40. Tignol J.-P. Galois' Theory of Algebraic Equations. — Avon: The Bath Press, 1987.
41. Völklein H. Groups as Galois Groups. An Introduction. — Cambridge University Press, 1996.

Ссылки на [19], [20] ниже в тексте заменены для наглядности эквивалентными ссылками на [ВА I], [ВА II].

## Глава 1

# ТЕОРЕТИКО-ГРУППОВЫЕ КОНСТРУКЦИИ

---

Настоящая глава развивает понятие группы, введённое в [ВА I, гл. 4]. В первую очередь акцент делается не на абстрактных группах, коим посвящено много специальных руководств, а на изучении разного рода естественных “действий” групп. Именно конкретные реализации групп послужили толчком к развитию общей теории групп и создали ей репутацию полезного инструмента математического исследования. На фоне частных (но, заметим, важных) примеров ещё настоятельнее становится идея рассмотрения (гомо-, эпи-, изо-) морфизмов групп, равно как теоретико-групповых конструкций, позволяющих сводить изучение сложных объектов к более простым.

## § 1. Классические группы малых размерностей

**1. Общие определения.** Курс линейной алгебры и геометрии снабжает нас новыми образцами групп, которые заслуживают того, чтобы остановиться на них чуть подробнее. Выделение в группах преобразований аффинных, евклидовых, эрмитовых и симплектических пространств подгрупп, оставляющих на месте фиксированную точку (например, начало координат), приводит к так называемым классическим группам  $GL(n)$ ,  $SL(n)$ ,  $O(n)$ ,  $SO(n)$ ,  $U(n)$ ,  $SU(n)$ ,  $Sp(n)$ . Отметим, что их истинное место — среди групп Ли, о которых мы упоминали в [ВА II] и о которых вкратце речь будет идти в гл. 2. Мы не ставим своей целью сколько-нибудь полное описание свойств классических групп; это делается в других книгах. При небольших  $n$  говорят о классических группах малых размерностей. С группами  $GL(n)$ ,  $SL(n)$  мы имели случай встречаться ранее (см. [ВА I]). Желая избежать большой зависимости от геометрии, напомним, что выбор ортонормированного базиса в пространстве приводит к эквивалентному матричному определению ортогональной и унитарной групп:

$$O(n) = \{A \in M_n(\mathbb{R}) \mid {}^t A \cdot A = A \cdot {}^t A = E\},$$

$$SO(n) = \{A \in O(n) \mid \det A = 1\},$$

$$U(n) = \{A \in M_n(\mathbb{C}) \mid A^* \cdot A = A \cdot A^* = E\},$$

$$SU(n) = \{A \in U(n) \mid \det A = 1\}.$$

Здесь  $A^* = {}^t \bar{A}$  — матрица, получающаяся из  $A = (a_{ij})$  транспонированием и заменой коэффициентов  $a_{ij}$  комплексно сопряжёнными

числами  $\bar{a}_{ij}$ . Группы  $\mathrm{SL}(n)$ ,  $\mathrm{SO}(n)$ ,  $\mathrm{SU}(n)$  носят название *специальных линейных, ортогональных и унитарных*. В частности,

$$\begin{aligned} \mathrm{O}(1) &= \{\pm 1\}, \quad \mathrm{SO}(1) = 1 := \{1\}, \\ \mathrm{U}(1) &= \{e^{i\varphi} \mid 0 \leq \varphi < 2\pi\}, \quad \mathrm{SU}(1) = 1, \\ \mathrm{SO}(2) &= \left\{ \begin{vmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{vmatrix} \mid 0 \leq \varphi < 2\pi \right\} \cong \mathrm{U}(1). \end{aligned}$$

Изоморфизм между группами  $\mathrm{SO}(2)$  и  $\mathrm{U}(1)$  задаётся естественным соответствием

$$\begin{vmatrix} \cos \varphi & -\sin \varphi \\ \sin \varphi & \cos \varphi \end{vmatrix} \mapsto e^{i\varphi}.$$

Так как геометрическим изображением комплексных чисел  $e^{i\varphi}$ ,  $0 \leq \varphi < 2\pi$ , является окружность  $S^1$  единичного радиуса в  $\mathbb{R}^2$ , то говорят ещё, что группа  $\mathrm{SO}(2)$  и окружность  $S^1$  *топологически эквивалентны*. Точный смысл этой терминологии разъясняется в курсе геометрии.

Замечательная и гораздо менее очевидная связь существует между группами  $\mathrm{SU}(2)$  и  $\mathrm{SO}(3)$ . Остановимся предварительно на геометрическом изображении группы  $\mathrm{SU}(2)$ , которое приведёт нас впоследствии к геометрическому изображению группы  $\mathrm{SO}(3)$ .

**2. Параметризация групп  $\mathrm{SU}(2)$ ,  $\mathrm{SO}(3)$ .** По известной теореме Эйлера каждый элемент группы  $\mathrm{SO}(3)$  собственных вращений трёхмерного евклидова пространства  $\mathbb{R}^3$  является вращением вокруг некоторой неподвижной оси. Скажем, матрицы

$$B_\varphi = \begin{vmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad C_\theta = \begin{vmatrix} 1 & 0 & 0 \\ 0 & \cos \theta & -\sin \theta \\ 0 & \sin \theta & \cos \theta \end{vmatrix} \quad (1)$$

отвечают вращениям вокруг осей  $Oz$  и  $Ox$  соответственно на углы  $\varphi$  и  $\theta$ . Используя параметризацию вращений углами Эйлера  $\varphi$ ,  $\theta$ ,  $\psi$  ( $0 \leq \varphi, \psi < 2\pi$ ,  $0 \leq \theta < \pi$ ), геометрический смысл которых нас пока не интересует, любую матрицу  $A \in \mathrm{SO}(3)$  можно записать в виде

$$A = B_\varphi C_\theta B_\psi, \quad (2)$$

где  $B_\varphi$ ,  $C_\theta$ ,  $B_\psi$  — указанные выше матрицы (1).

Пусть, далее,

$$g = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} \in \mathrm{SU}(2).$$

Имеем

$$g^* = {}^t \bar{g} = \begin{vmatrix} \overline{\alpha} & \overline{\gamma} \\ \overline{\beta} & \overline{\delta} \end{vmatrix}, \quad g^{-1} = \begin{vmatrix} \delta & -\beta \\ -\gamma & \alpha \end{vmatrix}.$$

Так как  $g \in \mathrm{U}(2) \iff g^* = g^{-1}$ , то  $\delta = \bar{\alpha}$  и  $\gamma = -\bar{\beta}$ . Таким образом, любая матрица  $g$  из  $\mathrm{SU}(2)$  имеет вид

$$g = \begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1. \quad (3)$$

Обратно, если  $g$  — матрица вида (3), то, очевидно,  $g \in \mathrm{SU}(2)$ . Значит, каждый элемент группы  $\mathrm{SU}(2)$  однозначно определяется парой комплексных чисел  $\alpha, \beta$  таких, что  $|\alpha|^2 + |\beta|^2 = 1$ . Если положить  $\alpha = \alpha_1 + i\alpha_2$ ,  $\beta = \beta_1 + i\beta_2$  с  $\alpha_k, \beta_k \in \mathbb{R}$ ,  $i = \sqrt{-1}$ , то условие  $|\alpha|^2 + |\beta|^2 = 1$ , переписанное в виде

$$\alpha_1^2 + \alpha_2^2 + \beta_1^2 + \beta_2^2 = 1,$$

даёт основание говорить, что группа  $\mathrm{SU}(2)$  топологически эквивалентна (гомеоморфна) сфере  $S^3$  в четырёхмерном вещественном пространстве  $\mathbb{R}^4$ .

Обратим внимание на унитарные матрицы

$$b_\varphi = \begin{vmatrix} e^{i\varphi/2} & 0 \\ 0 & e^{-i\varphi/2} \end{vmatrix}, \quad c_\theta = \begin{vmatrix} \cos(\theta/2) & i \sin(\theta/2) \\ i \sin(\theta/2) & \cos(\theta/2) \end{vmatrix}. \quad (4)$$

Как доказывается в курсе линейной алгебры (а в данном случае проверяется непосредственно), для унитарной матрицы  $g$  вида (3) существует унитарная матрица  $u$  такая, что

$$g = ub_\varphi u^{-1} \quad (5)$$

с  $\varphi$ , определяемым из уравнения  $\alpha_1 = \cos(\varphi/2)$ . Отметим также, что любой матрице (3) при  $\alpha\beta \neq 0$  можно придать вид

$$a(\varphi, \theta, \psi) = b_\varphi c_\theta b_\psi = \begin{vmatrix} \cos \frac{\theta}{2} \cdot e^{i(\varphi+\psi)/2} & i \sin \frac{\theta}{2} \cdot e^{i(\varphi-\psi)/2} \\ i \sin \frac{\theta}{2} \cdot e^{i(\psi-\varphi)/2} & \cos \frac{\theta}{2} \cdot e^{-i(\varphi+\psi)/2} \end{vmatrix}, \quad (6)$$

где<sup>1)</sup>

$$0 \leq \varphi < 2\pi, \quad 0 \leq \theta < \pi, \quad -2\pi \leq \psi < 2\pi.$$

Достаточно положить

$$\begin{aligned} |\alpha| &= \cos \frac{\theta}{2}, & \operatorname{Arg} \alpha &= \frac{\varphi + \psi}{2}, \\ |\beta| &= \sin \frac{\theta}{2}, & \operatorname{Arg} \beta &= \frac{\varphi - \psi + \pi}{2}, \end{aligned}$$

используя то обстоятельство, что каждое комплексное число  $z$  задаётся двумя вещественными параметрами,  $|z|$  и  $\arg z$  ( $\operatorname{Arg} z$  — главное значение аргумента  $\arg z$ ).

<sup>1)</sup> Из дальнейшего будет видно, что  $\varphi, \theta, \psi$  — те же углы Эйлера. Унитарным матрицам  $\pm g$  ставится в соответствие одно и то же вращение в  $\mathbb{R}^2$ , поэтому область изменения  $\psi$  сжимается до полуинтервала  $[0, 2\pi]$ .

Теперь мы готовы приступить к решению основной задачи этого параграфа.

**3. Эпиморфизм  $SU(2) \rightarrow SO(3)$ .** Поставим в соответствие каждому вектору  $\mathbf{x} = x_1\mathbf{e}_1 + x_2\mathbf{e}_2 + x_3\mathbf{e}_3$  трёхмерного евклидова пространства  $\mathbb{R}^3$  с нормой  $(\mathbf{x}|\mathbf{x}) = x_1^2 + x_2^2 + x_3^2$  комплексную матрицу второго порядка

$$H_{\mathbf{x}} = \begin{vmatrix} x_3 & x_1 + ix_2 \\ x_1 - ix_2 & -x_3 \end{vmatrix}. \quad (7)$$

Пространство  $M_2^+$  матриц вида (7) состоит из всех эрмитовых матриц с нулевым следом ( ${}^t\bar{H}_{\mathbf{x}} = H_{\mathbf{x}}$ ,  $\text{tr } H_{\mathbf{x}} = 0$ ), причём соответствие между векторами  $\mathbf{x} \in \mathbb{R}^3$  и матрицами  $H_{\mathbf{x}} \in M_2^+$  является, очевидно, взаимно однозначным. В частности, базисным векторам  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3 \in \mathbb{R}^3$  соответствуют базисные матрицы  $h_k = H_{\mathbf{e}_k}$ ,  $k = 1, 2, 3$ :

$$h_1 = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, \quad h_2 = \begin{vmatrix} 0 & i \\ -i & 0 \end{vmatrix}, \quad h_3 = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}; \quad (8)$$

$$H_{\mathbf{x}} = x_1 h_1 + x_2 h_2 + x_3 h_3, \quad M_2^+ = \langle h_1, h_2, h_3 \rangle.$$

Заметим, что каждому линейному оператору  $\mathcal{A}^+ : H_{\mathbf{x}} \mapsto H_{\mathbf{y}}$  на  $M_2^+$  с матрицей  $A$  в базисе (8) будет отвечать вполне определённый линейный оператор  $\mathcal{A} : \mathbf{x} \mapsto \mathbf{y}$  на  $\mathbb{R}^3$  с той же матрицей  $A$  в базисе  $\mathbf{e}_1, \mathbf{e}_2, \mathbf{e}_3$ , поскольку  $H_{\alpha\mathbf{x}} = \alpha H_{\mathbf{x}}$ ,  $H_{\mathbf{x}+\mathbf{x}'} = H_{\mathbf{x}} + H_{\mathbf{x}'}$ . Так как никакие другие базисы в дальнейшем не используются, то мы будем иногда отождествлять операторы и соответствующие им матрицы.

Пусть теперь  $g$  — фиксированный элемент группы  $SU(2)$ . Рассмотрим отображение

$$\Phi_g^+ : H_{\mathbf{x}} \mapsto g H_{\mathbf{x}} g^{-1}. \quad (9)$$

Так как следы подобных матриц совпадают, то  $\text{tr } \Phi_g^+(H_{\mathbf{x}}) = \text{tr } H_{\mathbf{x}} = 0$ . Кроме того,  $g^* = {}^t g = g^{-l}$ , поэтому

$$(g H_{\mathbf{x}} g^{-1})^* = (g^{-1})^* H_{\mathbf{x}}^* g^* = g H_{\mathbf{x}} g^{-1}$$

и, следовательно,  $\Phi_g^+(H_{\mathbf{x}}) \in M_2^+$ :

$$\Phi_g^+(H_{\mathbf{x}}) = \begin{vmatrix} y_3 & y_1 + iy_2 \\ y_1 - iy_2 & -y_3 \end{vmatrix} = H_{\mathbf{y}},$$

где  $\mathbf{y} = (y_1, y_2, y_3) \in \mathbb{R}^3$ . Из определяющих равенств (7) и (9) видно, что

$$\Phi_g^+(H_{\alpha\mathbf{x}+\alpha'\mathbf{x}'}) = \alpha \Phi_g^+(H_{\mathbf{x}}) + \alpha' \Phi_g^+(H_{\mathbf{x}'}).$$

Стало быть, отображение  $\Phi_g^+$  (соответственно  $\Phi_g$ ) — линейный оператор на  $M_2^+$  (соответственно на  $\mathbb{R}^3$ ).

Покажем, что  $\Phi_g: \mathbb{R}^3 \rightarrow \mathbb{R}^3$  — ортогональный оператор. В самом деле,

$$\begin{aligned} (\Phi_g(\mathbf{x})|\Phi_g(\mathbf{x})) &= (\mathbf{y}|\mathbf{y}) = -\det H_{\mathbf{y}} = -\det \Phi_g^+(H_{\mathbf{x}}) = \\ &= -\det gH_{\mathbf{x}}g^{-1} = -\det H_{\mathbf{x}} = x_1^2 + x_2^2 + x_3^2 = (\mathbf{x}|\mathbf{x}), \end{aligned}$$

т. е.  $\Phi_g$  сохраняет норму, а следовательно, и скалярное произведение. Пока не ясно, меняет ли  $\Phi_g$  ориентацию пространства  $\mathbb{R}^3$ , что зависит от знака  $\det \Phi_g$ . Мы знаем лишь, что  $\det \Phi_g = \pm 1$ . Как следует из определения,

$$\Phi_g^+(\Phi_{g'}H_{\mathbf{x}}) = g(g'H_{\mathbf{x}}g'^{-1})g^{-1} = (gg')H_{\mathbf{x}}(gg')^{-1} = \Phi_{gg'}^+(H_{\mathbf{x}}),$$

причём  $\Phi_E^+$  — единичная ортогональная матрица порядка 3 для  $E = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \in \mathrm{SU}(2)$ . Значит, соответствие

$$\Phi: g \mapsto \Phi_g \quad (\text{или } \Phi^+: g \mapsto \Phi_g^+)$$

является гомоморфизмом  $\mathrm{SU}(2)$  в  $\mathrm{O}(3)$ . Ядро состоит из унитарных матриц  $g$ , для которых  $\Phi_g^+ = \Phi_E^+$ . Другими словами,

$$\begin{aligned} \mathrm{Ker} \Phi &= \{g \in \mathrm{SU}(2) \mid gH = Hg \quad \forall H \in M_2^+\} = \\ &= \{g \in \mathrm{SU}(2) \mid gh_j = h_jg, \quad j = 1, 2, 3\}, \end{aligned}$$

где  $h_1, h_2, h_3$  — базис (8) пространства  $M_2^+$ . Прямая проверка показывает, что

$$\begin{aligned} g &= \begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix}, \quad gh_j = h_jg, \quad 1 \leq j \leq 3 \implies \\ &\implies g = \pm E \implies \mathrm{Ker} \Phi = \{\pm E\}. \end{aligned}$$

Посмотрим теперь на образы унитарных матриц (4) при гомоморфизме  $\Phi$ . Проведём вычисления для  $\Phi^+$  в базисе (8):

$$\begin{aligned} b_\varphi h_1 b_\varphi^{-1} &= (\cos \varphi)h_1 + (\sin \varphi)h_2, \\ b_\varphi h_2 b_\varphi^{-1} &= (-\sin \varphi)h_1 + (\cos \varphi)h_2, \\ b_\varphi h_3 b_\varphi^{-1} &= h_3. \end{aligned}$$

Значит (здесь мы свободно переходим от  $\Phi^+$  к  $\Phi$  и от матриц — к операторам),  $\Phi_{b_\varphi} = B_\varphi$  (см. (1)) — вращение трёхмерного евклидова пространства  $\mathbb{R}^3$  на угол  $\varphi$  вокруг оси  $Ox_3$  (или  $h_3$ ). Если  $\varphi$  и  $u$  выбрать такими, чтобы выполнялось соотношение (5), то поскольку  $\Phi$  — гомоморфизм, будем иметь

$$\Phi_g = \Phi_u \Phi_{b_\varphi} \Phi_u^{-1}, \quad \det \Phi_g = \det \Phi_u \cdot 1 \cdot (\det \Phi_u)^{-1} = 1.$$

Это показывает, что на самом деле  $\Phi$  — гомоморфизм  $SU(2)$  в  $SO(3)$ . Аналогичным образом проверяется, что  $\Phi_{c_\theta}$  — вращение на угол  $\theta$  вокруг оси  $Ox_1$ . Теперь для любой матрицы  $A \in SO(3)$  имеем

$$A = B_\varphi C_\theta B_\psi = \Phi_{b_\varphi} \Phi_{c_\theta} \Phi_{b_\psi} = \Phi_{b_\varphi c_\theta b_\psi} = \Phi_{a(\varphi, \theta, \psi)}.$$

Стало быть, образ  $\text{Im } \Phi$  содержит всю группу  $SO(3)$ , и нами доказана

**Теорема 1.** Группа  $SO(3)$  является гомоморфным образом группы  $SU(2)$  при гомоморфизме  $\Phi : g \mapsto \Phi_g$  с ядром  $\text{Ker } \Phi = \{\pm E\}$ . Каждое вращение из  $SO(3)$  отвечает ровно двум унитарным операторам  $g$  и  $-g$  из  $SU(2)$ .

**4. Геометрическое изображение группы  $SO(3)$ .** Из теоремы 1 непосредственно вытекает

**Следствие.** Группа  $SO(3)$  топологически эквивалентна (гомоморфна) трёхмерному проективному вещественному пространству  $\mathbb{RP}^3$ .

В самом деле, мы видели в п. 2, что элементы из  $SU(2)$  находятся во взаимно однозначном соответствии с точками сферы  $S^3$  в четырёхмерном вещественном пространстве  $\mathbb{R}^4$ . Линейным операторам  $\pm g \in SU(2)$  отвечают диаметрально противоположные точки на  $S^3$ , которые при гомоморфизме  $\Phi$  склеиваются (отождествляются). Получается одна из моделей проективного пространства  $\mathbb{RP}^3$ .  $\square$

В курсе линейной алгебры и геометрии (см. [ВА II, гл. 5, § 3]) проективное пространство  $\mathbb{RP}^n$  определяется как множество прямых пространства  $\mathbb{R}^{n+1}$ , проходящих через начало координат  $O$ . Каждая такая прямая пересекает единичную сферу  $S^n$  с центром в  $O$  ровно в двух диаметрально противоположных точках. Заданием одной из этих точек прямая однозначно восстанавливается. Это и значит, что пространство  $\mathbb{RP}^n$  может быть определено как факторпространство единичной сферы  $S^n$  из  $\mathbb{R}^{n+1}$  по отношению, устанавливающему эквивалентность диаметрально противоположных точек сферы  $S^n$ . В нашу задачу сейчас не входит задание топологии на  $\mathbb{RP}^n$ .

Мы пришли к довольно неожиданному результату. На сфере  $S^3$  и на проективном пространстве  $\mathbb{RP}^3$  устанавливаются структуры группы: в первом случае —  $SU(2)$ , во втором —  $SO(3)$ . Всякая попытка задать структуру непрерывной группы на  $S^2$  или на  $\mathbb{RP}^2$  окончится неудачей (результат, не относящийся к нашей теме).

Согласно теореме 1 и её следствию группа  $SO(3)$  “в два раза меньше”, чем группа  $SU(2)$ . Существование эпиморфизма  $SU(2) \rightarrow SO(3)$  делает естественным вопрос о существовании мономорфизма  $SO(3) \rightarrow SU(2)$ . Мы увидим в гл. 3, что ответ на этот вопрос оказывается отрицательным.

**5. Кватернионы.** Реализация  $SU(2)$  становится ещё более наглядной, если под  $\mathbb{R}^4$  мы будем понимать специальное четырёхмерное вещественное пространство, снабжённое структурой *тела* — ас-

соассоциативной, хотя и некоммутативной алгебры с делением над  $\mathbb{R}$  (все отличные от нуля элементы обратимы). Имеется в виду знаменитая алгебра кватернионов, построенная в 1848 г. Гамильтоном (W. Hamilton, 1805–1865) и в его честь обозначаемая буквой  $\mathbb{H}$ . По традиции для её базисных элементов используются символы **1** (единица), **i** (мнимая единица), **j** и **k**. Так как в  $\mathbb{H}$  должен выполняться закон дистрибутивности, то закон умножения целиком определяется “таблицей умножения”:

	<b>1</b>	<b>i</b>	<b>j</b>	<b>k</b>
<b>1</b>	<b>1</b>	<b>i</b>	<b>j</b>	<b>k</b>
<b>i</b>	<b>i</b>	-1	<b>k</b>	- <b>j</b>
<b>j</b>	<b>j</b>	- <b>k</b>	-1	<b>i</b>
<b>k</b>	<b>k</b>	<b>j</b>	- <b>i</b>	-1

Из этой таблицы сразу видно, что  $\mathbb{H}$  — ассоциативная (но некоммутативная) алгебра с центром  $Z(\mathbb{H}) = \mathbb{R}$  и **1** — её единичный элемент. Каждый элемент алгебры  $\mathbb{H}$  однозначно записывается в виде

$$\mathbf{q} = \alpha + \beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k} := \alpha \mathbf{1} + \beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k} \quad (10)$$

с вещественными коэффициентами  $\alpha, \beta, \gamma, \delta$ , так что

$$\mathbb{H} = \mathbb{R} \mathbf{1} + \mathbb{R} \mathbf{i} + \mathbb{R} \mathbf{j} + \mathbb{R} \mathbf{k}.$$

Между прочим, умножение в  $\mathbb{H}$  служит непосредственным продолжением умножения в поле комплексных чисел  $\mathbb{C}$ , покрываемом кватернионами  $\alpha + \beta \mathbf{i}$  (**1** отождествляется с вещественной единицей 1, а **i** — с  $i = \sqrt{-1}$ ). Фактически  $\mathbb{H}$  можно рассматривать как двумерную алгебру над  $\mathbb{C}$ . Действительно, для  $c, c' \in \mathbb{C}$ ,  $\mathbf{q}, \mathbf{q}' \in \mathbb{H}$  имеем

$$\begin{aligned} c(\mathbf{q} + \mathbf{q}') &= c\mathbf{q} + c\mathbf{q}', & (c + c')\mathbf{q} &= c\mathbf{q} + c'\mathbf{q}, \\ (cc')\mathbf{q} &= c(c'\mathbf{q}) = c'(c\mathbf{q}). \end{aligned}$$

Так как

$$\alpha \mathbf{1} + \beta \mathbf{i} + \gamma \mathbf{j} + \delta \mathbf{k} = (\alpha + \beta \sqrt{-1}) \mathbf{1} + (\gamma + \delta \sqrt{-1}) \mathbf{j},$$

то  $\dim_{\mathbb{C}} \mathbb{H} = 2$ .

Аналогия с  $\mathbb{C}$  просматривается и дальше. Так, *сопряжённым* с  $\mathbf{q}$  называется кватернион

$$\mathbf{q}^* = \alpha - \beta \mathbf{i} - \gamma \mathbf{j} - \delta \mathbf{k}$$

— аналог сопряжённого комплексного числа. Если  $\mathbf{q}$  — “чистый кватернион”, т.е.  $\alpha = 0$ , то  $\mathbf{q}^* = -\mathbf{q}$ . Величина

$$N(\mathbf{q}) := \mathbf{q} \cdot \mathbf{q}^* = \alpha^2 + \beta^2 + \gamma^2 + \delta^2, \quad (11)$$

вычисляемая посредством приведённой выше таблицы, называется *нормой* кватерниона  $\mathbf{q}$ . Очевидно, что  $\mathbf{q} \neq 0 \Rightarrow N(\mathbf{q}) \neq 0$ , а поэтому

всякий ненулевой кватернион обратим:

$$\mathbf{q}^{-1} = \frac{\mathbf{q}^*}{N(\mathbf{q})}, \quad \mathbf{q} \cdot \mathbf{q}^{-1} = \mathbf{1} = \mathbf{q}^{-1} \cdot \mathbf{q}. \quad (12)$$

Стало быть, множество  $\mathbb{H}^* := \mathbb{H} \setminus \{\mathbf{0}\}$  является группой (*мультиликативная группа алгебры кватернионов*).

Элементарно проверяется, что

$$(\mu_1 \mathbf{q}_1 + \mu_2 \mathbf{q}_2)^* = \mu_1 \mathbf{q}_1^* + \mu_2 \mathbf{q}_2^*, \quad (\mathbf{q}_1 \mathbf{q}_2)^* = \mathbf{q}_2^* \mathbf{q}_1^*;$$

$$N(\mathbf{q}_1 \mathbf{q}_2) = N(\mathbf{q}_1)N(\mathbf{q}_2).$$

Таким образом, отображение  $\mathbf{q} \mapsto \mathbf{q}^*$  суть *антиавтоморфизм* (представляющий множители) алгебры  $\mathbb{H}$ , а отображение  $\mathbf{q} \mapsto N(\mathbf{q})$  — гомоморфизм мультиликативной группы  $\mathbb{H}^*$  в  $\mathbb{R}^*$  с ядром

$$\mathrm{Sp}(1) := \mathrm{Ker} N = \{\mathbf{q} \in \mathbb{H} \mid N(\mathbf{q}) = 1\}. \quad (13)$$

Группа  $\mathrm{Sp}(1)$  называется *симплектической*; она имеет прямое отношение к линейным симплектическим группам  $\mathrm{Sp}(2n, \mathbb{K})$ , кратко рассмотренным в [ВА II], но мы на этом останавливаться не будем.

Из (10), (11) и (13) видно, что группа  $\mathrm{Sp}(1)$  топологически эквивалентна сфере в специальном четырёхмерном пространстве  $\mathbb{H}$ . С аналогичным свойством, касающимся группы  $\mathrm{SU}(2)$ , мы встречались в п. 2. Соединить эти два свойства совсем несложно. Рассмотрим отображение  $\Gamma : \mathbb{H} \longrightarrow M_2(\mathbb{C})$ , которое каждому кватерниону  $\mathbf{q} = c + \mathbf{j}c'$  вида (10) ставит в соответствие комплексную матрицу

$$\Gamma(\mathbf{q}) = \begin{vmatrix} \alpha + i\beta & \gamma + i\delta \\ -(\gamma - i\delta) & \alpha - i\beta \end{vmatrix} = \begin{vmatrix} c & c' \\ -\bar{c}' & \bar{c} \end{vmatrix}. \quad (14)$$

Очевидно,

$$\begin{aligned} \Gamma(\mu_1 \mathbf{q}_1 + \mu_2 \mathbf{q}_2) &= \mu_1 \Gamma(\mathbf{q}_1) + \mu_2 \Gamma(\mathbf{q}_2), \\ \Gamma(\mathbf{q}_1 \mathbf{q}_2) &= \Gamma(\mathbf{q}_1)\Gamma(\mathbf{q}_2), \quad \Gamma(\mathbf{1}) = E \end{aligned}$$

— свойства, присущие *линейному представлению* над  $\mathbb{C}$  в том общем смысле, который будет придан этому понятию позднее. Вспомним попутно, что в [ВА I, гл. 5] первоначальным алгебраическим изображением комплексных чисел были матрицы  $\begin{vmatrix} a & b \\ -b & a \end{vmatrix} \in M_2(\mathbb{R})$ .

Из (14) следует, что

$$\Gamma(\mathrm{Sp}(1)) = \left\{ \begin{vmatrix} c & c' \\ -\bar{c}' & \bar{c} \end{vmatrix} \mid |c|^2 + |c'|^2 = 1 \right\} = \mathrm{SU}(2),$$

т.е.  $\Gamma$  реализует изоморфизм групп  $\mathrm{SU}(2)$  и  $\mathrm{Sp}(1)$ . К искомому эпиморфизму  $\mathrm{Sp}(1) \longrightarrow \mathrm{SO}(3)$  мы придём следующим образом. Каждому кватерниону  $\mathbf{q}$  с единичной нормой поставим в соответствие отображение  $\Psi_{\mathbf{q}} : \mathbb{H} \longrightarrow \mathbb{H}$ , полагая

$$\Psi_{\mathbf{q}}(\mathbf{p}) = \mathbf{q} \mathbf{p} \mathbf{q}^{-1}. \quad (15)$$

Так как  $\mathbf{q}^{-1} = \mathbf{q}^*$  (см. (12)), то

$$\Psi_{\mathbf{q}}(\mathbf{p}^*) = \mathbf{q}\mathbf{p}^*\mathbf{q}^{-1} = (\mathbf{q}^{-1})^*\mathbf{p}^*\mathbf{q}^* = (\Psi_{\mathbf{q}}(\mathbf{p}))^*$$

Если  $\mathbf{p}^* = -\mathbf{p}$  — чистый кватернион, то  $(\Psi_{\mathbf{q}}(\mathbf{p}))^* = \Psi_{\mathbf{q}}(\mathbf{p}^*) = -\Psi_{\mathbf{q}}(\mathbf{p})$ , и, значит, подпространство  $\mathbb{H}^-$  чистых кватернионов инвариантно относительно  $\Psi_{\mathbf{q}}$ . Мы пришли к линейному оператору

$$\Psi_{\mathbf{q}}: \mathbb{H}^- \longrightarrow \mathbb{H}^-.$$

Как непосредственно вытекает из (15),  $\Psi_{\mathbf{q}_1 \mathbf{q}_2} = \Psi_{\mathbf{q}_1} \Psi_{\mathbf{q}_2}$ , т.е. элементы группы  $\mathrm{Sp}(1)$  “представляются” матрицами третьего порядка:

$$\Psi_{\mathbf{q}}(x_1 \mathbf{i} + x_2 \mathbf{j} + x_3 \mathbf{k}) = y_1 \mathbf{i} + y_2 \mathbf{j} + y_3 \mathbf{k}; \quad y_\mu = \sum_{\nu=1}^3 a_{\mu\nu} x_\nu.$$

Отождествим трёхмерное евклидово пространство  $\mathbb{R}^3$  с пространством чисто мнимых кватернионов:

$$\mathbb{R}^3 = \{\mathbf{p} \in \mathbb{H}^- \mid |\mathbf{p}|^2 := N(\mathbf{p})\}.$$

С таким определением квадрата длины  $|\mathbf{p}|^2$  имеем

$$|\Psi_{\mathbf{q}}(\mathbf{p})|^2 = N(\Psi_{\mathbf{q}}(\mathbf{p})) = N(\mathbf{q})|\mathbf{p}|^2N(\mathbf{q}^{-1}) = |\mathbf{p}|^2,$$

поскольку по условию  $N(\mathbf{q}) = 1$ . Значит,  $\Psi_{\mathbf{q}}$  — линейный оператор, сохраняющий длину, и мы имеем гомоморфизм  $\Psi: \mathrm{Sp}(1) \longrightarrow \mathrm{O}(3)$ . Стоит отметить ещё раз, что  $\Psi_{\mathbf{q}} = \mathcal{E}$  в точности при  $\mathbf{q} = \pm 1$ , и поэтому  $\mathrm{Ker} \Psi = \{\pm 1\}$ .

Вспомним теперь, что  $\mathrm{Sp}(1) \sim S^3$ . Так как любую точку  $\mathbf{q} \in S^3$  можно соединить с точкой  $\mathbf{1}$  гладкой кривой  $\mathbf{r}(t)$ , то  $\Psi_{\mathbf{r}(t)}$  является кривой, соединяющей  $\Psi_{\mathbf{q}}$  с тождественным оператором  $\Psi_{\mathbf{1}}$ . Определитель  $\det$  — непрерывная функция оператора, зависящего от параметра  $t$ , и так как  $\det \Psi_{\mathbf{1}} = 1$ , то  $\det \Psi_{\mathbf{r}(t)} = 1$ . В частности,  $\det \Psi_{\mathbf{q}} = 1$ . Стало быть,  $\Psi_{\mathrm{Sp}(1)} \subset \mathrm{SO}(3)$ .

Осталось убедиться, что  $\Psi$  — сюръективное отображение. С этой целью предъявим в качестве образов известные нам матрицы (1).

а)  $\mathbf{q} = \cos \frac{\theta}{2} \mathbf{1} + \sin \frac{\theta}{2} \mathbf{i} \implies \Psi_{\mathbf{q}}(\mathbf{i}) = \mathbf{i}$ , т.е. ось  $\mathbf{i}$  в  $\mathbb{R}^3$  остаётся при этом преобразовании инвариантной. Так как

$$\Psi_{\mathbf{q}}(\mathbf{j}) \left( \cos \frac{\theta}{2} \mathbf{1} + \sin \frac{\theta}{2} \mathbf{i} \right) \mathbf{j} \left( \cos \frac{\theta}{2} \mathbf{1} - \sin \frac{\theta}{2} \mathbf{i} \right) = \cos \theta \mathbf{j} + \sin \theta \mathbf{k},$$

$$\Psi_{\mathbf{q}}(\mathbf{k}) = -\sin \theta \mathbf{j} + \cos \theta \mathbf{k},$$

то  $\Psi_{\mathbf{q}}$  отвечает матрице  $C_\theta$ . Аналогично, если  $\mathbf{q} = \cos \frac{\varphi}{2} \mathbf{1} + \sin \frac{\varphi}{2} \mathbf{k}$ , то  $\Psi_{\mathbf{q}}$  отвечает матрице  $B_\varphi$  поворота вокруг оси  $\mathbf{k}$ .

Таким образом, справедлива

Теорема 1'. Отображение  $\Psi$  (соответственно  $\Psi \Gamma^{-1}$ ) является гомоморфизмом группы  $\mathrm{Sp}(1)$  (соответственно  $\mathrm{SU}(2)$ ) на группу  $\mathrm{SO}(3)$  с ядром  $\{\pm \mathbf{1}\}$  (соответственно  $\{\pm E\}$ ).

## УПРАЖНЕНИЯ

**1.** Используя геометрическое изображение группы  $SU(2)$ , показать, что

$$(0, 1, 0, 0) * (0, 0, 1, 0) = (0, 0, 0, 1) \neq (0, 0, 1, 0) * (0, 1, 0, 0)$$

(произведение точек на  $S^3$ ). Те же точки  $(0, 1, 0, 0), (0, 0, 1, 0)$ , рассматриваемые на  $\mathbb{RP}^3$ , перестановочны.

**2.** Показать, что если коэффициенты унитарных матриц

$$K_1(t) = \begin{vmatrix} \cos \frac{t}{2} & i \sin \frac{t}{2} \\ i \sin \frac{t}{2} & \cos \frac{t}{2} \end{vmatrix}, \quad K_2(t) = \begin{vmatrix} \cos \frac{t}{2} & -\sin \frac{t}{2} \\ \sin \frac{t}{2} & \cos \frac{t}{2} \end{vmatrix},$$

$$K_3(t) = \begin{vmatrix} e^{it/2} & 0 \\ 0 & e^{-it/2} \end{vmatrix}$$

продифференцировать по  $t$  и положить затем  $t = 0$ , то получатся матрицы

$$K_1 = \frac{i}{2} \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = \frac{i}{2} h_1, \quad K_2 = \frac{i}{2} \begin{vmatrix} 0 & i \\ -i & 0 \end{vmatrix} = \frac{i}{2} h_2, \quad K_3 = \frac{i}{2} \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} = \frac{i}{2} h_3,$$

составляющие базис пространства  $M_2^-$  косоэрмитовых матриц

$$K = \begin{vmatrix} ik_3 & -k_2 + ik_1 \\ k_2 + ik_1 & -ik_3 \end{vmatrix}, \quad k_j \in \mathbb{R},$$

с нулевым следом:  $K^* = -K$ ,  $\operatorname{tr} K = 0$ .

**3.** Кватернионные единицы  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  порождают в  $\operatorname{Sp}(1)$  интересную подгруппу — группу кватернионов  $Q_8$  порядка 8, играющую заметную роль в разного рода вопросах. Какое отношение к  $Q_8$  имеют матрицы

$$\pm \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad \pm \begin{vmatrix} i & 0 \\ 0 & -i \end{vmatrix}, \quad \pm \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}, \quad \pm \begin{vmatrix} 0 & i \\ i & 0 \end{vmatrix}?$$

**4.** Можно ли построить ассоциативную алгебру с делением  $A$  над  $\mathbb{R}$  размерности 3, содержащую  $\mathbb{C}$  в качестве подалгебры?

**5.** Эйфория, возникшая в связи с открытием кватернионов, привела к созданию общества сторонников кватернионных функций — аналога функций комплексного переменного. Хотя больших достижений на этом пути не было достигнуто, нельзя отрицать, что кватернионы имеют прямое отношение к математической физике. В какой-то мере это можно усмотреть, введя дифференциальный оператор

$$\nabla = \mathbf{i} \frac{\partial}{\partial x} + \mathbf{j} \frac{\partial}{\partial y} + \mathbf{k} \frac{\partial}{\partial z}$$

на трёхмерном функциональном пространстве с базисом  $\{\mathbf{i}, \mathbf{j}, \mathbf{k}\}$ . Справедливы следующие соотношения:

$$\nabla t = \mathbf{i} \frac{\partial t}{\partial x} + \mathbf{j} \frac{\partial t}{\partial y} + \mathbf{k} \frac{\partial t}{\partial z}$$

— градиент скаляра  $t$ ;

$$\nabla^2 t = -\Delta t = - \left( \frac{\partial^2 t}{\partial x^2} + \frac{\partial^2 t}{\partial y^2} + \frac{\partial^2 t}{\partial z^2} \right)$$

— выражение из теории потенциала;

$$\nabla \underbrace{(\mathbf{i}u + \mathbf{j}v + \mathbf{k}w)}_{\text{поле}} = - \left( \underbrace{\frac{\partial u}{\partial x} + \frac{\partial v}{\partial y} + \frac{\partial w}{\partial z}}_{\text{дивергенция поля}} \right) + \underbrace{\mathbf{i} \left( \frac{\partial w}{\partial y} - \frac{\partial v}{\partial z} \right) + \mathbf{j} \left( \frac{\partial u}{\partial z} - \frac{\partial w}{\partial x} \right) + \mathbf{k} \left( \frac{\partial v}{\partial x} - \frac{\partial u}{\partial y} \right)}_{\text{вихрь (ротор) поля}}.$$

Предлагается провести все необходимые вычисления, опираясь на правила умножения в алгебре кватернионов.

## § 2. Смежные классы по подгруппе

**1. Элементарные свойства.** Пусть  $G, G'$  — две произвольные группы с нейтральными элементами  $e, e'$ . Из определения гомоморфизма  $f : G \rightarrow G'$  и из рассмотренных нами в [ВА I; ВА II] многочисленных примеров видно,  $\text{Ker } f$  — подгруппа в  $f$ , причём  $x(\text{Ker } f) = (\text{Ker } f)x, x \in G$ .

**Определение.** Подгруппа  $K \subset G$  называется *нормальной* в  $G$ , если

$$xKx^{-1} = K \quad \forall x \in G.$$

Таким образом, ядра гомоморфизмов всегда являются нормальными подгруппами. Значение этого факта мы оценим в должной мере несколько позднее. Заметим пока, что далеко не всякая подгруппа нормальна в  $G$ . Например, в  $S_3$  циклическая подгруппа  $\langle (123) \rangle = A_3$  нормальна, а  $\langle (12) \rangle = \{e, (12)\}$  таковой не является (не рекомендуется называть  $\langle (12) \rangle$  “ненормальной подгруппой”).

Обратим внимание на то обстоятельство, что все элементы множества

$$a \text{Ker } f = \{ab \mid b \in \text{Ker } f\}, \quad a \in G,$$

отображаются в один и тот же элемент  $f(a)$  группы  $G'$ :  $f(ab) = f(a)f(b) = f(a)e' = f(a)$ . В свою очередь, если  $f(g) = f(a)$ , то  $f(a^{-1}g) = f(a^{-1})f(g) = f(a)^{-1}f(g) = e'$ , откуда  $a^{-1}g = b \in \text{Ker } f$  и  $g = ab \in a \text{Ker } f$ . Этот факт указывает на целесообразность разбиения  $G$  на подмножества вида  $a \text{Ker } f$ . Изучим такое разбиение в общем случае независимо от гомоморфизмов.

**Определение.** Пусть  $H$  — подгруппа группы  $G$ . *Левым смежным классом группы  $G$  по подгруппе  $H$*  (коротко:  $G$  по  $H$ ) называется множество  $gH$  элементов вида  $gh$ , где  $g$  — фиксированный элемент из  $G$ , а  $h$  пробегает все элементы подгруппы  $H$ . Элемент  $g$  называется *представителем* смежного класса  $gH$ .

Аналогично определяются *правые смежные классы*  $Hg$ . Иногда левые смежные классы в нашем смысле называются правыми, а правые — левыми. Важно придерживаться лишь одной какой-нибудь терминологии. Если  $H = \text{Ker } f$  — ядро гомоморфизма, то  $gH = Hg$  ввиду нормальности  $H$  в  $G$ . Заметим, что одним из смежных классов является сама подгруппа  $H = He = eH$ . Никакой другой смежный класс подгруппой не является. Действительно, если  $gH$  — подгруппа, то  $e \in gH$ , откуда  $e = gh$ ,  $g = h^{-1}$  и  $gH = h^{-1}H = H$ .

**Теорема 1.** *Два левых смежных класса  $G$  по  $H$  совпадают или не имеют общих элементов. Разбиение  $G$  на левые смежные классы по  $H$  определяет на  $G$  отношение эквивалентности.*

**Доказательство.** Пусть классы  $g_1H$  и  $g_2H$  имеют общий элемент  $a = g_1h_1 = g_2h_2$ . Тогда  $g_2 = g_1h_1h_2^{-1}$ , а любой элемент  $g_2h$  класса  $g_2H$  имеет вид  $g_1h_1h_2^{-1}h = g_1h'$ , где  $h' = h_1h_2^{-1}h \in H$ . Значит,  $g_2H \subset g_1H$ . Аналогично доказывается, что всякий элемент из класса  $g_1H$  содержится в  $g_2H$  и, стало быть,  $g_1H = g_2H$ .

Так как любой наперёд заданный элемент  $g \in G$  содержится в  $gH$ , то проведённое рассуждение показывает, что  $G$  представляется в виде объединения непересекающихся левых смежных классов по подгруппе  $H$ :

$$G = \bigcup_i g_iH.$$

Согласно общему принципу, изложенному в [ВА I, гл. 1, § 6], это разбиение индуцирует на  $G$  отношение эквивалентности, которое определяется очевидным образом:

$$a \sim b \iff a^{-1}b \in H.$$

Если угодно, в рефлексивности, симметричности и транзитивности этого отношения можно убедиться непосредственно:  $a \sim a$ , поскольку  $a^{-1}a = e \in H$ ;  $a \sim b \iff a^{-1}b = h \iff b^{-1}a = h^{-1} \in H \iff b \sim a$ ;  $a \sim b$ ,  $b \sim c \implies b^{-1}a = h_1$ ,  $c^{-1}b = h_2 \implies c^{-1}a = c^{-1}bh_1 = h_2h_1 \in H \implies a \sim c$ .  $\square$

Аналогичное утверждение имеет место для правых смежных классов.

Разложение на смежные классы возникает естественным образом в группах перестановок. Пусть, например,  $G = S_n$  — симметрическая группа, действующая на множестве  $\Omega = \{1, 2, \dots, n\}$ . Если рассмотреть совокупность  $H$  элементов  $\pi \in S_n$  таких, что  $\pi(n) = n$ , то, как нетрудно убедиться,  $H$  — подгруппа в  $S_n$ , которую можно отождествить с  $S_{n-1}$ . Пусть  $\tau_0 = e$ ,  $\tau_i = (i, n)$  — транспозиция, переводящая  $n$  в  $i$  ( $i = 1, 2, \dots, n-1$ ). Ясно, что

$$S_n = \bigcup_{k=0}^{n-1} \tau_k S_{n-1}.$$

Рассмотрим разложение  $S_3$  в левые и правые смежные классы по подгруппе  $\langle(12)\rangle = S_2$ :

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

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

Мы видим, что множество левых смежных классов  $gS_2$  не совпадает с множеством правых смежных классов  $S_2g'$ . Тем не менее между множествами  $\{gH\}$  и  $\{Hg'\}$  всегда имеется биективное соответствие, при котором

$$x = gh \in gH \iff x^{-1} = h^{-1}g^{-1} \in Hg^{-1}.$$

Действительно, если, например,  $h_1g_1^{-1} = h_2g_2^{-1}$ , то  $g_1 = g_2h_2^{-1}h_1$  и  $g_1H = g_2H$ . В частности, если  $\{e, x, y, z, \dots\}$  — множество представителей левых (соответственно правых) смежных классов, то  $\{e, x^{-1}, y^{-1}, z^{-1}, \dots\}$  — множество представителей правых (соответственно левых) смежных классов. Мощности этих множеств совпадают.  $\square$

Множество всех левых смежных классов  $G$  по  $H$  условимся обозначать символом  $G/H$  (или  $(G/H)_l$ , если возникает необходимость рассматривать одновременно множество  $(G/H)_r$  правых смежных классов  $G$  по  $H$ ). Для мощности  $\text{Card } G/H$  этого множества используется название “индекс подгруппы  $H$  в  $G$ ” и вводится специальное обозначение  $(G : H)$ , хорошо согласующееся с обозначением  $(G : e)$  порядка  $|G|$  группы  $G$  (число смежных классов по единичной подгруппе). Так как отображение  $H \rightarrow gH$  взаимно однозначно (вспомните доказательство теоремы Кэли и отображение  $L_g$ ), то  $\text{Card } gH = (H : e)$ . Таким образом, имеет место легко запоминающаяся формула

$$(G : e) = (G : H)(H : e),$$

из которой вытекает классическая

**Теорема 2 (Лагранж).** Порядок конечной группы делится на порядок каждой своей подгруппы.

**Следствие.** Порядок любого элемента делит порядок группы. Группа простого порядка  $p$  всегда циклическая и с точностью до изоморфизма единственная.

Действительно, порядок любого элемента  $g \in G$  совпадает с порядком порождённой им циклической подгруппы  $\langle g \rangle$  [BA I, гл. 4, § 2, теорема 2]. Если, далее,  $|G| = p$  — простое число, а  $H$  — неединичная подгруппа, то делимость  $p$  на  $|H|$  означает, что  $|H| = p$ , откуда  $H = G$ . Стало быть,  $G$  совпадает с циклической подгруппой, порождённой любым элементом  $g \neq e$ . Все циклические группы данного порядка изоморфны [BA I, гл. 4, § 2, теорема 3]. Это даёт право говорить об единственности.  $\square$

В связи с теоремой Лагранжа возникает “искушение” для каждого делителя  $m$  порядка  $n$  группы  $G$  искать в  $G$  подгруппу порядка  $m$ . Но для этого в общем-то нет оснований. Желающие могут проверить (а остальные должны подтвердить это на экзамене), что в знакопеременной группе  $A_4$  порядка 12 нет подгрупп порядка 6. Тем не менее, как мы сейчас убедимся, в некоторых группах “обращение теоремы Лагранжа” справедливо.

**2. Строение циклических групп.** Из [ВА I] нам уже известно, что все циклические группы одинакового порядка изоморфны, а порядок элемента в любой группе совпадает с порядком порождённой им циклической подгруппы. На самом деле справедлива

*Теорема 3. Всякая подгруппа циклической группы есть снова циклическая группа. Подгруппы бесконечной циклической группы  $(\mathbb{Z}, +)$  исчерпываются (бесконечными) группами  $(m\mathbb{Z}, +)$ ,  $m \in \mathbb{N}$ , а подгруппы циклической группы порядка  $q$  находятся во взаимно однозначном соответствии с (положительными) делителями  $d$  числа  $q$ .*

**Доказательство.** Будем для разнообразия рассматривать произвольную циклическую группу  $A = \langle a \rangle$  в аддитивной записи. Каждый её элемент, стало быть, имеет вид  $ka$ , где  $k \in \mathbb{Z}$  или же  $k = 0, 1, \dots, q - 1$ , если  $A$  — конечная группа порядка  $q$ . Пусть  $B$  — ненулевая подгруппа в  $A$ . Если  $ka \in B$  для какого-то  $k \neq 0$ , то и  $-ka \in B$ . Среди всех элементов  $ka \in B$  с положительными  $k$  выберем элемент  $ma$ , где  $m$  наименьшее.

Записав любое  $k > 0$  в виде  $k = lm + r$ ,  $0 \leq r < m$ , мы видим, что из  $ka \in B$  следует  $ra = ka - l(ma) \in B$ , т.е.  $r = 0$ . Значит,  $B = \langle a \rangle$  — циклическая группа.

Все бесконечные циклические группы изоморфны группе  $(\mathbb{Z}, +)$ . В данном случае образующими служат 1 или  $-1$ , так что по доказанному любая подгруппа в  $(\mathbb{Z}, +)$  определяется натуральным числом  $m$  и имеет вид

$$m\mathbb{Z} = \langle m \cdot 1 \rangle = \{0, \pm m, \pm 2m, \dots\}.$$

Очевидно, что все эти подгруппы бесконечны.

Пусть теперь  $\langle a \rangle = \{0, a, \dots, (q - 1)a\}$ ,  $qa = 0$ . Мы знаем, что  $B = \{0, ma, 2ma, \dots\}$ , где  $m \in \mathbb{N}$ , причём  $sa \in B$ ,  $s \in \mathbb{N} \implies s = mt$ . Утверждается, что  $m$  делит  $q$ . Действительно, пусть  $q = dm + r$ ,  $0 \leq r < m$ . Тогда

$$0 = qa = d(ma) + ra,$$

откуда  $ra = -d(ma) \in B$ . Минимальность  $m$  влечёт  $r = 0$ , и мы имеем  $q = dm$ . Таким образом,

$$B = \{0, ma, 2ma, \dots, (d - 1)ma\} = mA$$

— подгруппа в  $A$  порядка  $d$ . Когда  $m$  пробегает по всем положительным делителям числа  $q$ , то же самое делает  $d$ , и мы получаем ровно по одной подгруппе каждого порядка  $d$ , делящего  $q$ .  $\square$

**Следствие.** В циклической группе  $\langle a \rangle$  порядка  $q$  подгруппа порядка  $d$ ,  $d \mid q$ , совпадает с множеством элементов  $b \in \langle a \rangle$  таких, что  $db = 0$ .

**Доказательство.** Если  $dm = q$ , то  $b \in B = mA$  и  $db = 0$ . Обратно: пусть  $b = la \in \langle a \rangle$  и  $db = 0$ . Из условия  $dla = 0$  следует, что  $dl = qk = dm$ , откуда  $l = mk$  и  $b = la = k(ma) \in mA$ .  $\square$

### УПРАЖНЕНИЯ

1. Доказать, что в любой группе подгруппа индекса 2 обязательно нормальна.
2. При помощи упр. 1 попробуйте доказать, что с точностью до изоморфизма  $S_3$  — единственная неабелева группа порядка 6.

## § 3. Действие групп на множествах

**1. Гомоморфизмы  $G \rightarrow S(\Omega)$ .** Теория групп началась для нас в [ВА I, гл. 4], с примеров групп преобразований — подгрупп группы  $S(\Omega)$  всех взаимно однозначных отображений множества  $\Omega$  на себя. Этот подход соответствует как историческому пути развития теории групп, так и значению групп преобразований в других областях математики. Так называемая абстрактная теория групп, являющаяся порождением более поздней эпохи (первая половина XIX столетия), далеко отошла от групп преобразований, но многие её понятия несут на себе отпечаток старого времени. Именно, источник этих понятий чаще всего покоится на идеи *реализации (представления)* данной группы  $G$  в  $S(\Omega)$ , где  $\Omega$  — подходящим образом выбранное множество. Под реализацией  $G$  в  $S(\Omega)$  удобно понимать любой гомоморфизм  $\Phi : G \rightarrow S(\Omega)$ . Если  $\Phi_g$  — преобразование из  $S(\Omega)$ , отвечающее элементу  $g \in G$ , то  $\Phi_e = e_\Omega$  — единичное преобразование  $\Omega \rightarrow \Omega$  и  $\Phi_{gh} = \Phi_g \circ \Phi_h$ ;  $g, h \in G$ . Образ  $\Phi_g(x)$  точки (элемента)  $x \in \Omega$  относительно преобразования  $\Phi_g$  часто обозначается просто символом  $gx$ , что даёт право говорить об отображении  $(g, x) \mapsto gx$  декартова произведения  $G \times \Omega$  в  $\Omega$ . Правильнее было бы писать  $g \circ x$  или  $g * x$ , чтобы не получалось путаницы с умножением в  $G$ , но большей частью в этом нет необходимости. Отмеченные выше свойства преобразования  $\Phi_g$  записываются в виде:

- i)  $ex = x$ ,  $x \in \Omega$ ;
- ii)  $(gh)x = g(hx)$ ,  $g, h \in G$ .

Всякий раз, когда имеется отображение  $(g, x) \mapsto gx$  декартова произведения  $G \times \Omega$  в  $\Omega$ , удовлетворяющее свойствам i), ii), говорят, что группа *действует* (слева) на множестве  $\Omega$ , а  $\Omega$  является

$G$ -множеством. С другой стороны, имея  $G$ -множество  $\Omega$ , мы посредством формулы

$$\Phi_g(x) = gx, \quad x \in \Omega,$$

для каждого  $g \in G$  определим отображение  $\Phi_g : \Omega \rightarrow \Omega$ , причём из i), ii) следует, что  $\Phi : g \mapsto \Phi_g$  будет гомоморфизмом  $G$  в  $S(\Omega)$ . Говорят ещё (в особенности, когда  $|\Omega| < \infty$ ), что с действием  $G$  на  $\Omega$  ассоциировано представление  $(\Phi, \Omega)$  группы  $G$  в группу перестановок. Ядро  $\text{Ker } \Phi$  называют ядром действия группы  $G$ . Если  $\Phi$  — мономорфизм (иначе: если  $gx = x \ \forall x \in \Omega \implies g = e$ ), то говорят, что группа  $G$  действует эффективно на множестве  $\Omega$ .

**Замечание.** Каждое действие  $G$  на  $\Omega$  индуцирует действие  $G$  на  $\Omega^k = \Omega \times \dots \times \Omega$  по очевидному правилу  $g(x_1, \dots, x_k) = (gx_1, \dots, gx_k)$ . Кроме того, имеется индуцированное действие  $G$  на множестве всех подмножеств  $\mathcal{P}(\Omega)$  (см. [ВА I, гл. 1, § 5, упр. 4]). Полагаем  $g\emptyset = \emptyset$ , а если  $T$  — непустое подмножество в  $\Omega$ , то  $gT = \{gt \mid t \in T\}$ . Свойства i), ii) проверяются непосредственно. Легко понять, что  $T$  и  $gT$  имеют одинаковую мощность, так что  $G$  индуцирует действие на подмножествах одинаковой мощности.

**2. Орбиты и стационарные подгруппы точек.** Две точки  $x, x' \in \Omega$  называются эквивалентными относительно группы  $G$ , действующей на  $\Omega$ , если  $x' = gx$  для некоторого элемента  $g \in G$ . Свойства рефлексивности, симметричности и транзитивности, легко получающиеся при помощи i), ii) (см. п. 1), показывают, что мы имеем дело с истинным отношением эквивалентности, разбивающим  $\Omega$  на непересекающиеся классы эквивалентности. Эти классы эквивалентности принято называть *G-орбитами*. Орбиту, содержащую элемент  $x_0 \in \Omega$ , естественно обозначать символом  $G(x_0)$ ; таким образом,  $G(x_0) = \{gx_0 \mid g \in G\}$ . Используются, однако, и другие обозначения, подчёркивающие особенности того или иного действия  $G$  на  $\Omega$ . Понятие орбиты пришло из геометрии. Если, например,  $G = \text{SO}(2)$  — группа вращений на плоскости вокруг начальной точки  $O$ , то орбитой точки  $P$  будет служить окружность с центром в  $O$ , проходящая через  $P$ , а множество  $\Omega = \mathbb{R}^2$  будет объединением концентрических окружностей, включая окружность нулевого радиуса (точка  $O$ ). Для нас понятие орбиты также не является новым. Мы им пользовались в [ВА I, гл. 4] при разложении перестановки  $\pi \in S_n$  в произведение независимых циклов. В качестве  $G$  бралась циклическая группа  $\langle \pi \rangle$ .

Пусть  $x_0$  — фиксированная точка в  $\Omega$ . Рассмотрим множество

$$\text{St}(x_0) = \{g \in G \mid gx_0 = x_0\} \subset G.$$

Так как  $ex_0 = x_0$ , а  $g, h \in \text{St}(x_0) \implies gh^{-1} \in \text{St}(x_0)$ , то  $\text{St}(x_0)$  — подгруппа в  $G$ . Она называется *стационарной подгруппой* (или *стабилизатором*) в  $G$  точки  $x_0 \in \Omega$  и часто обозначается символом  $G_{x_0}$ . Для

рассмотренного выше действия группы  $\mathrm{SO}(2)$  на  $\mathbb{R}^2$  имеем  $\mathrm{St}(O) = \mathrm{SO}(2)$  и  $\mathrm{St}(P) = e$ , если  $P \neq O$ . В общем случае

$$gx_0 = g'x_0 \iff g^{-1}g' \in \mathrm{St}(x_0) \iff g' \in g\mathrm{St}(x_0).$$

Стало быть, левые смежные классы  $g\mathrm{St}(x_0)$  группы  $G$  по стационарной подгруппе  $\mathrm{St}(x_0)$  находятся во взаимно однозначном соответствии с точками орбиты  $G(x_0)$ . В частности,

$$\mathrm{Card} G(x_0) = \mathrm{Card}(G/\mathrm{St}(x_0)) = (G : \mathrm{St}(x_0)). \quad (1)$$

Здесь, как и раньше,  $G/\mathrm{St}(x_0)$  — фактормножество  $G$  по  $\mathrm{St}(x_0)$ , а  $(G : \mathrm{St}(x_0))$  — индекс подгруппы  $\mathrm{St}(x_0)$  в  $G$ . Мощность  $\mathrm{Card} G(x_0)$  часто называется *длиной  $G$ -орбиты точки  $x_0$* . Из (1) и из теоремы Лагранжа следует, что *длина любой орбиты относительно конечной группы  $G$  является делителем порядка группы*.

Обратим ещё внимание на то обстоятельство, что точку  $x_0$  в правой части соотношения (1) можно заменить на любую точку  $x'_0 \in G(x_0)$ . Действительно,

$$\mathrm{Card} G(x_0) = \mathrm{Card} G(x'_0) = (G : \mathrm{St}(x'_0)).$$

Более сильное утверждение о стационарных подгруппах заключается в следующем. Пусть  $x'_0 = gx_0$ . Тогда

$$\mathrm{St}(x'_0)gx_0 = \mathrm{St}(x'_0)x'_0 = x'_0 = gx_0,$$

откуда  $g^{-1}\mathrm{St}(x'_0) = x_0$ , т.е.

$$g^{-1}\mathrm{St}(x'_0)g \subset \mathrm{St}(x_0).$$

Аналогично,

$$g\mathrm{St}(x_0)g^{-1} \subset \mathrm{St}(x'_0),$$

поскольку

$$\mathrm{St}(x_0)g^{-1}x'_0 = \mathrm{St}(x_0)x_0 = x_0 = g^{-1}x'_0.$$

Значит, имеет место равенство

$$\mathrm{St}(x'_0) = g\mathrm{St}(x_0)g^{-1} = \{ghg^{-1} \mid h \in \mathrm{St}(x_0)\}.$$

В духе примера 1, рассматриваемого ниже, две подгруппы  $H, H' \subseteq G$  называются *сопряжёнными*, если  $H' = gHg^{-1}$  для некоторого  $g \in G$ . Сформулируем полученные результаты в виде теоремы.

**Теорема 1.** *Пусть группа  $G$  действует на множестве  $\Omega$ . Если две точки  $x_0, x'_0 \in \Omega$  лежат в одной орбите, то их стационарные подгруппы сопряжены:*

$$x'_0 = gx_0 \implies \mathrm{St}(x'_0) = g\mathrm{St}(x_0)g^{-1}.$$

*Если, далее,  $G$  — конечная группа и*

$$\Omega = \Omega_1 \cup \Omega_2 \cup \dots \cup \Omega_r$$

— разбиение  $\Omega$  на конечное число орбит с представителями  $x_1, x_2, \dots, x_r$ , то

$$|\Omega| = \sum_{i=1}^r (G : \text{St}(x_i)). \quad (2)$$

Формула (2) лежит в основе многих применений “метода орбит” к конечным группам.

**3. Примеры действий групп на множествах.** Мы остановимся лишь на примерах, относящихся собственно к теории групп.

Пример 1 (действие сопряжением). На  $\Omega = G$  определяется действие любого элемента  $g \in G$  посредством формулы

$$x \mapsto I_g(x) = gxg^{-1} \quad \forall x \in G.$$

Можно было бы писать  $g \circ x = gxg^{-1}$ , но мы предпочли воспользоваться старым нашим обозначением из [BA I, гл. 4, § 2, п. 4] для внутреннего автоморфизма  $I_g$ , отвечающего элементу  $g \in G$ .

Действие элемента  $g$ , отождествлённое с действием  $\text{Inn}(G)$ , называется *сопряжением* (или *трансформированием*). Его ядром служит *центр* группы  $G$ :

$$Z(G) = \{z \in G \mid I_g(z) = z \quad \forall g \in G\} = \{z \in G \mid zg = gz \quad \forall g \in G\}.$$

Орбита элемента  $x \in G = \Omega$ , обозначаемая здесь символом  $x^G$ , называется *классом сопряжённых элементов*, *классом сопряжённости* или просто *сопряжённым классом*, содержащим  $x$ . Если  $a, b \in x^G$ , то иногда пишут  $a \overset{G}{\sim} b$ . Для стационарной подгруппы  $\text{St}(x)$ , называемой в этом случае *централизатором* элемента  $x$ , чаще используется обозначение  $C(x)$  (или  $C_G(x)$ , если нужно выделить группу  $G$ ).

Действие сопряжением, согласно замечанию в конце п. 1, переносится на подмножества и подгруппы в  $G$ . Два подмножества  $H, T \subset C \subset G$  *сопряжены*, если  $T = gHg^{-1}$  при некотором  $g \in G$ .

Пусть  $H$  — подгруппа в  $G$ . Принято говорить, что

$$N(H) := N_G(H) := \text{St}(H) = \{g \in G \mid gHg^{-1} = H\}$$

— *нормализатор* подгруппы  $H$  в  $G$ . В частности,  $H \triangleleft G$  ( $H$  — нормальная подгруппа в  $G$ ), если  $N(H) = G$ , что согласуется с определениями в § 2, п. 1. В соответствии с соотношением (1) *длина орбиты*  $H^G$  (*число сопряжённых с  $H$  подгрупп*) *совпадает с индексом нормализатора*  $N(H)$  *в  $G$* .

Пусть, далее,  $G$  — конечная группа и  $x_1^G, \dots, x_r^G$  — её сопряжённые классы, причём первые  $q$  из них одноэлементные:

$$x_i^G = \{x_i\}, \quad i = 1, \dots, q \quad (x_1 = e).$$

Тогда  $Z(G) = \{x_1, x_2, \dots, x_q\}$ , а соотношения (1) и (2) переписываются в виде

$$|x_i^G| = (G : C(x_i)), \quad i = 1, \dots, q, q+1, \dots, \quad (1')$$

$$|G| = |Z(G)| + \sum_{i=q+1}^r (G : C(x_i)). \quad (2')$$

Пусть, скажем,  $G = S_3$ . Тогда  $r = 3$ ,  $q = 1$  (т.е.  $Z(S_3) = e$ ) и

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

— разбиение  $S_3$  на сопряжённые классы. Размеры этих классов (длины орбит) делят  $|S_3| = 6$ , как и предписывается соотношением (1').

Соотношение (2') приводит немедленно к следующему интересному утверждению.

**Теорема 2.** *Всякая конечная  $p$ -группа  $G$  (группа порядка  $p^n > 1$ ,  $p$  — простое число) обладает центром  $Z(G) \neq e$ .*

**Доказательство.** Если  $G$  — абелева группа, то  $G = Z(G)$ , и доказывать нечего. В противном случае  $r > q$ ,  $(G : C(x_i)) = p^{n_i}$ ,  $n_i \geq 1$  при  $i > q$ , и соотношение (2), переписанное в виде

$$p^n = |Z(G)| + \sum_{i=q+1}^r p^{n_i},$$

показывает, что  $|Z(G)|$  делится на  $p$ .  $\square$

Существование неабелевой  $p$ -группы установить легко. Достаточно рассмотреть группу верхних треугольных матриц

$$P = \left\{ \begin{array}{c} \left( \begin{array}{ccc} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{array} \right) \\ \mid a, b, c \in Z_p \end{array} \right\}$$

с коэффициентами в конечном поле из  $p$  элементов.

**Пример 2 (сдвиг).** Определённое формулой  $L_a(g) = ag$  отображение  $L_a : G \rightarrow G$ , которое мы использовали при доказательстве теоремы Кэли (см. [BA I, гл. 4, § 3]), обычно называют *левым сдвигом* на  $a$ . Так как  $eg = g$  и  $(ab)g = a(bg)$ , то левые сдвиги задают действие  $G$  на себе, которое индуцирует действие на подмножествах группы  $G$ . Пусть, в частности,  $H$  — подгруппа и  $G/H$  — множество левых смежных классов  $gH$ ,  $g \in G$ .

Ясно, что отображение

$$(x, gH) \mapsto x(gH) = (xg)H$$

определяет действие  $L^H$  группы  $G$  на  $G/H$ . Ядром  $\text{Ker } L^H$  этого действия является множество

$$\{x \in G \mid L_x^H(gH) = gH \quad \forall g \in G\} = \{x \in G \mid xgH = gH \quad \forall g \in G\}.$$

Другими словами,  $x \in \text{Ker } L^H \iff g^{-1}xg \in H$  для всех  $g \in G$ , или, что эквивалентно,  $x \in gHg^{-1} \forall g \in G$ . Таким образом,

$$\text{Ker } L^H = \bigcap_{g \in G} gHg^{-1}$$

— наибольшая нормальная подгруппа группы  $G$ , содержащаяся в  $H$ . Эффективность действия  $G$  на  $G/H$  равносильна отсутствию подгруппы  $K \subset H$ ,  $K \neq e$ , нормальной в  $G$ .

Во всяком случае, любую подгруппу  $H$  индекса  $n$  в  $G$  можно использовать для представления  $(L_x^H, G/H)$  группы  $G$  перестановками  $L_x^H$  на смежных классах  $G$  по  $H$ . Это представление (возможно, неточное) гораздо более экономно, чем то, которое получается посредством применения теоремы Кэли.

**Пример 3 (транзитивные группы).** Группу перестановок  $G \subset S_n$ , действующую на множестве  $\Omega = \{1, 2, \dots, n\}$ , называют *транзитивной*, если орбита  $G_i$  некоторой (а следовательно, и любой) точки  $i \in \Omega$  совпадает с  $\Omega$ . Другими словами, действие  $G \times \Omega \rightarrow \Omega$  транзитивно на  $\Omega$ , когда для каждой пары точек  $i, j \in \Omega$  найдётся по крайней мере один элемент  $g \in G$  с  $g(i) = j$ .

Пусть  $\Omega^{[k]}$  — совокупность упорядоченных  $k$ -элементных подмножеств в  $\Omega$ . Группа  $G$ , действующая на  $\Omega$ , индуцирует действие на  $\Omega^{[k]}$ ; если при этом имеет место транзитивность на  $\Omega^{[k]}$ , то  $G$  называется *k-транзитивной* на  $\Omega$ . Скажем, симметрическая группа  $S_n$   $n$ -транзитивна на  $\Omega$ , а знакопеременная группа  $A_n$  ( $n - 2$ )-транзитивна.

Любая группа  $G$  действует транзитивно на множестве  $G/H$  левых смежных классов  $G$  по  $H$  (см. пример 2). Действительно, если  $g_iH, g_jH$  — два смежных класса, то  $g_jg_i^{-1}(g_iH) = g_jH$ . Тем более удивительно, что получение *прямыми средствами* информации о  $k$ -транзитивных группах фиксированной степени  $n$  при  $k > 5$  весьма затруднительно. Лишь весьма окольным путём в начале 80-х годов XX столетия была доказана гипотеза К. Жордана, что всего таких групп две:  $S_n$  и  $A_n$ .

Мы собираемся получить любопытные количественные результаты о транзитивных группах, которые понадобятся нам в дальнейшем. Пусть  $G$  — транзитивная группа на  $\Omega$ . Стационарную подгруппу  $\text{St}(i)$  точки  $i \in \Omega$  обозначим символом  $G_i$ . Нам известно (см. теорему 1), что если  $i = g_i(1)$ , то  $G_i = g_iG_1g_i^{-1}$ ,  $i = 1, 2, \dots, n$  ( $g_1 = e$ ). Кроме того, элементы  $g_i$  можно выбрать в качестве представителей левых смежных классов  $G$  по  $G_1$ :

$$G = G_1 \cup g_2G_1 \cup \dots \cup g_nG_1. \quad (3)$$

В частности,  $|G| = n|G_1|$ , что согласуется с общими результатами о длинах орбит (см. п. 2).

Теорема 3. Пусть  $G$  — транзитивная группа на  $\Omega$ , и для любого  $g \in G$  пусть  $N(g)$  — число точек в  $\Omega$ , оставшихся на месте при действии  $g$ .

Тогда:

i)  $\sum_{g \in G} N(g) = |G|$  (поделив обе части равенства i) на  $|G|$ , получаем, что “в среднем” каждый элемент оставляет неподвижной одну точку;

ii) если  $G$  — 2-транзитивная группа, то  $\sum_{g \in G} N(g)^2 = 2|G|$ .

Доказательство. i) Имеем

$$\sum_{g \in G} N(g) = \sum_{j=1}^n \Gamma(j),$$

где  $\Gamma(j)$  — число элементов в  $G$ , оставляющих на месте символ  $j$ . Другими словами,  $\Gamma(j) = |G_j|$ . Но в силу транзитивности

$$|G_j| = |g_j G_1 g_j^{-1}| = |G_1|,$$

где  $g_j$  взяты из разложения (3). Стало быть,

$$\sum_{g \in G} N(g) = \sum_{j=1}^n |G_j| = \sum_{j=1}^n |G_1| = n|G_1| = |G|.$$

ii) Условие 2-транзитивности  $G$  означает, что на множестве  $\Omega_1 = \Omega \setminus \{1\}$  стационарная подгруппа  $G_1$  действует транзитивно, т.е.  $G_1$ -орбитами будут  $\{1\}$  и  $\Omega_1$ . Пусть  $N'(x)$  — число точек в  $\Omega_1$ , неподвижных при действии  $x \in G$ . Соотношение i), применённое к паре  $(G_1, \Omega_1)$ , даёт

$$\sum_{x \in G_1} N'(x) = |G_1|.$$

Так как  $N(x) = 1 + N'(x)$  для  $x \in G_1$  (добавляется точка 1), то имеем

$$\sum_{x \in G_1} N(x) = 2|G_1|.$$

Точно такие же соотношения справедливы для всех других  $G_j$ :

$$\sum_{x \in G_j} N(x) = 2|G_j| = 2|G_1|.$$

Суммируя по  $j$ , получаем

$$\sum_{j=1}^n \sum_{x \in G_j} N(x) = 2n|G_1| = 2|G|.$$

Слева  $N(x)$  считается по одному для каждой подгруппы  $G_j$ , в которой содержится  $x$ . Но  $x$  оставляет на месте  $N(x)$  точек и, следовательно, содержит ровно в  $N(x)$  подгруппах  $G_j$ . Это означает,

что каждый элемент  $x$  вносит в сумму член  $N(x)^2$ . С другой стороны, любой элемент  $y \in G$ , не содержащийся в объединении  $\bigcup_j G_j$ , переставляет все точки, так что  $N(y) = 0$ . Поэтому можно записать соотношение

$$\sum_{g \in G} N(g)^2 = \sum_{j=1}^n \sum_{x \in G_j} N(x) = 2|G|. \quad \square$$

**4. Однородные пространства.** Для геометрии особый интерес представляет тот случай, когда  $\Omega$  — топологическое пространство (например, прямая  $\mathbb{R}$  или сфера  $S^2$ ),  $G$  — так называемая непрерывная (или топологическая) группа, а действие  $(g, x) \mapsto gx$  подчиняется разумному требованию:

iii)  $f(x) = gx$  — непрерывная функция двух переменных  $g$  и  $x$ .

Группа  $G$ , действующая на  $\Omega$  так, что выполняются свойства i), ii) из п. 1 и iii), называется *группой движений* пространства  $\Omega$ . При этом могут быть движения, сохраняющие какую-нибудь метрику на  $\Omega$ . Пространство  $\Omega$  называется *однородным*, если  $G$  действует на  $\Omega$  транзитивно в смысле примера 3, т. е. все точки из  $\Omega$  принадлежат одной  $G$ -орбите.

Из общих соображений пп. 1–2 ясно, что имеется взаимно однозначное соответствие между точками однородного пространства  $\Omega$  и смежными классами  $G$  по одной из стационарных подгрупп  $H$ . При этом движению  $g \in G$  пространства  $\Omega$  отвечает отображение  $g'H \mapsto gg'H$  на множестве  $G/H$ .

Рассмотрим с новой точки зрения хорошо известный нам из § 1 пример группы  $\mathrm{SO}(3)$ . Группу  $\mathrm{SO}(3)$  удобно представлять себе действующей на двумерной сфере  $S^2$  единичного радиуса. Очевидно, что любой паре точек  $P, Q \in S^2$  отвечает некоторое движение (вращение), переводящее  $P$  в  $Q$ , т. е.  $S^2$  — однородное пространство с группой движений  $\mathrm{SO}(3)$ . Стационарная подгруппа  $\mathrm{St}(P)$  любой точки  $P \in S^2$  оставляет неподвижной всю ось, проходящую через  $P$  и центр  $O$  сферы. Поэтому  $\mathrm{St}(P) \cong \mathrm{SO}(2)$  — группа вращений плоскости, перпендикулярной к оси  $OP$ . Так как элементы группы  $\mathrm{SO}(2)$  отождествляются с точками окружности  $S^1$  единичного радиуса, то группу  $\mathrm{SO}(3)$  можно представлять себе в виде пирога, слоями которого являются единичные окружности, “пронумерованные” точками двумерной сферы:  $\mathrm{SO}(3)/S^1 \approx S^2$ . В этом случае говорят о *расщеплении* (о проекции  $p : \mathrm{SO}(3) \rightarrow S^2$ ) с *базой*  $S^2$  и *слоем*  $p^{-1}(P) \approx S^1$ ,  $P \in S^2$ . Точный смысл всех этих понятий разъясняется в курсах геометрии и топологии, поэтому мы ограничимся сказанным.

## УПРАЖНЕНИЯ

**1.** Пусть  $\Phi$  и  $\Phi'$  — гомоморфизмы группы  $G$  в  $S(\Omega)$  и  $S(\Omega')$  соответственно. Тогда определённые ими действия на  $\Omega$  и на  $\Omega'$  называются *эквивалентными*, если существует биективное отображение  $\sigma : \Omega \rightarrow \Omega'$ , делающее диаграмму

$$\begin{array}{ccc} \Omega & \xrightarrow{\sigma} & \Omega' \\ \Phi_g \downarrow & & \downarrow \Phi'_g \\ \Omega & \xrightarrow{\sigma} & \Omega' \end{array}$$

коммутативной при всех  $g \in G$ . Таким образом,  $\Phi'_g = \sigma \Phi_g \sigma^{-1}$ . Доказать, что каждое транзитивное действие группы  $G$  эквивалентно действию  $G$  на левых смежных классах по некоторой подгруппе  $H$ .

**2.** Опираясь на теорему 2, доказать, что все группы порядка  $p^2$  ( $p$  — простое число) абелевы.

**3.** Показать, что центр группы  $P$ , приведённой в конце примера 1, имеет вид

$$Z(P) = \left\{ \begin{vmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \mid c \in Z_p \right\}.$$

Найти сопряжённые классы группы  $P$ .

**4.** Пусть  $n$  — натуральное число. Запишем его в виде суммы  $n = n_1 + n_2 + \dots + n_m$  с  $n_1 \geq n_2 \geq \dots \geq n_m \geq 1$ . Число всех таких разбиений с  $m = 1, 2, \dots$  обозначим через  $p(n)$ , так что  $p(3) = 3$ ,  $p(4) = 5$  и т.д. Разложение  $\pi = \pi_1 \pi_2 \dots \pi_m$  каждой перестановки  $\pi \in S_n$  в произведение независимых циклов (см. [ВА I, гл. 1, § 8]) однозначно определяет разбиение числа  $n$ . Показать, что классы сопряжённости группы  $S_n$  находятся в биективном соответствии с разбиениями числа  $n$ .

**5.** Пусть перестановка  $\pi \in S_n$  записывается в виде произведения  $r$  циклов длины 1,  $s$  циклов длины 2,  $t$  циклов длины 3 и т.д., так что  $n = r + 2s + 3t + \dots$  Показать, что мощность сопряжённого класса в  $S_n$ , содержащего перестановку  $\pi$ , выражается формулой

$$|\pi^{S_n}| = \frac{n!}{1^r r! 2^s s! 3^t t! \dots}.$$

**6.** Пусть группа  $G$  действует на множестве  $\Omega$ . Назовём подмножество  $\Gamma \subset \Omega$  *инвариантным* относительно  $G$  (или *G-инвариантным*), если  $gx \in \Gamma$  для всех  $g \in G$  и  $x \in \Gamma$ . Например, инвариантными множествами при действии  $SO(2)$  на  $\mathbb{R}^2$  являются концентрические кольца.

Показать, что всякое инвариантное подмножество в  $\Omega$  является объединением орбит, причём  $G$ -орбита любого элемента  $x \in \Omega$  есть не что иное, как наименьшее инвариантное подмножество, содержащее  $x$ .

**7.** Показать, что для группы  $G$  с подгруппой  $H$  действие  $H \times G \rightarrow G$ , определённое сдвигом  $(h, g) \mapsto hg$ , задаёт разбиение  $G$  на правые смежные классы  $G$  по  $H$ .

**8.** Видоизменив доказательство теоремы 1, получить соотношение

$$r(G : \Omega) = \frac{1}{|G|} \sum_{g \in G} N(g),$$

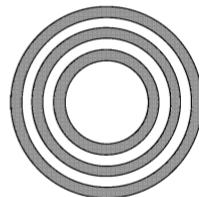


Рис. 1

где  $r(G : \Omega)$  — число орбит группы перестановок  $G$ , действующей на множестве  $\Omega$ .

**9** (G.R. Goodson, 1999). Наряду с централизатором  $C(a) = \{x \in G \mid xa = ax\}$  в группе  $G$  рассматривают ещё *косой централизатор*

$$D(a) = \{x \in G \mid xa = a^{-1}x\},$$

встречающийся в теории динамических систем. Вообще говоря,  $D(a)$  не является группой.

Доказать, что:

- 1)  $D(a)$  группа  $\iff a^2 = e$  и  $D(a) = C(a)$ ;
- 2) множество  $E(a) = C(a) \cup D(a)$  всегда является группой.

## § 4. Факторгруппы и гомоморфизмы

Этот параграф, в особенности п. 2, представляет известные трудности, и к нему нужно возвращаться несколько раз, чтобы на конкретных примерах усвоить небольшое число абстрактных утверждений.

**1. Понятие о факторгруппе.** Отношение эквивалентности  $\sim$  на группе  $G$ , определённое разложением  $G$  в смежные классы по нормальной подгруппе  $H$  (см. § 2), обладает одним замечательным свойством. Именно, если  $a, b$  — произвольные элементы группы  $G$  и  $a \sim c, b \sim d$ , то по определению имеем  $a^{-1}c = h_1 \in H, b^{-1}d = h_2 \in H$ , откуда

$$(ab)^{-1}cd = b^{-1}a^{-1}cd = b^{-1}(a^{-1}c)d = b^{-1}h_1b(b^{-1}d) = h'_1h_2 \in H$$

и, стало быть,  $ab \sim cd$ . Здесь использовано свойство нормальности  $H$  в  $G$ :  $b^{-1}h_1b = h'_1 \in H$ . Итак,

$$a \sim c, b \sim d \implies ab \sim cd.$$

Фактически это означает, что операция умножения на группе  $G$  индуцирует операцию умножения на фактормножестве  $G/\sim$ , которое мы условились обозначать  $G/H$ .

Имеет смысл говорить о композиции (об умножении) произвольных подмножеств  $A, B$  группы  $G$ , понимая под  $AB$  множество всех произведений  $ab$  с  $a \in A, b \in B$ . Ассоциативность в  $G$  влечёт соотношение

$$(AB)C = \{(ab)c\} = \{a(bc)\} = A(BC),$$

и подмножество  $H \subset G$  является подгруппой в  $G$  в точности тогда, когда  $H^2 = H, H^{-1} = \{h^{-1} \mid h \in H\} \subset H$ .

С этой точки зрения смежный класс  $aH$  равен произведению однэлементного множества  $\{a\}$  на подгруппу  $H$ . Произведением смежных классов  $aH, bH$  является множество  $aH \cdot bH$ , которое, вообще

говоря, не обязано быть снова смежным классом по  $H$ . Рассмотренное в § 2 разложение  $S_3$  по  $H = \{e, (12)\}$  показывает, например, что

$$H \cdot (13)H = (13)H \cup (23)H.$$

Совсем иная ситуация получается, когда  $H$  — нормальная подгруппа группы  $G$ . Так как  $gH = Hg$  для всех  $g \in G$ , то

$$aH \cdot bH = a(Hb)H = a(bH)H = abH^2 = abH,$$

причём рассуждения, приведённые выше, показывают, что смежный класс  $abH$  не зависит от представителей  $a, b$  смежных классов  $aH, bH$ .

Свойства

$$aH \cdot bH = abH,$$

$$H \cdot aH = aH \cdot H = aH,$$

$$a^{-1}H \cdot aH = aH \cdot a^{-1}H = eH = H$$

показывают, что справедлива

**Теорема 1.** *Если  $H$  — нормальная подгруппа в  $G$ , то операция умножения  $aH \cdot bH = abH$  наделяет фактормножество  $G/H$  строением группы, называемой факторгруппой  $G$  по  $H$ . Смежный класс  $H$  служит единичным элементом в  $G/H$ , а  $a^{-1}H = (aH)^{-1}$  — элементом, обратным к  $aH$ .*

В случае конечной группы  $G$  порядок факторгруппы  $G/H$  определяется по формуле

$$|G/H| = \frac{|G|}{|H|} = (G : H),$$

котрая вытекает из всего сказанного и из теоремы Лагранжа (см. § 2).

В случае аддитивно записываемых абелевых групп бинарная операция на  $G/H$  вводится соотношением

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

Соответственно  $G/H$  часто называют группой  $G$  по модулю  $H$ , а в применении к паре  $G = \mathbb{Z}, H = m\mathbb{Z}$  употребительно также выражение “группа  $\mathbb{Z}$  по модулю  $m$ ”.

**2. Теоремы о гомоморфизмах групп.** Согласно теореме 1 с каждой нормальной подгруппой  $K$  группы  $G$  ассоциируется некая новая группа  $G/K$ , которая была названа факторгруппой  $G$  по  $K$ . Так, наряду с эпиморфизмом  $\Phi: \mathrm{SU}(2) \rightarrow \mathrm{SO}(3)$ , описанным в § 1, естественно ввести факторгруппу  $\mathrm{SU}(2)/\{\pm E\}$  и сравнить её с образом  $\mathrm{Im} \Phi = \mathrm{SO}(3)$ . Как нетрудно догадаться,  $\mathrm{SU}(2)/\{\pm E\} \cong \mathrm{SO}(3)$ , но чтобы каждый раз не проводить рассуждения заново, полезно

установить ряд общих фактов о подгруппах, гомоморфизмах и факторгруппах. Впредь запись  $K \triangleleft G$  означает, что  $K$  — нормальная подгруппа в  $G$ .

**Теорема 2** (основная теорема о гомоморфизмах). *Пусть  $\varphi : G \rightarrow H$  — гомоморфизм групп с ядром  $K = \text{Ker } \varphi$ . Тогда  $K$  — нормальная подгруппа в  $G$  и  $G/K \cong \text{Im } \varphi$ . Обратно, если  $K \triangleleft G$ , то существует группа  $H$  (а именно  $G/K$ ) и эпиморфизм  $\pi : G \rightarrow H$ , ядро которого совпадает с  $K$ .*

( $\pi$  часто называют *естественным отображением* или *естественному гомоморфизму*.)

**Доказательство.** Мы уже знаем, что  $\text{Ker } \varphi = K \triangleleft G$ . Определим отображение  $\bar{\varphi} : G/K \rightarrow H$ , полагая

$$\bar{\varphi}(gK) = \varphi(g).$$

Если  $g_1K = g_2K$ , то  $g_1^{-1}g_2 \in K$ ,  $\varphi(g_1^{-1}) = e$ , и, стало быть,  $\varphi(g_1) = \varphi(g_2)$ , а это значит, что отображение  $\bar{\varphi}$  определено корректно (т.е. не зависит от выбора представителя смежного класса). Так как  $\bar{\varphi}(g_1K \cdot g_2K) = \bar{\varphi}(g_1g_2K) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \bar{\varphi}(g_1K)\bar{\varphi}(g_2K)$ , то  $\bar{\varphi}$  — гомоморфизм. На самом деле  $\bar{\varphi}$  — мономорфизм, потому что из  $\bar{\varphi}(g_1K) = \bar{\varphi}(g_2K)$  следует  $\varphi(g_1) = \varphi(g_2)$ , откуда  $\varphi(g_1^{-1}g_2) = e$ ,  $g_1^{-1}g_2 \in K$  и  $g_1K = g_2K$ . Ясно также, что  $\text{Im } \bar{\varphi} = \text{Im } \varphi$ .

Обратно, пусть  $K \triangleleft G$ . Возьмём в качестве  $\pi$  функцию, которая сопоставляет любому элементу из  $G$  его смежный класс по  $K$ , т.е. положим  $\pi(g) = gK$ . Ясно, что все требуемые свойства выполняются.  $\square$

Следует заметить, что заданием ядра гомоморфизма определяется неоднозначно. Например, автоморфизмы  $g \mapsto g$  и  $g \mapsto g^{-1}$  абелевой группы простого порядка  $p > 2$  различны, но ядра их совпадают ( $= e$ ).

Имея гомоморфизм  $\rho : G \rightarrow G_1$  и подгруппу  $H \subset G$ , естественно посмотреть на ограничение  $\rho|_H$  и на образ подгруппы  $H$  относительно этого гомоморфизма. Следующая теорема значительно упрощает анализ всех возможных ситуаций.

**Теорема 3** (первая теорема об изоморфизме). *Пусть  $G$  — группа,  $H$  и  $K$  — её подгруппы, причём  $K$  нормальна в  $G$ . Тогда  $HK = KHK$  — подгруппа в  $G$ , содержащая  $K$ . Далее, пересечение  $H \cap K$  является нормальной подгруппой в  $H$ , а отображение*

$$\varphi : hK \longmapsto h(H \cap K)$$

— изоморфизмом групп

$$HK/K \cong H/(H \cap K).$$

**Доказательство.** Условие  $K \triangleleft G$ , переписанное в виде  $gK = Kg$ ,  $g \in G$ , означает, в частности, что  $hK = Kh$  для всех  $h \in H$ .

Множество  $HK = \{hk \mid h \in H, k \in K\}$  состоит из некоторого числа смежных классов  $hK$ :  $HK = \bigcup_{h \in H} hK$ . Заменив здесь  $hK$  на  $Kh$ , мы придём к равенству

$$HK = \bigcup_{h \in H} hK = \bigcup_{h \in H} Kh = KH.$$

Очевидно, что единичный элемент  $e$ , содержащийся в  $H$  и  $K$ , содержится также в  $HK$ . Далее,  $(hk)^{-1} = k^{-1}h^{-1} = h^{-1}(kh^{-1})^{-1}$ , поэтому обратные ко всем элементам из  $HK$  лежат в  $HK$ . Наконец,  $HK \cdot HK = H \cdot KH \cdot K = H \cdot HK \cdot K = HK$ , т.е. множество  $HK$  замкнуто относительно умножения. Мы видим, что подмножество  $HK \subset G$  является подгруппой в  $G$ .

Так как  $K \subset HK$  и  $K \triangleleft HK$ , то имеет смысл говорить о факторгруппе  $HK/K$ . Пусть  $\pi: G \rightarrow G/K$  — естественный эпиморфизм и  $\pi_0 := \pi|_H$  — ограничение  $\pi$  на  $H$ . Его образ  $\text{Im } \pi_0$  состоит из смежных классов  $hK$ ,  $h \in H$ , т.е. из всех смежных классов  $G$  по  $K$ , имеющих представителей в  $H$ . Другими словами,  $\text{Im } \pi_0 = HK/K$ . Итак, мы имеем эпиморфизм

$$\pi_0: H \rightarrow HK/K.$$

Его ядро  $\text{Ker } \pi_0$ , состоит из  $h \in H$ , для которых  $\pi_0(h) = hK = K$  — единица в  $HK/K$ . Но  $hK = K \iff h \in H \cap K$ , откуда  $\text{Ker } \pi_0 = H \cap K$ . Как всякое ядро гомоморфизма,  $H \cap K$  — нормальная подгруппа в  $H$  (что без труда проверяется непосредственно).

По основной теореме о гомоморфизмах (теорема 2) соответствие  $\bar{\pi}_0: h(H \cap K) \mapsto \pi_0(h) = hK$  устанавливает изоморфизм  $H/(H \cap K) \cong HK/K$ . Так как  $\bar{\pi}_0$  — биективное отображение, то  $\varphi := \bar{\pi}_0^{-1}: hK \mapsto h(H \cap K)$  также является изоморфизмом групп  $HK/K$  и  $H/(H \cap K)$ .  $\square$

Коль скоро имеется первая теорема об изоморфизме, то должна существовать и вторая. Так оно и есть, но мы сформулируем лишь облегчённый ее вариант, носящий специальное название.

**Теорема 4** (теорема о соответствии). *Пусть  $G$  — группа,  $H$  и  $K$  — её подгруппы, причём  $K \triangleleft G$  и  $K \subset H$ . Тогда  $\bar{H} = H/K$  — подгруппа в  $\bar{G} = G/K$  и  $\pi^*: H \mapsto \bar{H}$  является биективным отображением множества  $\Omega(G, K)$  подгрупп в  $G$ , содержащих  $K$ , на множество  $\Omega(\bar{G})$  всех подгрупп группы  $\bar{G}$ . Если  $H \in \Omega(G, K)$ , то  $H \triangleleft G \iff \bar{H} \triangleleft \bar{G}$ , причём*

$$G/H \cong \bar{G}/\bar{H} = (G/K)/(H/K).$$

**Доказательство.** Пусть  $H \in \Omega(G, K)$ . Из определения  $G/K$  непосредственно вытекает, что  $H/K$  — подгруппа в  $G/K$ . Чтобы убедиться в инъективности отображения  $\pi^*: H \mapsto \bar{H}$ , рассмотрим две подгруппы  $H_1, H_2 \in \Omega(G, K)$ , для которых  $H_1/K = H_2/K$ . Тогда

$h_1 \in H_1 \Rightarrow h_1 K = h_2 K$ ,  $h_2 \in H_2 \Rightarrow h_1 = h_2 k$ , а так как  $K \subset H_2$ , то  $h_1 \in H_2$ , откуда  $H_1 \subset H_2$ . Аналогично проверяется включение  $H_2 \subset H_1$ . Стало быть,  $H_1 = H_2$ .

Установим теперь сюръективность отображения  $\pi^*$ . Пусть  $\overline{H} \in \Omega(\overline{G})$  и  $H$  — множество тех элементов в  $G$ , из которых состоят все смежные классы по  $K$  — элементы группы  $\overline{H} \subset \overline{G}$ . Тогда, в частности,  $K \subset H$  и  $a, b \in H \Rightarrow aK, bK \in \overline{H} \Rightarrow abK = aKbK \in \overline{H} \Rightarrow ab \in H$  и  $a \in H \Rightarrow aK \in \overline{H} \Rightarrow a^{-1}K = (aK)^{-1} \in \overline{H} \Rightarrow a^{-1} \in H$ . Стало быть,  $H$  — подгруппа в  $G$ , причём  $\overline{H} = H/K$  (обычно  $H$  называют *прообразом* в  $G$  подгруппы  $\overline{H} \subset \overline{G}$ ).

Довольно очевидна импликация  $H \in \Omega(G, K)$ ,  $H \triangleleft G \Rightarrow \overline{H} \triangleleft \overline{G}$ , формально вытекающая из равенств  $gKhK \cdot (gK)^{-1} = ghg^{-1}K = h'K \in \overline{H}$  для всех  $g \in G, h \in H$ . Но по тем же причинам  $\overline{H} \triangleleft \overline{G} \Rightarrow ghg^{-1}K = gK \cdot hK \cdot (gK)^{-1} = h'K \Rightarrow ghg^{-1} \in H \Rightarrow H \triangleleft G$ .

Наконец, в ситуации  $H \in \Omega(G, K)$ ,  $H \triangleleft G$ , по доказанному можно рассмотреть два естественных эпиморфизма

$$\pi : G \longrightarrow G/K, \quad \bar{\pi} : \overline{G} \longrightarrow \overline{G}/\overline{H}$$

( $\bar{g} \mapsto \bar{\pi}(\bar{g})$ , где  $\bar{g} = gK \in \overline{G}$ ) и их композицию — эпиморфизм

$$\sigma = \bar{\pi} \circ \pi : G \longrightarrow \overline{G}/\overline{H},$$

определенный правилом  $\sigma(g) = \bar{\pi}(\bar{g}) = \bar{g}\overline{H}$ . Имеем

$$\begin{aligned} \text{Ker } \sigma &= \{g \in G \mid \sigma(g) = \overline{H}\} = \{g \in G \mid \bar{g} \in \overline{H}\} = \\ &= \{g \in G \mid gK = hK \text{ для некоторого } h \in H\} = H. \end{aligned}$$

Следовательно, по основной теореме о гомоморфизмах отображение  $gH \mapsto \bar{g}\overline{H}$  является изоморфизмом между  $G/H$  и  $\overline{G}/\overline{H}$ .  $\square$

Пример 1. Пусть  $n = dm$  — натуральное число с делителем  $d > 1$ . Очевидно, что  $n\mathbb{Z} \subset d\mathbb{Z}$ , и отображение  $x \mapsto dx + n\mathbb{Z}$  является эпиморфизмом аддитивных групп:

$$\mathbb{Z} \longrightarrow d\mathbb{Z}/n\mathbb{Z} = \{di + n\mathbb{Z} \mid i = 0, 1, \dots, m-1\},$$

с ядром  $m\mathbb{Z}$ . По теореме 2 имеем изоморфизм

$$Z_m := \mathbb{Z}/m\mathbb{Z} \cong d\mathbb{Z}/n\mathbb{Z}$$

(что довольно понятно и так). При помощи теоремы 4 находим

$$\mathbb{Z}/d\mathbb{Z} \cong (\mathbb{Z}/n\mathbb{Z})/(d\mathbb{Z}/n\mathbb{Z}),$$

т.е.  $Z_d \cong Z_n/Z_m$ .

Вспоминая о теореме Лагранжа, мы приходим к утверждению, что *все подгруппы и факторгруппы циклической группы сами являются циклическими группами*.

Этот результат можно получить, конечно, и без теорем о гомоморфизмах.

Пример 2. Выделим в симметрической группе  $S_4$  подгруппы

$$V_4 = \{e, (12)(34), (13)(24), (14)(23)\} \triangleleft S_4,$$

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

(в данном случае  $S_3$  — стационарная подгруппа точки  $i = 4$ ). Так как, очевидно,  $S_3 \cap V_4 = e$ , то для подгруппы  $H = S_3 V_4$  по теореме 3 имеем

$$H/V_4 \cong S_3/(S_3 \cap V_4) \cong S_3.$$

В частности,  $|H| = |V_4| \cdot |S_3| = 24$ , т.е.  $H = S_4$ . Итак,  $S_4$  обладает подгруппой, изоморфной  $S_3$ , и аналогичной факторгруппой. Применяя теорему 4, мы получаем описание множества  $\Omega(S_4, V_4)$  подгрупп в  $S_4$ , содержащих  $V_4$ :

$$\Omega(S_4, V_4) = \{V_4, \langle(12)\rangle V_4, \langle(13)\rangle V_4, \langle(23)\rangle V_4, A_4 = \langle(123)\rangle V_4, S_4\}$$

Обратим внимание на то обстоятельство, что для любого делителя  $d$  числа 24 в  $S_4$  имеется хотя бы одна подгруппа порядка  $d$ . В частности, имеется ровно четыре подгруппы  $\langle(123)\rangle, \langle(124)\rangle, \langle(134)\rangle, \langle(234)\rangle$  порядка 3 и три подгруппы  $\langle(12)\rangle V_4, \langle(13)\rangle V_4, \langle(23)\rangle V_4$  порядка 8 (это так называемые 3-силовские и 2-силовские подгруппы). Собственных (т.е. не равных  $e$  и  $S_4$ ) нормальных подгрупп всего две:  $V_4$  и  $A_4$ .

Действительно, если  $K \triangleleft S_4$  и  $K \cap V_4 \neq e$ , то  $K \supset V_4$ , потому что неединичные элементы в  $V_4$  все сопряжены относительно  $S_4$ . Обращаясь к множеству  $\Omega(S_4, V_4)$ , мы видим, что  $K = V_4$  или  $K = A_4$ . Если же  $K \cap V_4 = e$ ,  $K \neq e$ , то

$$K \triangleleft S_4, \quad V_4 \triangleleft S_4 \implies KV_4 \triangleleft S_4,$$

и остается принять, что  $KV_4 = S_4$ ,  $K \cong S_3$ . Но  $S_3$  содержит транспозицию, а все транспозиции сопряжены в  $S_4$  и порождают  $S_4$ . С другой стороны, они должны содержаться в  $K$ . Полученное противоречие показывает, что случай  $K \cap V_4 = e$  невозможен.

### 3. Коммутант. Выражение

$$(x, y) = xyx^{-1}y^{-1},$$

называемое *коммутатором* элементов  $x, y$  группы  $G$ , служит корректирующим членом, необходимым для того, чтобы поменять местами  $x$  и  $y$ :

$$xy = (x, y)yx.$$

Если  $x$  и  $y$  перестановочны, то  $(x, y) = e$ . Интуитивно ясно, что чем больше в группе  $G$  коммутаторов, отличных от  $e$ , тем значительнее отклонение закона умножения в  $G$  от коммутативного. Пусть  $M$  — множество всех коммутаторов в  $G$ . *Коммутантом* (или *произвольной подгруппой*) группы  $G$  называют подгруппу  $G'$  ( $= G^{(1)} = = (G, G)$ ), порождённую множеством  $M$  (см. [BA I, гл. 4, § 2, упр. 1, 2]):

$$G' = \langle(x, y) \mid x, y \in G\rangle := \text{gr}(x, y).$$

Хотя  $(x, y)^{-1} = yxy^{-1}x^{-1} = (y, x)$  — коммутатор, произведение двух коммутаторов быть им уже не обязано, так что  $G'$  состоит из всех возможных произведений вида

$$(x_1, y_1)(x_2, y_2) \dots (x_k, y_k), \quad x_i, y_i \in G.$$

Конечно, в каждом конкретном случае желательно иметь более точное описание коммутанта  $G'$ .

Пример.  $G = S_n$ . Коммутатор  $(\alpha, \beta) = \alpha\beta\alpha^{-1}\beta^{-1}$  любых двух перестановок  $\alpha, \beta \in S_n$  является, очевидно, чётной перестановкой. Поэтому  $S'_n \subset A_n$ . Далее,

$$(ij)(ik)(ij)^{-1}(ik)^{-1} = (ij)(ik)(ij)(ik) = (ijk),$$

а так как тройными циклами  $(ijk)$  порождается вся знакопеременная группа  $A_n$  (см. [ВА I, гл. 4, § 2, упр. 11]), то мы приходим к выводу, что  $S'_n = A_n$ .

Отметим, что  $S'_n \triangleleft S_n$ , и факторгруппа  $S_n/S'_n$  абелева.

Возвращаясь к общей ситуации, мы рассмотрим произвольный гомоморфизм групп  $\varphi: G \rightarrow \overline{G}$ . Так как

$$\varphi((x, y)) = \varphi(xyx^{-1}y^{-1}) = \varphi(x)\varphi(y)\varphi(x)^{-1}\varphi(y)^{-1},$$

то  $\varphi(G') \subset (\overline{G})'$ , причём  $\varphi(G') = (\overline{G})'$ , если  $\varphi$  — эпиморфизм. Пусть теперь  $K$  — нормальная подгруппа в  $G$  и  $\varphi = I_a: x \mapsto axa^{-1}$  — внутренний автоморфизм группы  $G$ , индуцирующий какой-то эндоморфизм на  $K$ . Согласно сказанному выше  $I_a(K') \subset K'$  при любом  $a \in G$ , а это означает, что

$$K \triangleleft G \implies K' \triangleleft G. \quad (1)$$

В частности,  $G' \triangleleft G$ .

Докажем теперь общее утверждение, вскрывающее внутренний смысл понятия коммутанта.

**Теорема 5.** Любая подгруппа  $K \subset G$ , содержащая коммутант  $G'$  группы  $G$ , нормальна в  $G$ . Факторгруппа  $G/G'$  абелева и  $G'$  содержится в каждой нормальной подгруппе  $K$  такой, что  $G/K$  абелева (в частности, максимальный порядок абелевой факторгруппы  $G/K$  равен индексу  $(G : G')$ ).

**Доказательство.** Если  $x \in K$ ,  $g \in G$  и  $G' \subset K$ , то  $gxg^{-1} = (gxg^{-1}x^{-1})x = (g, x)x \in G'K = K$ , так что  $K \triangleleft G$ . Далее, из условий  $G' \subset K$ ,  $K \triangleleft G$ , выполняющихся, в частности, при  $K = G'$  (см. (1)), следует, что

$$(aK, bK) = aK \cdot bK \cdot a^{-1}K \cdot b^{-1}K = aba^{-1}b^{-1}K = (a, b)K = K,$$

т. е. коммутатор любых двух элементов факторгруппы  $G/K$  равен единичному элементу ( $= K$ ). Стало быть,  $G/K$  — абелева группа. Обратно, если  $K \triangleleft G$  и факторгруппа абелева, то

$$(a, b)K = (aK, bK) = K$$

для всех  $a, b \in G$ . Значит,  $(a, b) \in K$  и  $G' \subseteq K$ , поскольку  $G'$  порождается коммутаторами.  $\square$

**Замечание.** Мы знаем теперь две важные нормальные подгруппы любой группы  $G$ : центр  $Z(G)$  и коммутант  $G'$ . Связь между ними, вообще говоря, слабая, но общая закономерность такова: чем “ближе”  $G$  к абелевой группе, тем больше  $Z(G)$  и тем меньше  $G'$ . Более интересен следующий факт.

Факторгруппа  $G/Z(G)$  неабелевой группы  $G$  по центру  $Z(G)$  не может быть циклической.

Действительно, если  $G/Z(G)$  — циклическая группа, то  $G = \bigcup_i a^i Z(G)$ , и любой элемент из  $G$  имеет вид  $g = a^i z$ ,  $z \in Z(G)$ . В таком случае  $(g, h) = (a^i z, a^j z') = a^{i+j-i-j}(z, z') = e$  для любых двух элементов  $g, h \in G$ , а это значит, что  $G' = e$  и  $G$  — абелева группа, вопреки предположению.  $\square$

**4. Произведения групп.** Сейчас мы рассмотрим конструкцию, позволяющую по заданным группам строить новые группы. В различных частных случаях эта конструкция нам уже встречалась. Назовём (*внешним*) *прямым произведением* произвольных групп  $A$  и  $B$  множество  $A \times B$  всех упорядоченных пар  $(a, b)$  (не путать с коммутаторами!), где  $a \in A$ ,  $b \in B$ , с бинарной операцией

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

Строго говоря, следовало бы писать  $(a_1, b_1) * (a_2, b_2) = (a_1 \circ a_2, b_1 \diamond b_2)$ , где  $\circ, \diamond, *$  — бинарные операции на  $A, B$  и  $A \times B$  соответственно, но для упрощения записи все операции условимся обозначать точкой (впрочем, опуская и её). При аддитивной записи групп, например, абелевых, естественно говорить о прямой сумме  $A \oplus B$ .

В  $A \times B$  содержатся подгруппы  $A \times e, e \times B$ , изоморфные соответственно  $A$  и  $B$  (ещё одна условность: единичные элементы в  $A$  и  $B$  обозначаются одним символом  $e$ ). Отображение  $\varphi: A \times B \rightarrow B \times A$ , заданное равенством  $\varphi((a, b)) = (b, a)$ , очевидно, устанавливает изоморфизм групп  $A \times B$  и  $B \times A$ . Если у нас есть три группы  $A, B, C$ , то можно говорить о прямых произведениях  $(A \times B) \times C$  и  $A \times (B \times C)$ . Положив  $\psi(((a, b), c)) = (a, (b, c))$ , мы легко убеждаемся в том, что

$$(A \times B) \times C \cong A \times (B \times C).$$

Свойства коммутативности и ассоциативности прямого произведения дают нам возможность говорить о прямом произведении любого конечного числа групп  $G_1, G_2, \dots, G_n$  и писать

$$G_1 \times G_2 \times \dots \times G_n = \prod_{i=1}^n G_i,$$

не указывая явно посредством скобок, в каком порядке берутся попарные прямые произведения (мы превращаем тем самым множество всех групп в коммутативную полугруппу, элементами которой являются группы).

**Теорема 6.** Пусть  $G$  — группа с нормальными подгруппами  $A$  и  $B$ . Если  $A \cap B = e$  и  $AB = G$ , то  $G \cong A \times B$ .

**Доказательство.** Из равенства  $AB = G$  следует, что любой элемент  $g \in G$  записывается в виде  $g = ab$ , где  $a \in A, b \in B$ . Если

ещё  $g = a_1 b_1$ ,  $a_1 \in A$ ,  $b_1 \in B$ , то  $ab = a_1 b_1 \Rightarrow a_1^{-1} a = b_1 B^{-1} \in A \cap B = e$ . Следовательно,  $a_1 = a$ ,  $b_1 = b$ , и мы приходим к выводу, что запись  $g = ab$  однозначна. Далее,  $A \triangleleft G \Rightarrow k = a(ba^{-1}b^{-1}) = aa' \in A$ ;  $B \triangleleft G \Rightarrow k = (aba^{-1})b^{-1} = b'b^{-1} \in B$ , т. е. коммутатор  $k \in A \cap B = e$  — единичный элемент, и, стало быть,  $ab = ba$ .

Определим теперь отображение  $\varphi: G \rightarrow A \times B$ , полагая  $\varphi(g) = (a, b)$  для любого  $g = ab$ . Согласно вышесказанному  $\varphi(gg') = \varphi(aba'b') = \varphi(aa'bb') = (aa', bb') = (a, b)(a', b') = \varphi(ab)\varphi(a'b') = \varphi(g)\varphi(g')$ . Далее,  $\varphi(ab) = (e, e) \Leftrightarrow a = e, b = e$ , т. е.  $\text{Ker } \varphi = e$ . Эпиморфность  $\varphi$  очевидна. Таким образом,  $\varphi$  удовлетворяет всем свойствам изоморфного отображения групп.  $\square$

Группу  $G$ , удовлетворяющую условиям теоремы 6, принято называть (*внутренним*) *прямым произведением* своих подгрупп  $A, B$ . Отличие от внешнего прямого произведения состоит в том, что  $G$  содержит в качестве прямых множителей сами группы  $A, B$ , а не просто их изоморфные копии  $A \times e, e \times B$ . Разумеется, внешнее прямое произведение  $G = A \times B$  является также внутренним произведением подгрупп  $A \times e, e \times B$ , и при некотором навыке можно не делать различия между ними, употребляя сокращённое словосочетание “*прямое произведение*”.

Некоторую информацию о гомоморфизмах прямых произведений даёт

**Теорема 7.** Пусть  $G = A \times B$ , и пусть  $A_1 \triangleleft A, B_1 \triangleleft B$ . Тогда  $A_1 \times B_1 \triangleleft G$  и  $G/(A_1 \times B_1) \cong (A/A_1) \times (B/B_1)$ . В частности,  $G/A \cong B$ .

**Доказательство.** Пусть  $\alpha: A \rightarrow A/A_1$  и  $\beta: B \rightarrow B/B_1$  — естественные гомоморфизмы. Определим отображение  $\varphi: G \rightarrow (A/A_1) \times (B/B_1)$  посредством соотношения  $\varphi(ab) = (\alpha(a), \beta(b))$ . Непосредственно проверяется, что  $\varphi$  — гомоморфизм с ядром  $\text{Ker } \varphi = A_1 \times B_1$  и образом  $\text{Im } \varphi = (A/A_1) \times (B/B_1)$ .  $\square$

Как и в теории векторных пространств, легко доказать, что если  $G$  — группа с нормальными подгруппами  $G_1, \dots, G_n$ , то  $G \cong \prod_i G_i$  в том и только том случае, когда

$$G = \langle G_1, \dots, G_n \rangle \text{ и } G_j \cap \langle G_1, \dots, \widehat{G_j}, \dots, G_n \rangle$$

для всех  $j$  (“шапка” над  $G_j$  означает, что компонента  $G_j$  опущена). То же самое выражается следующим свойством:  $G$  — *прямое произведение* своих нормальных подгрупп  $G_1, \dots, G_n$ , коль скоро каждый элемент  $g \in G$  допускает, и притом однозначную, запись в виде  $g = g_1 \dots g_n$ ,  $g_i \in G_i$ . Прямое произведение  $n$  экземпляров группы  $H$  называют ещё *n-й прямой степенью* и обозначают  $H^n = H \times \dots \times H$ . В  $H^n$  выделяется специальная подгруппа — *диагональ*  $\Delta = \{(h, h, \dots, h) \mid h \in H\}$ , изоморфная  $H$ .

Если в теореме 6 опустить условие  $B \triangleleft G$ , то мы придём к понятию *полупрямого произведения*:  $G = AB$ ,  $A \cap B = e$ ,  $A \triangleleft G$  (иногда пишут

$G = A \lambda B$ ). В это определение следовало бы внести ещё описание действия подгруппы  $B$  автоморфизмами на нормальной подгруппе  $A$ , что обычно и делается в каждом конкретном случае.

**Замечание.** В виде прямых и полуправых произведений представляются многие известные нам группы. Например,  $S_n$  — полуправое произведение нормальной подгруппы  $A_n$  и циклической группы  $\langle (12) \rangle$  порядка 2:  $S_n \cong A_n \lambda Z_2$ . Используя обозначения из примера 2 п. 2, можно записать

$$A_4 = V_4 \lambda \langle (123) \rangle \cong (Z_2 \times Z_2) \lambda Z_3,$$

$$S_4 = V_4 \lambda S_3 \cong (Z_2 \times Z_2) \lambda (Z_3 \lambda Z_2).$$

Ещё один пример: группа  $A(1, \mathbb{R})$  аффинных преобразований  $\mathbb{R} \rightarrow \mathbb{R}$  (см. [ВА I, гл. 4] или [ВА II]) является полуправым произведением нормальной подгруппы сдвигов и подгруппы  $GL(1, \mathbb{R})$  преобразований, оставляющих точку  $x = 0$  на месте.

**5. Образующие и определяющие соотношения.** Вопрос о системах образующих группы  $G$  уже обсуждался в [ВА I, гл. 4]. Мы возвращаемся к нему, чтобы взглянуть на некоторые известные нам группы с новой точки зрения. Из результатов [ВА I, гл. 4] вытекает, что для циклических групп нет необходимости составлять громоздкие таблицы Кэли. Условная запись

$$C_n = \langle c \mid c^n = e \rangle \tag{3}$$

даёт всю необходимую информацию об абстрактной циклической группе  $C_n$  порядка  $n$ ; подразумевается, что  $C_n = \{e, c, c^2, \dots, c^{n-1}\}$ , причём  $c^s c^t = c^{s+t}$  при  $s + t < n$  и  $c^s c^t = c^{s+t-n}$  при  $s + t \geq n$ . С другой стороны, любая циклическая группа является с точностью до изоморфизма гомоморфным образом одной-единственной группы  $(\mathbb{Z}, +)$ .

Пусть теперь  $F_n$  — произвольная группа с нейтральным элементом  $e$ , порождённая  $n$  образующими  $f_1, \dots, f_n$ , так что каждый её элемент  $f$  записывается (возможно, многими способами) в виде

$$f = f_{i_1}^{s_1} f_{i_2}^{s_2} \cdots f_{i_k}^{s_k}, \quad i_j \in \{1, 2, \dots, n\}, s_j \in \mathbb{Z}, \tag{4}$$

где  $i_j \neq i_{j+1}$ ,  $j = 1, 2, \dots, k - 1$ . Это всегда достигается элементарными заменами  $f_i^s f_i^t = f_i^{s+t}$ ,  $f_i^0 = e$  и  $f_j e = e f_j = f_j$ .

При выполнении условия  $f = e \iff s_1 = \dots = s_k = 0$  для каждого  $f$ , записанного в виде (4), говорят, что  $F_n$  — свободная группа ранга  $n$ , порождённая  $n$  свободными образующими. Элементы группы  $F_n$  обычно называются словами в алфавите  $\{f_1, f_1^{-1}, \dots, f_n, f_n^{-1}\}$ . Несократимая запись (4) слова  $f$  и его длина  $l(f) = |s_1| + |s_2| + \dots + |s_k|$  однозначно определены; в противном случае пустое слово  $e := \emptyset = f f^{-1}$  (единичный элемент в  $F^n$ ) имело бы длину  $> 0$ . При данном  $n$

две свободные группы  $F_n$  и  $G_n$ , порождённые свободными образующими  $f_1, \dots, f_n$  и  $g_1, \dots, g_n$  соответственно, изоморфны; достаточно положить  $\Phi(f_i) = g_i$ ,  $1 \leq i \leq n$ , а для произвольного слова  $f$  вида (4) считать

$$\Phi(f) = g_{i_1}^{s_1} g_{i_2}^{s_2} \dots g_{i_k}^{s_k}$$

(единицы в  $F_n$  и  $G_n$  обозначаются одинаковыми символами). Если, однако,  $G_n$  не является свободной группой, то  $\Phi$  будет всего лишь эпиморфизмом с ядром  $\text{Кер } \Phi$ , состоящим из тех слов, которые при подстановке  $f_i \mapsto g_i$  переходят в единичный элемент группы  $G_n$ . Это универсальное свойство (возможность продолжения  $f_i \mapsto g_i$ ,  $1 \leq i \leq n$ , до эпиморфизма  $\Phi : F_n \rightarrow G_n$  для любой группы  $G_n$  с  $n$  образующими) можно принять за определение свободной группы  $F_n$ , но мы не будем на этом задерживаться.

Чтобы свободные группы не казались “мистическими объектами”, приведём некоторые их конкретные реализации.

$n = 1$ .  $F_1 \cong (\mathbb{Z}, +)$  — свободная абелева группа ранга 1, или, что то же самое, бесконечная циклическая группа.

$n = 2$ . Пусть  $\mathbb{Z}[t]$  — кольцо многочленов от  $t$  с целыми рациональными коэффициентами. В специальной линейной группе  $\text{SL}(2, \mathbb{Z}[t])$  рассмотрим подгруппу  $F$ , порождённую матрицами

$$A = \begin{vmatrix} 1 & t \\ 0 & 1 \end{vmatrix}, \quad B = \begin{vmatrix} 1 & 0 \\ t & 1 \end{vmatrix}.$$

Докажем, что  $F$  — свободная группа. Лёгкая индукция по  $k$  показывает, что элемент

$$W_k = A^{\alpha_1} B^{\beta_1} \dots A^{\alpha_k} B^{\beta_k}, \quad \alpha_i, \beta_i \neq 0, \quad 1 \leq i \leq k,$$

имеет вид

$$W_k = \begin{vmatrix} 1 + \dots + \sigma_k t^{2k} & t(\dots + \sigma_{k-1} \alpha_k t^{2(k-1)}) \\ t(\dots + \alpha_1^{-1} \sigma_k t^{2(k-1)}) & 1 + \dots + \alpha_1^{-1} \sigma_{k-1} \alpha_k t^{2(k-1)} \end{vmatrix},$$

где  $\sigma_k = \alpha_1 \beta_1 \dots \alpha_k \beta_k$ , а точками обозначены одночлены меньшей степени относительно  $t$ . Ясно, что  $W_k \neq E$ . Произвольный элемент группы  $F$  записывается либо в виде  $B^\beta A^\alpha \neq E$ , либо в виде  $W = B^\beta W_k A^\alpha$ . Если  $W = E$ , то  $W_k = B^{-\beta} A^{-\alpha}$ , что, однако, невозможно (сравнить степени при  $k > 1$ , а при  $k = 1$  сделать непосредственную проверку).

Небольшое дополнительное рассуждение показывает, что при подстановке  $t = m$ , где  $m$  — любое целое число  $\geq 2$ , группа  $F$  продолжает оставаться свободной.

Введём теперь следующее

**Определение.** Пусть  $F_n$  — свободная группа с  $n$  свободными образующими  $f_1, \dots, f_n$ ,  $S = \{w_i, i \in I\}$  — некоторое подмножество элементов  $w_i(f_1, \dots, f_n) \in F_n$  и  $K = \langle S^{F_n} \rangle$  — наименьшая

нормальная подгруппа в  $F_n$ , содержащая  $S$  (пересечение всех нормальных подгрупп, содержащих  $S$ ). Говорят, что группа  $G$  задана  $n$  образующими  $a_1, \dots, a_n$  и соотношениями  $w_i(a_1, \dots, a_n) = e$ ,  $i \in I$ , если существует эпиморфизм  $\pi: F_n \rightarrow G$  с ядром  $K$  такой, что  $\pi(f_k) = a_k$ ,  $1 \leq k \leq n$ . При этом пишут

$$G = \langle a_1, \dots, a_n \mid w_i(a_1, \dots, a_n) = e, i \in I \rangle$$

и называют  $G$  *конечно определённой группой*, коль скоро  $\text{Card } I < \infty$ .

Сама группа  $F_n$  “свободна от соотношений”, чем и объясняется её название. Из определения следует, что любая группа  $H$  с  $n$  образующими  $b_1, \dots, b_n$ , которые удовлетворяют тем же соотношениям  $w_i(b_1, \dots, b_n) = e$ ,  $i \in I$ , и, возможно, некоторым другим, является гомоморфным образом группы  $G$ . В частности,  $|H| \leq |G|$ . Вообще говоря, одна и та же группа допускает много разных заданий образующими и соотношениями, хотя для конкретной группы  $G$  иногда не так легко указать хотя бы одно задание. Самое существенное заключается в том, что не существует общего алгоритма, который для любой конечно определённой группы давал бы ответ на вопрос о конечности группы, о равенстве двух её слов и т.д. В этой области развит обширный аппарат комбинаторной теории групп. Рассмотрим пока пару содержательных примеров, где все упомянутые вопросы решаются до конца.

**Пример 1 (группа диэдра).** Группа  $G = \langle a, b \mid a^3 = b^2 = abab = e \rangle$  с двумя образующими и тремя соотношениями имеет порядок  $|G| \leq 6$ , поскольку  $ba = a^{-1}b^{-1} = (a^3)^{-1}a^2b \cdot (b^2)^{-1} = a^2b$  и  $G$ , во всяком случае, исчерпывается элементами  $e, a, a^2, b, ab, a^2b$ . Так как для перестановок  $(123), (12)$ , порождающих  $S_3$ , выполняются соотношения  $(123)^3 = (12)^2 = (123)(12)(123)(12) = e$ , то отображение  $\varphi: G \rightarrow S_3$ , определённое соответственно  $a \mapsto (123)$ ,  $b \mapsto (12)$ , будет изоморфизмом  $G \cong S_3$ . Стало быть, симметрическая группа  $S_3$  задаётся двумя образующими и тремя соотношениями. Напомним, что  $S_3$  отождествляется также с группой всех преобразований симметрий правильного треугольника.

Полная группа преобразований симметрий правильного  $n$ -угольника  $P_n$  называется *группой диэдра (диэдральной группой)* и обозначается символом  $D_n$ . Вращение

$$\mathcal{A} = \begin{vmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{vmatrix}$$

многоугольника в его плоскости на угол  $\theta = 2\pi/n$  вокруг центра  $O$ , расположенного в начале прямоугольной системы координат, порождает циклическую группу  $\langle \mathcal{A} \rangle$  порядка  $n$ . В  $D_n$  содержится

ещё отражение  $\mathcal{B} = \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix}$  многоугольника  $P_n$  относительно оси, проходящей через центр и одну из вершин (рис. 2).

По определению  $\mathcal{B}^2 = e$ . Различные преобразования симметрии

$$e, \mathcal{A}, \mathcal{A}^2, \dots, \mathcal{A}^{n-1}, \quad \mathcal{B}, \mathcal{A}\mathcal{B}, \dots, \mathcal{A}^{n-1}\mathcal{B} \tag{5}$$

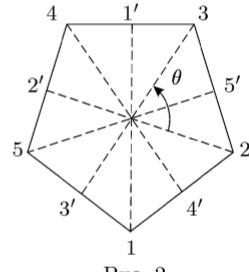


Рис. 2

в количестве  $2n$  штук исчерпывают всю группу  $D_n$ . В самом деле, всякое преобразование симметрии определяется своим действием на вершины  $1, 2, \dots, n$  многоугольника  $P_n$ . Если какое-то преобразование переводит  $1$  в  $k$ , то оно должно либо сохранять тот же циклический порядок вершин, как это делает  $\mathcal{A}^k$ , либо менять его на обратный, как это делает  $\mathcal{A}^{k-1}\mathcal{B}$ .

Поэтому никаких элементов, кроме (5), в  $D_n$  нет. Заметим, что преобразование  $\mathcal{B}\mathcal{A}$  совпадает с  $\mathcal{A}^{n-1}\mathcal{B}$ , поскольку оба преобразования обращают порядок вершин и переводят  $1$  в  $n$ . Таким образом, имеют место соотношения

$$\mathcal{A}^n = e, \quad \mathcal{B}^2 = e, \quad \mathcal{A}\mathcal{B}\mathcal{A}\mathcal{B} = e.$$

Это означает, что  $D_n$  является гомоморфным образом группы

$$G = \langle a, b \mid a^n = b^2 = abab = e \rangle.$$

Но, как и в случае  $n = 3$ , получаем  $ba = a^{n-1}b$ , так что любое слово в алфавите  $\{a, a^{-1}, b, b^{-1}\}$  сводится либо к  $a^i$ , либо к  $a^i b$ ,  $0 \leq i \leq n-1$ . Стало быть,  $|G| \leq 2n$ , а ввиду вышесказанного должен иметь место изоморфизм  $G \cong D_n$ . Тем самым получено задание группы диэдра образующими и определяющими соотношениями. Отождествим  $G$  с  $D_n$ :

$$D_n = \langle a, b \mid a^n = e, b^2 = e, (ab)^2 = e \rangle.$$

Так как  $\langle a \rangle \triangleleft D_n$  и  $D_n/\langle a \rangle$  — циклическая группа, то на основании теоремы 4 для коммутанта  $D'_n$  группы  $D_n$  имеем включение  $D'_n \subset \langle a \rangle$ . Но  $a^2 = aba^{-1}b^{-1} = (a, b) \in D'_n$  и при  $n$  нечётном  $D'_n = \langle a \rangle$ , а при  $n$  чётном  $D_n/\langle a^2 \rangle = \langle \bar{a}, \bar{b} \rangle$  — прямое произведение двух циклических групп порядка 2, откуда  $D'_n = \langle a^2 \rangle$ . В зависимости от чётности  $n$  меняются также центр  $Z(D_n)$  группы  $D_n$  и число  $r$  её классов сопряжённости. Приведём готовые (и легко проверяемые) таблицы:

$$n = 2m, \quad D'_n = \langle a^2 \rangle, \quad (D_n : D'_n) = 4, \quad Z(D_n) = \langle a^m \rangle, \quad r = m + 3,$$

1	1	2	...	2	$m$	$m$
$e$	$a^m$	$a$	...	$a^{m-1}$	$b$	$ab$

;

$$n = 2m + 1, \quad D'_n = \langle a \rangle, \quad (D_n : D'_n) = 2, \quad Z(D_n) = e, \quad r = m + 2,$$

1	2	...	2	2	$n$
$e$	$a$	...	$a^{m-1}$	$a^m$	$b$

.

Представители сопряжённых классов стоят в нижней строке, мощности этих классов — в верхней.

Стоит подчеркнуть, что вид определяющих соотношений (их левых частей) в записи  $w_i = e$ ) существенно зависит от выбора системы образующих группы. Например, диэдральная группа  $D_n$  порождается любыми отражениями относительно двух прямых, пересекающихся под углом  $\pi/m$ . Поэтому

$$D_n = \langle g_1, g_2 \mid g_1^2 = g_2^2 = (g_1g_2)^n = e \rangle.$$

Если исходить из прежнего задания, то можно положить  $g_1 = ab$ ,  $g_2 = b$ .

Пример 2 (группа кватернионов). В отличие от предыдущего примера мы с самого начала определим группу кватернионов  $Q_8$  образующими и соотношениями:

$$Q_8 = \langle a, b \mid a^4 = e, b^2 = a^2, bab^{-1} = a^{-1} \rangle.$$

Снова  $ba = a^{-1}b = a^3b$ , и поскольку  $b^2 = a^2$ , любое слово в алфавите  $\{a, a^{-1}, b, b^{-1}\}$  приводится к виду  $a^s b^t$ ,  $0 \leq s \leq 3$ ,  $0 \leq t \leq 1$ , так что  $|Q_8| \leq 8$ .

Можем ли мы утверждать, что  $|Q_8| = 8$ ? Да, но только после того, как будет предъявлена группа из 8 элементов, две образующие которой связаны теми же соотношениями, что и  $a, b$ . Такую группу порождают известные нам из упр. 3 из § 1 кватернионные единицы  $\mathbf{i}, \mathbf{j}, \mathbf{k}$  (отсюда и название группы), а также матрицы

$$A = \begin{vmatrix} i & 0 \\ 0 & -i \end{vmatrix}, \quad B = \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix} \quad (i = \sqrt{-1}).$$

Действительно,

$$A^4 = E, \quad B^2 = A^2, \quad BAB^{-1} = A^{-1},$$

$$\langle A, B \rangle = \left\{ \pm \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \pm \begin{vmatrix} i & 0 \\ 0 & -i \end{vmatrix}, \pm \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}, \pm \begin{vmatrix} 0 & i \\ i & 0 \end{vmatrix} \right\}.$$

Эти матрицы нам уже встречались в упр. 3 из § 1. Собственно говоря, там предлагалось проверить, что отображение  $a \mapsto A, b \mapsto B$  определяет изоморфизм  $Q_8 \cong \langle A, B \rangle$ . Заметим, что  $a^2 \in Z(Q_8)$ , и так как факторгруппа по центру неабелевой группы не может быть циклической (см. замечание после доказательства теоремы 4), то  $\langle a^2 \rangle = Z(Q_8)$ . Все группы порядка 4 абелевы, поэтому  $Q_8/Z(Q_8) \cong V_4$  — прямое произведение двух циклических групп порядка 2. Стало быть, коммутант  $Q'_8$  совпадает с  $Z(Q_8)$  и  $(Q_8 : Q'_8) = 4$ . Сведения о сопряжённых классах содержатся в таблице:

1	1	2	2	2
$e$	$a^2$	$a$	$b$	$ab$

Конечно определённые группы, простейшие примеры которых мы рассмотрели, встречаются в разных областях математики, например, в качестве так называемых фундаментальных групп многообразий. Неудивительно, что ещё многие относящиеся к ним вопросы остаются открытыми.

### УПРАЖНЕНИЯ

1. Вспомним определение из [ВА I, гл. 4, § 2, п. 4] внутреннего автоморфизма  $I_a : g \mapsto aga^{-1}$  и группы  $\text{Inn}(G) \subset \text{Aut}(G)$ . Показать, что  $\text{Inn}(G) \triangleleft \text{Aut}(G)$  и  $\text{Inn}(G) \cong G/Z(G)$ , где  $Z(G)$  — центр группы  $G$ . Факторгруппа  $\text{Out}(G) = \text{Aut}(G)/\text{Inn}(G)$  называется *группой внешних автоморфизмов*.

2. Пусть  $H$  и  $K$  — подгруппы группы  $G$ . Показать, что

$$|HK| \cdot |H \cap K| = |H| \cdot |K|$$

(аналог формулы, известной из теории линейных пространств). Показать, далее, что множество  $HK$  будет подгруппой тогда и только тогда, когда  $HK = KH$ ; в случае  $K \triangleleft G$  это условие автоматически выполняется.

3. Составим для симметрической группы  $S_4$  таблицу

1	3	6	8	6
$e$	$(12)(34)$	$(12)$	$(123)$	$(1234)$

аналогичную тем, которые мы использовали в только что рассмотренных примерах. Опираясь на достаточно очевидное соображение, что в любой группе нормальная подгруппа есть объединение некоторого множества сопряжённых

классов, повторить данное нами в примере 2 описание нормальных подгрупп группы  $S_4$ .

4. Показать, что  $Z(A \times B) = Z(A) \times Z(B)$ .

5. Если  $K_1, K_2 \triangleleft G$ ,  $K_1 \cap K_2 = e$ , то  $G$  изоморфна некоторой подгруппе в  $(G/K_1) \times (G/K_2)$ . Верно ли это?

6. Пусть  $K \triangleleft G = A \times B$ . Доказать, что либо подгруппа  $K$  абелева, либо одно из пересечений  $K \cap A$ ,  $K \cap B$  нетривиально. Дать пример группы  $A \times B$  с нетривиальной нормальной подгруппой  $K$  такой, что  $K \cap A = e$  и  $K \cap B = e$ . Тем самым из  $K \triangleleft A \times B$ , вообще говоря, не следует, что  $K = (K \cap A) \times (K \cap B)$ .

7. Является ли группа кватернионов  $Q_8$  полуправильным произведением каких-то двух своих собственных подгрупп?

8. Показать, что  $H \triangleleft Q_8$  для любой собственной подгруппы  $H \subset Q_8$ .

9. Показать, что группы  $D_4$  и  $Q_8$  не изоморфны.

10. Показать, что  $\text{Aut}(D_4) \cong D_4$  (так как  $|Z(D_4)| = 2$ , то, согласно упражнению 1,  $|\text{Out}(G)| = 2$ ).

11. Все комплексные корни из 1 степени  $p^i$ ,  $i = 0, 1, 2, \dots$ , образуют бесконечную группу  $C(p^\infty)$ . Она называется *квазициклической*, поскольку любое конечное число её элементов порождает циклическую группу. Проверить это и показать, что

$$C(p^\infty) = \langle a_1, a_2, a_3, \dots \mid a_1^p = 1, a_{i+1}^p = a_i; i = 1, 2, 3, \dots \rangle.$$

12 (J. Monthly, № 9, 1973). Пусть

$$G = \langle a, b \mid aba = ba^2b, a^3 = e, b^{2n-1} = e \rangle,$$

где  $n \in \mathbb{N}$ . Доказать, что  $n = 1$ , т. е.  $b = e$  и фактически  $G = \langle a \mid a^3 = e \rangle$  — циклическая группа порядка 3.

13. Построить мономорфизм  $f : S_n \longrightarrow \text{GL}(n)$  такой, что матрица  $f(\pi)$ ,  $\pi \in S_n$ , имеет определитель  $\det f(\pi) = \varepsilon_\pi$ .

Матрицы вида  $f(\pi)$ ,  $\pi \in S_n$ , называются *матрицами перестановок*. Ограничение  $f$  на  $A_n$  является мономорфизмом в  $\text{SL}(n, \mathbb{R})$ . Композиция  $f \circ L$  отображений  $L : G \longrightarrow S_n$  (теорема Кэли) и  $f : S_n \longrightarrow \text{GL}(n)$  приводит к мономорфизму  $G \longrightarrow \text{GL}(n)$  для любой конечной группы  $G$ .

Выписать отображение  $f$  в явном виде при  $n = 3$ .

14. Дополнить деталями следующее формальное определение *свободной группы*  $F_n$  ранга  $n$ . К алфавиту  $A = \{a_1, a_1^{-1}, \dots, a_n, a_n^{-1}\}$ , состоящему из  $n$  букв  $a_1, \dots, a_n$  и их “антитиподов”  $a_1^{-1}, \dots, a_n^{-1}$ , добавляется символ  $e := \emptyset$ . Пусть  $S$  — множество всех “слов”, получающихся выписыванием этих  $2n + 1$  символов в любом порядке в строки конечной длины. В словах допускаются повторения символов. Под *произведением*  $uv$  двух слов  $u, v$  понимается приписывание слова  $v$  к концу слова  $u$ . *Обратным* к  $u$  есть  $a_{i_1}^{\varepsilon_1} \dots a_{i_m}^{\varepsilon_m}$ ,  $\varepsilon_k = \pm 1$ ,  $k = 1, \dots, m$ , называется слово  $u^{-1} = a_{i_m}^{-\varepsilon_m} \dots a_{i_1}^{-\varepsilon_1}$ ,  $e^{-1} = e$ . На  $S$  вводится отношение эквивалентности  $\sim$ . Именно, два слова считаются эквивалентными, если одно получается из другого в результате применения конечного числа следующих элементарных преобразований:

$$ee \sim e,$$

$$a_i a_i^{-1} \sim e, \quad a_i^{-1} a_i \sim e,$$

$$a_i e \sim a_i, \quad a_i^{-1} e \sim a_i^{-1},$$

$$ea_i \sim a_i, \quad ea_i^{-1} \sim a_i^{-1}.$$

В каждом классе эквивалентности содержится одно-единственное “несократимое” (кратчайшее) слово. На классах эквивалентности по отношению  $\sim$  определена ассоциативная операция умножения (и обращение классов), индуцированная умножением слов. Единицей будет класс эквивалентности “пустого” слова  $e$ . Множество классов эквивалентности с данной операцией умножения и есть как раз свободная группа  $F_n$  с  $n$  свободными образующими  $a_1, \dots, a_n$  (*свободная группа ранга  $n$* ).

**Пример.** По “восьмёрке”, охватывающей своими петлями два столба, бегает в разных направлениях котёнок с нитяной шпулькой, укладывая последующие витки ниток поверх предыдущих. Когда котёнок находится в центре между столбами, то направление его движения может меняться произвольным образом. Пройденные им пути с начальными и конечными точками в центре интерпретируются, очевидно, как элементы свободной группы  $F_2$  ранга 2.

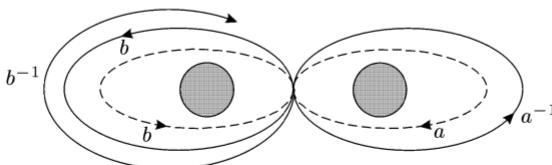


Рис. 3

Несократимым словам отвечают натянутые нитки, освобождённые от тривиальных петель  $aa^{-1}$ ,  $a^{-1}a$ ,  $bb^{-1}$ ,  $b^{-1}b$ . На рис. 3 участки  $a$  и  $a^{-1}$ ,  $b$  и  $b^{-1}$  изображены геометрически различными лишь для наглядности. Наш пример реализует  $F_2$  в виде совокупности классов “гомотопически эквивалентных путей” (топологическая терминология) лемнискаты. В этом смысле фундаментальной группой лепестка, изображённого на рис. 6 в комментариях к 3.3.2 в разделе ответов и решений, будет свободная группа  $F_5$ .

## Глава 2

# СТРОЕНИЕ ГРУПП

---

Изучаемые алгебраические объекты становятся более привлекательными, если их свойства можно выразить на языке элементарных, в том или ином смысле объектов и операций (циклических групп, прямых и полупрямых произведений и т.д.), а сами объекты (в нашем случае группы) обнаруживают изначально или на более позднем этапе тесную связь с другими областями математики. Мы видели в гл. 1, что даже такие маленькие группы, как  $Q_8$ ,  $S_4$  допускают дальнейшее расщепление, полезное во многих отношениях. Бытовавшая когда-то наивная точка зрения, что конечные группы можно перечислять, опираясь на утверждения типа теоремы Кэли, ушла в прошлое: самые мощные компьютеры конца XX века не справились с доказательством существования “монстра  $M$ ” — простой группы порядка

$$|M| = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$

Это было сделано человеком. С другой стороны, задача перечисления с точностью до изоморфизма групп сравнительно небольшого порядка  $4096 = 2^{12}$  представляет значительную сложность как для машин, так и для человека.

В этой главе внимание будет сосредоточено на небольшом числе классов групп, знакомство с которыми полезно каждому математику.

### § 1. Разрешимые и простые группы

**1. Разрешимые группы.** Понятие коммутанта, введённое в гл. 1, приводит к важному и весьма обширному классу групп. Пусть, как и прежде,  $G'$  коммутант группы  $G$ . В  $G'$  также можно рассмотреть коммутант  $(G')' = G''$ , называемый *второй производной группой* (*вторым коммутантом*) группы  $G$ . Продолжая этот процесс, мы определим  $k$ -ю производную группу  $G^{(k)} = (G^{(k-1)})'$ . Согласно импликации (1) из § 4 гл. 1  $G^{(k)} \triangleleft G$  и, тем более,  $G^{(k)} \triangleleft G^{(k-1)}$ . Получается ряд нормальных подгрупп (*производный ряд*)

$$G \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \dots \triangleright G^{(k)} \triangleright G^{(k+1)} \triangleright \dots \quad (1)$$

с абелевыми факторгруппами  $G^{(k)} / G^{(k+1)}$ .

Определение. Группа  $G$  называется *разрешимой*, если ряд (1) обрывается на единичной подгруппе, т.е.  $G^{(m)} = e$  для некоторого наименьшего индекса  $m$  — *ступени разрешимости* группы  $G$ .

Очевидно, что любая абелева, в том числе циклическая группа является разрешимой ступени 1. Кроме того, в любой разрешимой группе  $G$  ступени разрешимости  $m$  имеется абелева нормальная подгруппа  $\neq e$ , а именно  $G^{(m-1)}$ . Как показывают рассмотренные в гл. 1 примеры,  $S'_4 = A_4$ ,  $A'_4 = V_4$ ,  $V'_4 = e$ . Стало быть, знакопеременная группа  $A_4$  разрешимая ступени 2, а симметрическая группа  $S_4$  разрешимая ступени 3. Более общим является

Пример. Пусть

$$T := T(n, \mathbb{K}) = \{A = (a_{ij}) \subset \mathrm{GL}(n, \mathbb{K}) \mid a_{ij} = 0 \quad \forall i > j\}$$

— группа верхне-треугольных матриц с коэффициентами в произвольном поле  $\mathbb{K}$ . Прямая проверка показывает, что  $T^{(n+1)} = E$ , так что  $T(n, \mathbb{K})$  — разрешимая группа при любом  $n$ . Между прочим, её коммутант  $T' = \mathrm{UT}(n, \mathbb{K})$  (группа верхне-треугольных матриц с единицами по главной диагонали) обладает более сильным свойством, чем разрешимость. Если для произвольной группы  $G$  положить

$$G_1 := G, \quad G_2 = G', \quad G_{k+1} = \langle G_k, G \rangle = \{(u, v) \mid u \in G_k, v \in G\},$$

то получится *нижний центральный ряд* группы  $G$ :

$$G = G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \dots \trianglerighteq G_k \trianglerighteq G_{k+1} \dots \quad (2)$$

Группа  $G$  называется *нильпотентной класса  $c$* , если  $G_c \neq e$ , но  $G_{c+1} = e$ . Группа  $\mathrm{UT}(n, \mathbb{K})$  нильпотентная класса  $n$ .

Справедлива следующая несложная

**Теорема 1.** *Группа  $G$  с нормальной подгруппой  $K$  разрешима в том и только том случае, когда разрешимы одновременно  $K$  и  $G/K$ .*

**Доказательство.** Если  $H \subset G$ , то  $H' \subset G', \dots, H^{(k)} \subset G^{(k)}$ , и отсюда непосредственно следует, что любая подгруппа  $H$  разрешимой группы  $G$  разрешима.

Пусть теперь  $K$  — нормальная подгруппа разрешимой группы  $G$  и  $\overline{G} = G/K$  — соответствующая факторгруппа. Естественный гомоморфизм  $\pi : G \rightarrow \overline{G}$  приводит к эпиморфизму  $G'$  на  $\overline{G}'$  (поскольку, очевидно,  $\varphi((g_1, g_2)) = (\varphi(g_1), \varphi(g_2))$  для любого гомоморфизма  $\varphi : G \rightarrow \overline{G}$ ) и, стало быть, — к эпиморфизму  $G^{(k)}$  на  $\overline{G}^{(k)}$ . Это и позволяет сделать заключение о разрешимости  $\overline{G}$ .

Чтобы доказать утверждение теоремы в обратную сторону, воспользуемся, заменив  $\varphi$  на  $\pi$ , уже отмеченным равенством

$$(\overline{g_1}, \overline{g_2}) = \overline{(g_1, g_2)}, \quad (3)$$

т.е.  $(g_1 K, g_2 K) = (g_1, g_2) K$  (формально надо различать коммутататоры в  $G$  и в  $\overline{G}$ ). Пусть  $s$  — ступень разрешимости факторгруппы  $\overline{G}$  и  $t$  — ступень разрешимости подгруппы  $K$ . Многократно используя (3), мы приходим к равенству  $\overline{G^{(i)}} = (\overline{G})^{(i)}$  при любом  $i$ . В частности,  $\overline{G^{(s)}} = (\overline{G})^{(s)} = \overline{e} = K$ . Таким образом, имеет место включение

$G^{(s)} \subset K$ , откуда получаем  $G^{(s+t)} \subset K^{(t)} = e$ , т.е.  $G$  — разрешимая группа.  $\square$

**Следствие.** Пусть  $K_1, K_2$  — разрешимые нормальные подгруппы произвольной группы  $G$ . Тогда  $K_1 K_2$  является также разрешимой нормальной подгруппой в  $G$ .

**Доказательство.** Из гл. 1 мы уже знаем, что  $K_1 K_2$  — нормальная подгруппа группы  $G$ . Далее, по теореме об изоморфизме имеем

$$K_1 K_2 / K_2 \cong K_1 / (K_1 \cap K_2).$$

Теперь достаточно применить теорему 1.  $\square$

Доказанное следствие приводит к следующему утверждению: *произведение всех разрешимых нормальных подгрупп конечной группы  $G$  будет максимальной разрешимой нормальной подгруппой  $F(G)$  в  $G$ , и факторгруппа  $G/F(G)$  таких подгрупп уже не содержит*.

Своему названию разрешимые группы обязаны теории Галуа, о чём уже упоминалось в [ВА I]. Разрешимость группы  $S_4$  и всех её подгрупп служит причиной разрешимости в радикалах алгебраических уравнений степени  $n \leq 4$ . Более детально с этими вопросами можно познакомиться в гл. 5, § 5.

**2. Простые группы.** Существуют группы  $\neq e$ , совпадающие со своим коммутантом и, стало быть, не являющиеся разрешимыми. Более того, мы сейчас установим существование неабелевых групп, в которых вообще нет нетривиальных ( $\neq e$  и  $G$ ) нормальных подгрупп. Такие группы принято называть *простыми*.

**Лемма.** Любая нормальная подгруппа  $K$  группы  $G$  является объединением некоторого множества сопряжённых классов группы  $G$ .

**Доказательство.** Если  $x \in K \triangleleft G$ , то и  $gxg^{-1} \in K$  для всех  $g \in G$ . Следовательно, вместе с каждым элементом  $x \in K$  в  $K$  содержится целиком класс сопряжённых элементов  $x^G$  и  $K = \bigcup_{i \in I} x_i^G$ .  $\square$

**Теорема 2.** Знакопеременная группа  $A_5$  простая.

**Доказательство.** Действительно, в группе  $A_5$ , помимо единичной перестановки  $e$ , имеется 15 элементов  $(ij)(kl)$  порядка 2 (по три элемента этого вида в стационарной подгруппе каждой из точек 1, 2, 3, 4, 5),  $20 = 2\binom{5}{3}$  элементов  $(ijk)$  порядка 3 и  $24 = 4!$  элемента  $(1i_1i_2i_3i_4)$  порядка 5. Элементы порядка 2 все сопряжены: они, очевидно, сопряжены в  $S_5$ , а так как стационарная подгруппа (относительно действия сопряжением) элемента  $(12)(34)$  содержит нечётную перестановку  $(12)$ , то сопряжение может быть осуществлено чётными перестановками. То же самое относится к элементам порядка 3. Но элементы порядка 5, сопряжёные в  $S_5$ , в группе  $A_5$  распадаются на два класса с представителями  $(12345)$  и  $(12354)$ . В самом деле,  $(45)(12345)(45)^{-1} = (12354)$ , а централизатором (стационарной подгруппой) элемента  $(12345)$  в  $A_5$  служит циклическая

группа порядка 5, порождённая этим элементом. Итак, мы имеем таблицу

1	15	20	12	12
e	(1 2)(3 4)	(1 2 3)	(1 2 3 4 5)	(1 2 3 5 4)

В нижней строке указаны представители сопряжённых классов, а в верхней — мощности этих классов. Пусть теперь  $K$  — нормальная подгруппа в  $A_5$ . Согласно лемме

$$|K| = \delta_1 \cdot 1 + \delta_2 \cdot 15 + \delta_3 \cdot 20 + \delta_4 \cdot 12 + \delta_5 \cdot 12,$$

где  $\delta_1 = 1$  (так как  $e \in K$ ) и  $\delta_i = 0$  или  $\delta_i = 1$  при  $i = 2, 3, 4, 5$ . Не трудно убедиться в том, что условие на  $|K|$  быть делителем порядка  $|A_5| = 60$  (теорема Лагранжа) оставляет лишь две возможности:

- a)  $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 0$ ;  $K$  — единичная подгруппа;
- б)  $\delta_2 = \delta_3 = \delta_4 = \delta_5 = 1$ ;  $K = A_5$ .

Это и доказывает, что  $A_5$  — простая группа.  $\square$

Индукцией по  $n$  теперь можно установить (см. упр. 3), что *простыми являются все группы  $A_n$ ,  $n \geq 5$*  (результат Э. Галуа). Так как подгруппы разрешимых групп разрешимы (теорема 1), то из теоремы 2 во всяком случае следует, что симметрическая группа  $S_n$  неразрешима при  $n \geq 5$ .

**Теорема 3.** *Группа вращений  $SO(3)$  является простой.*

**Доказательство.** Согласно теореме 1 из § 1 гл. 1 достаточно убедиться в том, что любая нормальная подгруппа  $K$  группы  $SU(2)$ , содержащая ядро  $\{\pm E\}$  эпиморфизма  $\Phi : SU(2) \rightarrow SO(3)$  и отличная от  $\pm E$ , совпадает с  $SU(2)$ . Соотношение (5) § 1 гл. 1 можно интерпретировать по-новому, сказав, что в каждом сопряжённом классе группы  $SU(2)$  содержится диагональная матрица  $d_\varphi = b_{2\varphi} = \text{diag}\{e^{i\varphi}, e^{-i\varphi}\}$ . Так как по лемме  $K$  является объединением некоторого семейства сопряжённых классов группы  $SU(2)$ , то без ограничения общности считаем  $d_\varphi \in K$  для некоторого  $\varphi > 0$  такого, что  $\sin \varphi \neq 0$ .

В  $K$  должен содержаться также любой коммутатор

$$\begin{aligned} (d_\varphi, g) &= d_\varphi(gd_\varphi^{-1}g^{-1}) = \\ &= \left\| \begin{array}{cc} e^{i\varphi} & 0 \\ 0 & e^{-i\varphi} \end{array} \right\| \left\| \begin{array}{cc} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{array} \right\| \left\| \begin{array}{cc} e^{-i\varphi} & 0 \\ 0 & e^{i\varphi} \end{array} \right\| \left\| \begin{array}{cc} \bar{\alpha} & -\beta \\ \bar{\beta} & \alpha \end{array} \right\| = \\ &= \left\| \begin{array}{cc} |\alpha|^2 + |\beta|^2 e^{i2\varphi} & 0 \\ 0 & |\alpha|^2 + |\beta|^2 e^{-i2\varphi} \end{array} \right\|, \end{aligned}$$

где  $|\alpha|^2 + |\beta|^2 = 1$  (см. (3) из § 1 гл. 1). Для следа матрицы  $(d_\varphi, g)$  получаем выражение

$$\text{tr}(d_\varphi, g) = 2|\alpha|^2 + |\beta|^2(e^{i2\varphi} + e^{-i2\varphi}) = 2(1 - 2|\beta|^2 \sin^2 \varphi).$$

Здесь  $|\beta|$  принимает любое значение из отрезка  $[0, 1]$  и  $\sin \varphi \neq 0$ . Снова в силу (5) из § 1 гл. 1 найдётся унитарная матрица  $h \in SU(2)$

такая, что  $h[d_\varphi, g]h^{-1} = d_\psi = \text{diag}\{e^{i\psi}, e^{-i\psi}\}$ , причём  $d_\psi \in K$ . Так как  $e^{i\psi}, e^{-i\psi}$  — корни характеристического уравнения

$$\lambda^2 + (4|\beta|^2 \sin^2 \varphi - 2)\lambda + 1 = 0$$

матрицы  $(d_\varphi, g)$ , то, заставляя  $|\beta|$  пробегать значения от 0 до 1, мы получим для  $\psi$  любую точку на отрезке  $[0, 2\varphi]$ . Итак, в  $K$  содержится любой элемент  $d_\psi$  и определённый параметром  $\psi$  сопряжённый класс при  $0 \leq \psi \leq 2\varphi$ . Поскольку для всякого  $\sigma > 0$  найдётся натуральное число  $n$ , удовлетворяющее условию  $0 < \psi := \sigma/n \leq 2\varphi$ , можно утверждать, что в  $K$  содержится наперёд заданный элемент  $d_\sigma = d_\psi^n$ .  $\square$

**Теорема 4.** *Проективная специальная линейная группа  $\text{PSL}(2, F)$  над полем с числом элементов  $|F| > 3$  простая.*

**Доказательство.** 1) Выделим некоторые подгруппы и элементы:

$$\begin{aligned} U &= \left\{ u(\alpha) = \begin{vmatrix} 1 & \alpha \\ 0 & 1 \end{vmatrix} \mid \alpha \in F \right\}, \\ \overline{U} &= \left\{ \overline{u}(\alpha) = \begin{vmatrix} 1 & 0 \\ \alpha & 1 \end{vmatrix} \mid \alpha \in F \right\}, \\ D &= \left\{ d(\lambda) = \begin{vmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{vmatrix} \mid \lambda \in F^* \right\}; \\ B &= DU = UD = \left\{ \begin{vmatrix} \alpha & \beta \\ 0 & \alpha^{-1} \end{vmatrix} \right\} \end{aligned}$$

— стандартная *борелевская подгруппа*. Заметим, что

$$d(\lambda) = u(\lambda - 1)\overline{u}(1)u(\lambda^{-1} - 1)\overline{u}(-\lambda),$$

поэтому борелевская подгруппа  $B$  порождается *унипотентными подгруппами*  $U$  и  $\overline{U}$ . Выделим ещё элемент

$$w = u(1)\overline{u}(-1)u(1) = \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}.$$

2) Группа  $G = \text{SL}(2, F)$  обладает разложением

$$G = B \cup BwB, \quad B \cap BwB = \emptyset. \tag{4}$$

Чтобы в этом убедиться, рассмотрим естественное действие  $G$  слева на столбцы. Группа изотропии столбца  $e^1 = [1, 0]$  совпадает, очевидно, с  $U$ . Орбита  $Be^1$  состоит из всех столбцов  $[\lambda, 0]$ ,  $\lambda \neq 0$ . С другой стороны,  $we^1 = [0, -1]$ , и поэтому орбита  $Bwe^1$  состоит из всех столбцов  $[\beta, \lambda^{-1}]$  со второй компонентой  $\neq 0$ . Так как эти две орбиты покрывают орбиту  $Ge^1$ , то отсюда следует, что  $B \cup BwB = G$ , поскольку группа изотропии  $U$  содержит в  $B$ .

Разложение (4) называется *разложением Брюа*. Оно допускает далёкое обобщение, которого мы не касаемся.

3) Борелевская подгруппа  $B$  максимальна в  $G$ .

Действительно, из разложения (4) следует, что любой элемент  $h \in H$ , не содержащийся в  $B$ , содержится в  $BwB$ , т.е.  $h = b_1wb_2$ , откуда  $w \in H$  и, таким образом,  $H = G$ .

4) Если  $|F| \geq 4$ , то  $G = \mathrm{SL}(2, F) = G'$ .

Берём  $0 \neq \lambda \in F$ ,  $\lambda^2 \neq 1$ , что при  $|F| > 3$  возможно. Тогда из коммутационного соотношения

$$d(\lambda)u(\alpha)d(\lambda)^{-1}u(\alpha)^{-1} = u(\alpha(\lambda^2 - 1))$$

следует, что  $B' = U$  и  $G' \supseteq U$ , а поскольку  $G' \triangleleft G$ , мы получаем включение  $G' \supseteq wUw^{-1} = \overline{U}$ . Но, как это следует из 1) и 2),  $U$  и  $\overline{U}$  порождают  $G$ . Таким образом,  $G' = G$ .

5) При  $|F| \geq 4$  группа  $\mathrm{PSL}(2, F) = \mathrm{SL}(2, F)/Z$  простая ( $Z = \{\pm E\}$  — центр).

Воспользуемся легко проверяемым равенством

$$\bigcap_{x \in G} xBx^{-1} = Z.$$

Нам нужно показать, что если  $H \triangleleft G = \mathrm{SL}(2, F)$ , то либо  $H \subset Z$ , либо  $H \supset G'$ . Ввиду максимальности  $B$  (см. 3)), мы имеем  $HB = B$  или  $HB = G$ . Если  $HB = B$ , то  $H \subset B$ . Так как  $H \triangleleft G$ , то  $H = xHx^{-1} \subset xBx^{-1} \quad \forall x \in G$ , т.е.  $H \subset Z$ .

С другой стороны,

$$HB = G \implies w = hb, \quad h \in H, b \in B.$$

В таком случае

$$\overline{U} = wUw^{-1} = hbUb^{-1}h^{-1} = hUh^{-1} \subset HU,$$

поскольку  $H \triangleleft G$ . Так как  $U \subset HU$ , а  $U, \overline{U}$  порождают  $G$ , то  $HU = G$ . Следовательно,

$$G/H = HU/H \cong U/(U \cap H)$$

— абелева группа, откуда  $H \supset G'$ . Теперь утверждение о простоте группы  $\mathrm{PSL}(2, F)$  очевидно.  $\square$

Другими средствами теорема 4 была впервые доказана Э. Галуа. Уже из теорем 2–4 видно, что в классе простых групп содержатся важные для приложений группы, как конечные, так и бесконечные. Может показаться удивительным, но сколько-нибудь разумное описание всех существующих конечных простых групп потребовало бы нескольких сотен страниц.

## УПРАЖНЕНИЯ

## 1. Цепочка подгрупп

$$e = G_0 \subset G_1 \subset \dots \subset G_n \subset G_{n+1} = G, \quad (*)$$

где  $G_{i-1} \triangleleft G_i$ ,  $1 \leq i \leq n+1$ , называется *нормальным рядом* группы  $G$ . Нормальным называется также ряд убывающих подгрупп

$$G = G_0 \supset G_1 \supset \dots \supset G_n \supset G_{n+1} = e,$$

где  $G_{i+1} \triangleleft G_i$ .

Если все члены ряда  $(*)$  различны и  $G_{i-1} \triangleleft H \triangleleft G_i \implies H = G_{i-1}$  или  $H = G_i$  при всех  $i$ , то говорят о *композиционном ряде* группы  $G$ . Факторгруппы  $F_i = G_i/G_{i-1}$  в этом случае называются *композиционными факторами*.

Показать, что:

1) любой нормальный ряд конечной группы можно уплотнить до композиционного ряда, вставляя в него дополнительные члены до тех пор, пока это будет возможно;

2) факторы  $F_i$  являются простыми группами (или циклическими группами простых порядков);

3) группа  $G$  разрешима ровно тогда, когда все её композиционные факторы являются циклическими группами простых порядков.

Упомянем без доказательства о теореме Жордана–Гельдера, согласно которой набор композиционных факторов группы  $G$  с точностью до изоморфизма и порядка следования не зависит от выбора композиционного ряда.

2. Доказать, что любая конечная  $p$ -группа разрешима.

3. Доказать простоту знакопеременной группы  $A_n$ ,  $n \geq 5$ , следуя набросанной ниже схеме рассуждений.

а) В нормальной подгруппе  $K \triangleleft A_n$ ,  $K \neq e$ , следует взять перестановку  $\pi \neq e$ , оставляющую на месте максимально возможное число  $m$  символов из  $\Omega = \{1, 2, \dots, n\}$ . Если  $m = n - 3$ , то  $\pi = (ijk)$  и  $K = A_n$  (см. [ВА I, гл. 4, § 2, упр. 11]), поэтому считаем  $m < n - 3$ .

б) Если  $\pi = (123\dots) \dots$  — разложение  $\pi$  на независимые циклы, то чётность  $\pi$  и условие  $m < n - 3$  влекут неравенство  $m < n - 5$ . Возможно ещё, что  $\pi = (12)(34)\dots$  состоит из независимых циклов длины 2.

в) В любом случае рассмотреть коммутатор  $(\pi, \sigma) = \pi\sigma\pi^{-1}\sigma^{-1} \neq e$  с  $\sigma = (345)$  и проверить, что он оставляет на месте более  $m$  символов. Это противоречит выбору  $m$  и доказывает утверждение.

4. Показать, что знакопеременная группа  $A_5$  не содержит подгрупп порядков 15 и 20.

## § 2. Теоремы Силова

Мы уже обращали внимание на тот факт, что в конечной группе  $G$  порядка  $|G|$  может и не быть подгруппы порядка  $d$ , делящего  $|G|$ . Минимальным таким примером служит пара  $G = A_4$ ,  $d = 6$ .

Так как в неабелевой простой группе не может быть подгрупп индекса 2 (ввиду их нормальности), то по теореме 2 из § 1 в знакопеременной группе  $A_5$  порядка 60 нет подгрупп порядка 30 (см. также упр. 4 из § 1). На этом фоне особенно замечательными выглядят общие закономерности, установленные более 125 лет назад норвежским

математиком Силовым. Они относятся к  $p$ -группам (с которыми мы встречались в § 3 из гл. 1), содержащимся в качестве подгрупп группы  $G$ . Существование элемента порядка  $p$  в абелевой группе, порядок которой делится на  $p$ , было подмечено ещё О. Коши.

Пусть  $|G| = p^n m$ , где  $p$  — простое число, а  $m$  — целое число, взаимно простое с  $p$ . Подгруппу  $P \subset G$  порядка  $|P| = p^n$  (если таковая существует) будем называть *силовской  $p$ -подгруппой* группы  $G$ . Как и в § 3 гл. 1, под  $N(P)$  понимается нормализатор подгруппы  $P$  в  $G$ .

**Теорема 1** (первая теорема Силова). *Силовские  $p$ -подгруппы существуют.*

**Теорема 2** (вторая теорема Силова). *Пусть  $P$  и  $P_1$  — любые две силовские  $p$ -подгруппы группы  $G$ . Тогда найдётся элемент  $a \in G$ , для которого  $P_1 = aPa^{-1}$ . Другими словами, все силовские  $p$ -подгруппы сопряжены.*

**Теорема 3** (третья теорема Силова). *Для числа  $N_p$  силовских  $p$ -подгрупп группы  $G$  имеют место равенство  $N_p = (G : N(P))$  и сравнение  $N_p \equiv 1 \pmod{p}$ .*

Доказательства теорем 1–3 служат иллюстрацией общих методов и соображений, изложенных в § 3 из гл. 1. Начнём с теоремы 2.

**Доказательство теоремы 2.** Итак, пусть силовские  $p$ -подгруппы в  $G$  существуют и  $P$  — одна из них. Пусть, далее,  $P_1$  — произвольная  $p$ -подгруппа группы  $G$ , не обязательно силовская. Заставим  $P_1$  действовать левыми сдвигами на множестве  $G/P = \bigcup_i g_i P$  левых смежных классов  $G$  по  $P$  (ограничение действия  $G$  на  $G/P$ , описанного в § 3 гл. 1). Согласно результатам гл. 1 длина любой орбиты относительно  $P_1$  делит порядок  $|P_1| = p^k$ ,  $k \leq n$ . Таким образом,

$$m = \frac{p^n m}{p^n} = \frac{|G|}{|P|} = |G/P| = p^{k_1} + p^{k_2} + \dots,$$

где  $p^{k_1}, p^{k_2}, \dots$  — длины орбит. Так как  $\text{НОД}(m, p) = 1$ , то хотя бы одна орбита имеет длину  $p^{k_i} = 1$ , т. е.

$$P_1 \cdot aP = aP \tag{1}$$

для некоторого элемента  $a = g_i \in G$  (это похоже на доказательство теоремы 2 из § 3 гл. 1). Переписав соотношение (1) в виде  $P_1 \cdot aPa^{-1} = aPa^{-1}$ , мы приходим к заключению, что

$$P_1 \subset aPa^{-1} \tag{2}$$

(поскольку  $aPa^{-1}$  — группа). В частности, если  $P_1$  — силовская  $p$ -подгруппа, то  $|P_1| = |P|$ , и из (2) следует, что  $P_1 = aPa^{-1}$ .  $\square$

**Доказательство теорем 1 и 3.** Теорему 1 можно интерпретировать как следствие теоремы 3, ибо  $N_p \equiv 1 \pmod{p}$ , а  $N_p \neq 0 \iff S \neq \emptyset$ ,  $S$  — множество всех силовских  $p$ -подгрупп группы  $G$ .

Что касается теоремы 3, то равенство  $N_p = (G : N(P))$  прямо вытекает из сопряжённости силовских  $p$ -подгрупп (теорема 2) и из общего утверждения о длине орбиты  $H^G$  в § 3 из гл. 1. К сравнению  $N_p \equiv 1 \pmod{p}$  мы придём, рассмотрев несколько более общую ситуацию. Именно, пусть  $|G| = p^s t$ , где  $s \leq n$ ,  $t$  может делиться на  $p$ , и пусть  $N_p(s)$  — число всех подгрупп порядка  $p^s$  в  $G$ . Оказывается, что имеет место сравнение  $N_p(s) \equiv 1 \pmod{p}$ ; в частности,  $G$  содержит подгруппы любого порядка  $p^s$ ,  $s = 1, 2, \dots, n$  и  $N_p(n) = N_p$ .

Рассуждаем следующим образом. Действие левыми сдвигами группы  $G$  на себе индуцирует согласно замечанию в конце п. 1 из § 2 действие  $G$  на множестве

$$\Omega = \{M \subset G \mid |M| = p^s\}$$

всех  $p^s$ -элементных подмножеств  $\{g_1, \dots, g_{p^s}\}$ . Напомним, что  $g \cdot \{g_1, \dots, g_{p^s}\} = \{gg_1, \dots, gg_{p^s}\}$ . Множество  $\Omega$  разбивается на  $G$ -орбиты  $\Omega_i : \Omega = \bigcup_i \Omega_i$ , так что

$$|\Omega| = \sum_i |\Omega_i|, \quad |\Omega_i| = (G : G_i),$$

где  $G_i = \{g \in G \mid gM_i = M_i\}$  — стационарная подгруппа некоторого представителя  $M_i \in \Omega_i$ .

Так как  $G_i M_i = M_i$ , то  $M_i = \bigcup_{j=1}^{\nu_i} G_i g_{ij}$  — объединение нескольких правых смежных классов  $G$  по  $G_i$ . Поэтому  $p^s = |M_i| = \nu_i |G_i|$ , откуда  $|G_i| = p^{s_i} \leq p^s$ . В случае  $|G_i| < p^s$  имеем  $|\Omega_i| = p^{s-s_i} \equiv 0 \pmod{pt}$ ; равенства  $|G_i| = p^s$  и  $|\Omega_i| = t$  эквивалентны. Получаем

$$\binom{|G|}{p^s} = |\Omega| \equiv \sum_{|\Omega_i|=t} |\Omega_i| \pmod{pt}. \quad (3)$$

Согласно вышесказанному  $|\Omega_i| = t \implies |G_i| = p^s \implies M_i = G_i a_i$  ( $a_i = g_{ij}$  — некоторый элемент из  $G$ ) и, стало быть,  $a_i^{-1} M_i = a_i^{-1} G_i a_i = P_i$  — подгруппа порядка  $p^s$ . Орбита  $\Omega_i$  исчерпывается некоторым числом левых смежных классов  $gP_i$  группы  $G$  по  $P_i$ .

Обратно: каждая подгруппа  $H \subset G$  порядка  $|H| = p^s$  приводит к орбите  $\Omega' = \{gH \mid g \in G\}$  длины  $t$ . Различные подгруппы  $H_i$  с  $|H_i| = p^s$  приводят к различным орбитам  $\Omega'_i$ , поскольку из  $H_i = gH_j$  следует  $e = gh_j$ , откуда  $g = h_j^{-1} \in H_j$  и  $H_i = H_j$ . Таким образом, имеется взаимно однозначное соответствие между подгруппами порядка  $p^s$  и орбитами  $\Omega_i$  длины  $t$ . Сравнение (3) переписывается в виде

$$\binom{|G|}{p^s} \equiv \sum_{|\Omega_i|=t} |\Omega_i| \equiv t N_p(s) \pmod{pt}, \quad (4)$$

где следовало бы писать  $N_p(s, G)$ , чтобы подчеркнуть зависимость  $N_p(s)$  от  $G$ .

До сих пор специфика группы  $G$  не играла никакой роли. Если взять за  $G$  циклическую группу порядка  $p^st$ , то для неё  $N_p(s, G) = 1$  (теорема 3 из § 2 гл. 1), и поэтому

$$\binom{|G|}{p^s} \equiv t \cdot 1 \pmod{pt}. \quad (5)$$

Так как левые части сравнений (4) и (5) по одному и тому же модулю  $pt$  совпадают, то имеем

$$t \equiv tN_p(s) \pmod{pt},$$

а это и даёт искомое сравнение  $N_p(s) \equiv 1 \pmod{p}$ .  $\square$

Хотя фактически доказано больше, чем требовалось, мы не намерены этим воспользоваться, отсылая интересующихся к специальной литературе.

**Пример.** Пусть  $G = \mathrm{SL}(2, Z_p)$  — группа всех  $2 \times 2$ -матриц с определителем 1 над полем  $Z_p$  из  $p$  элементов. Из разложения

$$\mathrm{GL}(2, Z_p) = \bigcup_{i=1}^{p-1} \left\{ \begin{array}{cc} i & 0 \\ 0 & 1 \end{array} \right\} \mathrm{SL}(2, Z_p)$$

полной линейной группы  $\mathrm{GL}(2, Z_p)$  в смежные классы по  $\mathrm{SL}(2, Z_p)$  следует, что

$$|\mathrm{GL}(2, Z_p)| = (p-1) |\mathrm{SL}(2, Z_p)|. \quad (6)$$

Рассматривая  $\mathrm{GL}(2, Z_p)$  как группу автоморфизмов двумерного векторного пространства  $V$  над  $Z_p$ , легко найти порядок  $|\mathrm{GL}(2, Z_p)|$ . Действительно,  $\mathrm{GL}(2, Z_p)$  действует на множестве пар  $\{\mathbf{v}_1, \mathbf{v}_2\}$  базисных векторов. Образом  $\mathbf{v}_1$  может быть любой отличный от нуля вектор  $\mathbf{f}_1 \in V$  (их всего  $p^2 - 1$  штук), а при всяком выборе  $\mathbf{f}_1$  образом  $\mathbf{v}_2$  может быть любой вектор  $\mathbf{f}_2$  из  $V \setminus \langle \mathbf{f}_1 \rangle$  (таких векторов имеется  $p^2 - p$  штук). Стало быть,  $|\mathrm{GL}(2, Z_p)| = (p^2 - 1)(p^2 - p)$ , что в сочетании с (6) приводит к формуле

$$|\mathrm{SL}(2, Z_p)| = p(p^2 - 1).$$

По крайней мере две силовские  $p$ -подгруппы группы  $\mathrm{SL}(2, Z_p)$  мы находим сразу:

$$P = \left\{ \left\| \begin{array}{cc} 1 & \alpha \\ 0 & 1 \end{array} \right\| \mid \alpha \in Z_p \right\}, \quad \overline{P} = \left\{ \left\| \begin{array}{cc} 1 & 0 \\ \alpha & 1 \end{array} \right\| \mid \alpha \in Z_p \right\}.$$

В соответствии с теоремой 3 имеем

$$N_p = (G : N(P)) = 1 + kp > 1,$$

а так как

$$\left\| \begin{array}{cc} \lambda & 0 \\ 0 & \lambda^{-1} \end{array} \right\| \left\| \begin{array}{cc} 1 & \alpha \\ 0 & 1 \end{array} \right\| \left\| \begin{array}{cc} \lambda^{-1} & 0 \\ 0 & \lambda \end{array} \right\| = \left\| \begin{array}{cc} 1 & \lambda^2 \alpha \\ 0 & 1 \end{array} \right\|$$

и, следовательно, нормализатор  $N(P)$  содержит подгруппу

$$H = \left\{ \left\| \begin{array}{cc} \lambda & \alpha \\ 0 & \lambda^{-1} \end{array} \right\| \mid \alpha, \lambda \in Z_p, \lambda \neq 0 \right\}$$

порядка  $p(p-1)$ , то остаётся единственная возможность

$$N(P) = H, \quad N_p = 1 + p.$$

Между группой

$$\mathrm{SL}(2, \mathbb{Z}_2) = \left\{ \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}, \begin{vmatrix} 0 & 1 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, \right. \\ \left. \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} \right\}$$

и симметрической группой  $S_3$  непосредственно устанавливается изоморфизм

$$(1 \ 2 \ 3) \mapsto \begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}, \quad (1 \ 2) \mapsto \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$$

(обе группы имеют одинаковое задание образующими и соотношениями). При  $p > 2$  группа  $G = \mathrm{SL}(2, \mathbb{Z}_p)$  имеет центр  $Z(G) = \{\pm E\}$  порядка 2. Факторгруппа  $\mathrm{PSL}(2, \mathbb{Z}_p) = G/Z(G)$ , которую естественно называть, как и в [ВА II], *проективной специальной группой* (она является группой преобразований проективной прямой

$$Z_p \mathbb{P}^1 = \mathbb{P}(V) = \{0, 1, \dots, p-1\} \cup \{\infty\},$$

играет важную роль в алгебре со времён Галуа. Дело в том, что при  $p > 3$  группа  $\mathrm{PSL}(2, \mathbb{Z}_p)$  простая, и это, наряду с  $A_n$ , — один из самых ранних примеров конечных простых групп.

Обратимся снова к общему случаю и получим одно полезное уточнение теоремы Силова.

**Теорема 4.** *Справедливы следующие утверждения:*

i) *силовская  $p$ -подгруппа  $P$  группы  $G$  нормальна в  $G$  тогда и только тогда, когда  $N_p = 1$ ;*

ii) *конечная группа  $G$  порядка  $|G| = p_1^{n_1} \dots p_k^{n_k}$  является прямым произведением своих силовских  $p_i$ -подгрупп  $P_1, \dots, P_k$  в точности тогда, когда все эти подгруппы нормальны в  $G$ .*

**Доказательство.** i) Все силовские подгруппы, отвечающие данному простому делителю  $p$  порядка  $|G|$ , по второй теореме Силова сопряжены, и если  $P$  — одна из них, то

$$N_p = 1 \iff xPx^{-1} = P \quad \forall x \in G \iff P \triangleleft G.$$

ii) Если  $G = P_1 \times \dots \times P_k$  — прямое произведение своих силовских подгрупп, то  $P_i \triangleleft G$  как любой прямой множитель. Значит, условие нормальности необходимо.

Пусть теперь  $P_i \triangleleft G$ ,  $1 \leq i \leq k$ , т.е.  $N_{p_i} = 1$ . Заметим, во-первых, что

$$x \in P_i \cap P_j, i \neq j \implies x^{p_i^s} = e, x^{p_j^t} = e \implies x = e.$$

Стало быть,  $P_i \cap P_j = e$ , а отсюда для любых  $x_i \in P_i$ ,  $x_j \in P_j$  имеем

$$(x_i, x_j) = \begin{cases} (x_i x_j x_i^{-1}) x_j^{-1} = x'_j x_j^{-1} \in P_j \\ x_i (x_j x_i^{-1} x_j^{-1}) = x_i x'_i \in P_i \end{cases} \implies (x_i, x_j) = e,$$

т.е. элементы  $x_i$  и  $x_j$  перестановочны.

Представим на минуту, что единичный элемент  $e \in G$  записан в виде  $e = y_1 y_2 \dots y_k$ , где  $y_i \in P_i$  — элемент порядка  $a_i = p_i^{b_i}$ . Положив  $a = \prod_{i \neq j} a_i$  и воспользовавшись перестановочностью  $y_1, \dots, y_k$ , получим

$$e = (y_1 y_2 \dots y_k)^a = y_1^a y_2^a \dots y_k^a = y_j^a.$$

Но так как  $a$  и  $a_j$  взаимно просты, то  $y_j^{a_j} = y_j^a = e \implies y_j = e$ . Это верно при любом  $j$ , и, стало быть, равенство  $e = y_1 y_2 \dots y_k$  возможно лишь при  $y_1 = y_2 = \dots = y_k = e$ .

С другой стороны, каждый элемент  $x \in G$  порядка  $r = r_1 r_2 \dots r_k$ ,  $r_i = p_i^{s_i}$ , записывается в виде

$$x = x_1 x_2 \dots x_k, \quad |\langle x_i \rangle| = r_i, \quad 1 \leq i \leq k. \quad (7)$$

Достаточно положить  $x_i = x^{t_i r'_i}$ , где показатели определяются условиями

$$r'_i = \frac{r}{r_i}, \quad 1 = \sum_{i=1}^k t_i r'_i.$$

Если теперь  $x = x'_1 x'_2 \dots x'_k$  — другая запись  $x$  в виде произведения  $p_i$ -элементов, то в силу перестановочности  $x_i$ ,  $x'_i$  с различными нижними индексами будем иметь

$$e = (x'_1 x'_2 \dots x'_k) (x_1 x_2 \dots x_k)^{-1} = x'_1 x_1^{-1} \cdot x'_2 x_2^{-1} \dots x'_k x_k^{-1},$$

что, как было показано выше, влечет равенства  $x'_1 x_1^{-1} = x'_2 x_2^{-1} = \dots = x'_k x_k^{-1} = e$ , т.е.  $x'_1 = x_1, x'_2 = x_2, \dots, x'_k = x_k$ .

Итак, каждый элемент группы  $G$  записывается, и притом единственным образом, в виде (7), т.е. (см. § 2)  $G = P_1 \times \dots \times P_k$ .  $\square$

**Замечание.** Нормальная силовская  $p$ -подгруппа  $P$  группы  $G$  *характеристична* в  $G$ , т.е. инвариантна при действии любого автоморфизма  $\varphi \in \text{Aut}(G)$ . Действительно,  $|\varphi(P)| = |P|$ , поэтому  $\varphi(P)$  — силовская  $p$ -подгруппа, и, стало быть,  $\varphi(P) = P$ , если  $N_p = 1$ . Достойно замечания также то, что аналоги силовских подгрупп прослеживаются в алгебраических структурах, далёких от конечных групп.

### УПРАЖНЕНИЯ

**1.** Найти число силовских 5-подгрупп в  $A_5$ .

**2.** Проверить, что множество  $P$  матриц

$$\pm \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, \quad \pm \begin{vmatrix} 1 & -1 \\ -1 & -1 \end{vmatrix}, \quad \pm \begin{vmatrix} -1 & -1 \\ -1 & 1 \end{vmatrix}, \quad \pm \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}$$

над  $Z_3$  составляет группу, изоморфную группе кватернионов  $Q_8$  и являющуюся силовской 2-подгруппой в  $\text{SL}(2, Z_3)$ . Показать, что  $P \triangleleft \text{SL}(2, Z_3)$ .

**3.** Показать, что группы  $S_4$  и  $\text{SL}(2, Z_3)$  не изоморфны. Будут ли изоморфны группы  $\text{PSL}(2, Z_3)$  и  $A_4$ ?

**4.** Доказать, что всякая группа  $G$  порядка  $pq$  ( $p < q$  — простые числа) является либо циклической, либо неабелевой с нормальной силовской  $q$ -подгруппой, причём последнее возможно тогда и только тогда, когда  $q - 1$  делится на  $p$ . В частности, все группы порядка 15 циклические.

**5.** Получить заново (см. [ВА I, гл. 6 § 1, пример]) сравнение  $(p - 1)! + 1 \equiv 0 \pmod{p}$  для простого  $p$  путём прямого подсчёта числа  $N_p$  силовских  $p$ -подгрупп в симметрической группе  $S_p$ .

**6.** Убедиться в том, что группа  $G$  порядка  $|G| \leq 30$  не может быть простой.

### § 3. Конечно порождённые абелевы группы

Этот параграф написан так, что его зависимость от остального материала главы минимальна.

**1. Примеры и предварительные результаты.** Как уже не раз упоминалось, абелевы группы иногда удобно записывать аддитивно, используя  $+$  в качестве основной операции. Таким образом, если  $(A, +)$  — аддитивная абелева группа, то:

$$1) a + a' = a' + a \text{ для любых элементов } a, a' \in A;$$

$$2) na := \underbrace{a + a + \dots + a}_n \text{ при любом } n > 0, n \in \mathbb{Z};$$

3)  $0 \cdot a = 0$  (слева  $0 \in \mathbb{Z}$ , справа  $0$  — нейтральный элемент группы);

$$4) (-n)a = \underbrace{(-a) + (-a) + \dots + (-a)}_n \text{ при любом } n > 0, n \in \mathbb{Z}.$$

Понятно, что при этом выполнены свойства

$$m(na) = (mn)a, \quad (m + n)a = ma + na, \quad n(a + a') = na + na'.$$

Стало быть, для любого набора элементов  $a_1, \dots, a_m \in A$  мы можем рассматривать целочисленные комбинации

$$n_1a_1 + n_2a_2 + \dots + n_ma_m \in A$$

с коэффициентами  $n_i \in \mathbb{Z}$ .

**Определение.** Система элементов  $a_1, \dots, a_m$  аддитивной абелевой группы  $A$  называется *системой образующих* или *системой порождающих*, если

$$\{n_1a_1 + \dots + n_ma_m \mid n_i \in \mathbb{Z}\} = A,$$

т.е. каждый элемент  $a' \in A$  записывается, быть может, многими способами, в виде  $a' = n_1a_1 + \dots + n_ma_m$ . В таком случае пишут  $A = \langle a_1, a_2, \dots, a_m \rangle$ .

**Пример 1.** Обычная единица  $1$  — образующая группы  $(\mathbb{Z}, +)$ ;  $-1$  также будет образующей, но  $n \neq \pm 1$  образующей не является.

**Пример 2.** Абелева группа  $\mathbb{Z}^n$  целочисленных векторов (векторов с целыми координатами) в координатном пространстве  $\mathbb{Q}^n$  обладает системой образующих

$$\varepsilon_1 = (1, 0, \dots, 0), \quad \varepsilon_2 = (0, 1, \dots, 0), \quad \dots, \quad \varepsilon_n = (0, 0, \dots, 1).$$

Пример 3. В группе  $\mathbb{Z}^2$  можно взять и другие системы образующих, скажем,

$$b_1 = (1, 1), \quad b_2 = (1, -1), \quad b_3 = (4, 1).$$

Так как  $\varepsilon_1 = 3b_1 + 2b_2 - b_3$ ,  $\varepsilon_2 = -2b_1 - 2b_2 + b_3$ , то это действительно образующие группы  $\mathbb{Z}^2$ . Однако никакая пара элементов из множества  $\{b_1, b_2, b_3\}$  системой образующих группы  $\mathbb{Z}^2$  не является. Убедитесь в этом.

Нетрудно назвать группы, в которых нет никакой конечной системы образующих. Например, ими являются  $\mathbb{R}^{(+)} = (\mathbb{R}, +)$  и  $U = \{\alpha \in \mathbb{C} \mid |\alpha| = 1\}$  (группа с операцией умножения). Действительно, эти группы — несчётные множества, а группа с конечным числом образующих всегда счётна. Имеются и другие примеры:  $\mathbb{Q}^{(+)}$  или  $\mathbb{Q}^*$  (несложная проверка).

*Предложение 1. Прямая сумма*

$$A = A_1 \oplus \dots \oplus A_n$$

*конечного числа циклических групп  $A_i$  является группой с конечным числом образующих.*

*Доказательство.* Действительно, если  $A_i = \langle a_i \rangle$ , то элементы

$$(a_1, 0, \dots, 0), \quad (0, a_2, \dots, 0), \quad \dots, \quad (0, 0, \dots, a_n)$$

будут образующими группы  $A$ .  $\square$

*Предложение 2. Прямая сумма  $A = C_m \oplus C_n$  двух конечных циклических групп взаимно простых порядков  $m, n$  является циклической группой порядка  $mn$ .*

*Доказательство.* См. [ВА I, гл. 4, § 2, упр. 3].  $\square$

Итак, имеет место импликация

$$\text{НОД}(m, n) = 1 \implies C_m \oplus C_n \cong C_{mn}. \quad (1)$$

Мы видим, что абелевы группы с конечным числом образующих довольно разнообразны по своим свойствам. Они достойны детально-го изучения хотя бы потому, что возникают естественным образом в геометрии, в топологии, в гомологической алгебре. Стоит ещё добавить, что если  $G$  — произвольная конечно порождённая группа, а это обширный класс групп, то по теореме 5 из § 4 гл. 1 факторгруппа по коммутанту  $G/G'$  является абелевой группой с конечным числом образующих.

**2. Абелевы группы без кручения.** По определению группа  $A$  без кручения, если она не имеет ненулевых элементов конечного порядка, т.е.  $na = 0$ ,  $n \neq 0 \implies a = 0$ . Такие группы очень похожи на векторные пространства, как это будет видно из дальнейшего.

*Определение.* Система элементов  $a_1, \dots, a_k \in A$  называется *независимой*, если из равенства  $n_1 a_1 + \dots + n_k a_k = 0$ , где  $n_i \in \mathbb{Z}$ , следует, что  $n_1 = \dots = n_k = 0$ .

Система элементов  $a_1, \dots, a_n \in A$  называется *базисом*, если она:

- 1) независима;
- 2) является системой образующих группы  $A$ .

**Лемма 1.** *Если  $A = \langle a_1, \dots, a_m \rangle$ , а элементы  $b_1, \dots, b_n \in A$  образуют независимую систему, то  $n \leq m$ .*

**Доказательство.** Выразим  $b_i$  через  $a_1, \dots, a_m$ :

$$b_i = \sum_{j=0}^m \beta_{ij} a_j, \quad \beta_{ij} \in \mathbb{Z},$$

и рассмотрим целочисленные векторы-строки  $B_i = (\beta_{i1}, \dots, \beta_{im}) \in \mathbb{Q}^m$  (координатное векторное пространство над  $\mathbb{Q}$ ). Предположив противное,  $n > m$ , мы должны заключить, что система  $\{B_1, \dots, B_n\}$  линейно зависима. Значит, найдутся не все равные нулю  $r_i \in \mathbb{Q}$  такие, что

$$r_1 B_1 + r_2 B_2 + \dots + r_n B_n = 0. \quad (2)$$

Пусть  $d$  — общий знаменатель рациональных чисел  $r_i : r_i = s_i/d$ ,  $s_i \in \mathbb{Z}$ . Умножая обе части равенства (2) на  $d$ , получаем соотношение

$$s_1 B_1 + s_2 B_2 + \dots + s_n B_n = 0$$

с целыми коэффициентами. Расписывая его по координатно, придём к линейной системе

$$s_1 \beta_{1j} + s_2 \beta_{2j} + \dots + s_n \beta_{nj} = 0, \quad 1 \leq j \leq m.$$

В таком случае

$$\sum_{i=1}^n s_i b_i = \sum_{i=1}^n s_i \left( \sum_{j=1}^m \beta_{ij} a_j \right) = \sum_{j=1}^m \left( \sum_{i=1}^n s_i \beta_{ij} \right) a_j = 0$$

— противоречие.  $\square$

**Теорема 1.** *Справедливы следующие утверждения.*

- 1) *Всякая конечно порождённая абелева группа  $A$  без кручения обладает базисом.*
- 2) *Все базисы группы  $A$  равномощны (состоят из одинакового числа элементов).*

**Доказательство.** 1) Общая идея: уменьшение числа элементов в системе образующих до тех пор, пока она не станет независимой. Пусть  $\{a_1, \dots, a_m\}$  — некоторая система образующих группы  $A$ . Выражение вида  $s_1 a_1 + \dots + s_m a_m = 0$  естественно называть *соотношением* на  $a_1, \dots, a_m$ . Число, равное  $\min_i |s_i|$ , будем называть *высотой соотношения*, а соотношение на  $a_1, \dots, a_m$ , у которого высота минимальна, — *минимальным соотношением*. Такое соотношение всегда существует, поскольку высота — натуральное число. С другой стороны, минимальное соотношение не обязательно единственное. Доказательство распадается на ряд простых утверждений.

а) Если  $s_1a_1 + \dots + s_ma_m = 0$  — минимальное соотношение, то  $\text{НОД}(s_1, \dots, s_m) = 1$ .

Действительно, если  $s_i = ds'_i$ ,  $1 \leq i \leq m$ , то

$$d(s'_1a_1 + \dots + s'_ma_m) = 0 \implies s'_1a_1 + \dots + s'_ma_m = 0,$$

поскольку  $A$  — группа без кручения. При  $d > 1$  мы приходим к соотношению меньшей высоты, что исключено условием минимальности.

б) Если  $s_1a_1 + \dots + s_ma_m = 0$  — соотношение высоты 1 и, скажем,  $|s_k| = 1$ , то множество из  $m - 1$  элементов  $\{a_1, \dots, a_{k-1}, a_{k+1}, \dots, a_m\}$  будет системой образующих.

Это достаточно очевидно: по условию  $\sum_{i \neq k} s_i a_i \pm a_k = 0$ , поэтому  $a_k = \sum_{i \neq k} s'_i a_i$ ,  $s'_i = \pm s_i$ , так что оставшиеся элементы порождают  $A$ .

в) Если высота минимального соотношения системы  $\{a_1, \dots, a_m\}$  равна  $h > 1$ , то можно построить новую систему образующих  $\{a'_1, \dots, a'_m\}$ , высота минимального соотношения которой будет строго меньше  $h$ .

Действительно, мы можем так перенумеровать образующие, что  $|s_1| = \min |s_i| = h$ . Умножая, если надо, соотношение на  $-1$ , полагаем  $s_1 = h$ . Согласно а) не все  $s_i$  делятся на  $h$ . Производя ещё раз перенумерацию, можем считать, что  $h \nmid s_2 : s_2 = qh + r$ ,  $0 < r < h$ . Теперь наше соотношение перепишется в виде

$$ha'_1 + ra'_2 + s_3a'_3 + \dots + s_ma'_m = 0,$$

где  $a'_1 = a_1 + qa_2$ ,  $a'_i = a_i$ ,  $i > 1$ . Ясно, что  $\{a'_1, a'_2, \dots, a'_m\}$  будет системой образующих, удовлетворяющей соотношению высоты  $r < h$  (высота её минимального соотношения, возможно,  $\leq r$ ).

Утверждение 1) нашей теоремы доказывается теперь следующим образом. Пусть  $n$  — минимальное число образующих группы  $A$  и  $\{a_1, \dots, a_n\}$  — одна из таких систем. Считаем также, что она удовлетворяет соотношению минимальной высоты  $h$  (по всем системам мощности  $n$ ).

Если  $h = 1$ , то в соответствии с б) число образующих уменьшается по крайней мере до  $n - 1$ , что исключено нашим выбором. Если  $h > 1$ , то согласно в)  $\{a_1, \dots, a_n\}$  перестаёт быть системой с минимальным соотношением наименьшей (опять-таки по всем системам мощности  $n$ ) высоты. Остается признать, что  $\{a_1, \dots, a_n\}$  — независимая система, т.е. базис группы  $A$ .

2) Предположим, что  $\{a_1, \dots, a_m\}$ ,  $\{b_1, \dots, b_n\}$  — какие-то два базиса группы  $A$ . Дважды применяя лемму 1, получаем неравенства  $n \leq m$  и  $m \leq n$ , т.е.  $m = n$ .  $\square$

**Определение.** Конечно порождённая абелева группа  $A$  называется *свободной ранга  $n$*  и обозначается символом  $F_n^{ab}$ , если

$$A = F_n^{ab} \cong \mathbb{Z}^n = \mathbb{Z} \oplus \dots \oplus \mathbb{Z}.$$

Ранг группы, состоящей из одного нуля, считается равным нулю. Любой базис свободной абелевой группы  $A$  называется также её *свободной системой образующих*.

Только что доказанная теорема 1 утверждает на самом деле, что  *всякая конечно порождённая абелева группа  $A$  без кручения является свободной некоторого ранга  $n$ .*

Действительно, если  $\{a_1, \dots, a_n\}$  — базис группы  $A$ , то любой элемент  $a \in A$  однозначно записывается в виде  $a = \alpha_1 a_1 + \dots + \alpha_n a_n$ ,  $\alpha_i \in \mathbb{Z}$  (имея другую запись  $a = \alpha'_1 a_1 + \dots + \alpha'_n a_n$ , мы имели бы соотношение  $0 = a - a = (\alpha_1 - \alpha'_1) a_1 + \dots + (\alpha_n - \alpha'_n) a_n$ , откуда  $\alpha'_1 = \alpha_1, \dots, \alpha'_n = \alpha_n$ ). Сопоставление  $a \mapsto (\alpha_1, \dots, \alpha_n)$  задаёт, очевидно, изоморфизм  $A$  с группой  $\mathbb{Z}^n$  целочисленных векторов. Это и значит, что  $A$  — свободная группа ранга  $n$ .

**3. Свободные абелевые группы конечного ранга.** Следующее утверждение технического характера сильно упрощает изучение подгрупп и факторгрупп свободной абелевой группы.

**Теорема 2.** *Пусть  $B$  — ненулевая подгруппа свободной абелевой группы  $A$  конечного ранга  $n$ . Тогда в  $A$  и  $B$  можно выбрать базисы соответственно  $\{a_1, \dots, a_n\}$  и  $\{b_1, \dots, b_k\}$  такие, что  $b_i = m_i a_i$ , где  $m_i \geq 0$  — неотрицательные целые числа, причём  $m_{i-1} | m_i$ ;  $i = 2, 3, \dots, k$ ,  $k \leq n$  (возможно, что  $m_{k+1} = \dots = m_n = 0$ ).*

**Доказательство.** Выберем в  $A$  базис  $\{v_1, \dots, v_n\}$ , обладающий следующим экстремальным свойством:  $B$  содержит элемент

$$b_1 = m_1 v_1 + s_2 v_2 + \dots + s_n v_n$$

с положительным и самым минимальным коэффициентом  $m_1$ . Имеется в виду, что при другом упорядочении элементов  $v_i$ , при любом другом выборе базиса в  $A$  или для какого-либо иного элемента  $b \in B$  первый положительный коэффициент не может быть меньше  $m_1$ .

Утверждается, что тогда  $m_1 | s_i$ ,  $i = 2, \dots, n$ . Действительно, если  $s_i = q_i m_1 + r_i$ ,  $0 \leq r_i < m_1$ , то

$$b_1 = m_1 a_1 + r_2 v_2 + \dots + r_n v_n,$$

где  $a_1 = v_1 + q_2 v_2 + \dots + q_n v_n$ . Понятно, что  $\{a_1; v_2, \dots, v_n\}$  — базис группы  $A$ . Из экстремальности  $\{v_1, \dots, v_n\}$  следует, что  $r_2 = \dots = r_n = 0$ . Таким образом,  $b_1 = m_1 a_1$ .

По тем же причинам

$$b' = m'_1 a_1 + s'_2 v_2 + \dots + s'_n v_n \in B \implies m_1 | m'_1,$$

и если  $m'_1 = q m_1$ , то

$$b'' = b' - q b_1 \in \langle v_2, \dots, v_n \rangle,$$

т.е.

$$A = \langle a_1 \rangle \oplus A_1, \quad B = \langle b_1 \rangle + B_1,$$

где  $b_1 = m_1 a_1$ ,  $B_1 \subseteq A_1 := \langle v_2, \dots, v_n \rangle$ .

Итак,  $B_1$  — подгруппа свободной абелевой группы  $A_1$  ранга  $n - 1$ . Простая индукция по рангу приводит к заключению, что для пары  $(A_1, B_1)$  утверждение теоремы справедливо, т.е. в  $A_1$  найдутся элементы  $a_2, \dots, a_n$ , для которых

$$A_1 = \langle a_2, \dots, a_n \rangle, \quad B_1 = \langle b_2, \dots, b_k \rangle, \quad b_i = m_i a_i, \quad m_{i-1} | m_i, \quad i > 2.$$

На каком-то этапе, возможно, появятся нули:  $m_{k+1} = m_{k+2} = \dots = m_n = 0$ .

Осталось доказать, что  $m_1 | m_2$ . Положим  $m_2 = qm_1 + r$ ,  $0 \leq r < m_1$ , и заменим временно  $a_1$  на  $a'_1 = a_1 + qa_2$ . Относительно базиса  $\{a'_1, a_2, \dots, a_n\}$  группы  $A$  элемент  $b_1 + b_2 \in B$  имеет вид

$$b_1 + b_2 = m_1 a_1 + (qm_1 + r)a_2 = m_1 a'_1 + ra_2.$$

Отсюда видно, что при  $r > 0$  мы вступаем в противоречие со свойством экстремальности исходного базиса, или, что то же самое, с выбором  $m_1$ . Таким образом,  $r = 0$ , и доказательство завершено.  $\square$

В условиях теоремы 2 говорят о *согласованности* базисов в  $A$  и  $B$ .

**Следствие 1.** *Всякая подгруппа  $B$  свободной абелевой группы  $A$  ранга  $n$  свободна ранга  $k \leq n$ .*

**Доказательство.** По теореме 2 в группах  $A, B \neq 0$  можно выбрать согласованные базисы

$$A = \langle a_1, \dots, a_n \rangle, \quad B = \langle b_1, \dots, b_k \rangle, \quad b_i = m_i a_i, \quad 1 \leq i \leq k \leq n,$$

где  $m_1 | m_2, m_2 | m_3, \dots, m_{k-1} | m_k$  ( $m_{k+1} = \dots = m_n = 0$ ). Итак, любой элемент  $b \in B$  записывается в виде

$$b = s_1 m_1 a_1 + s_2 m_2 a_2 + \dots + s_k m_k a_k.$$

Если для некоторых  $s_1, s_2, \dots, s_k \in \mathbb{Z}$ , одновременно не равных нулю, будет  $b = 0$ , то мы приходим к нетривиальной линейной зависимости системы  $\{a_1, \dots, a_k\}$  с коэффициентами  $s_1 m_1, s_2 m_2, \dots, s_k m_k$ , что исключено, поскольку  $\{a_1, \dots, a_k\}$  — часть базиса группы  $A$ . Стало быть, система образующих  $\{b_1, \dots, b_k\}$  группы  $B$  независима (или свободна) и  $B$  — свободная группа ранга  $k \leq n$ .  $\square$

При  $n = 1$  утверждение следствия 1, конечно, нам известно: в группе  $(\mathbb{Z}, +)$  каждая ненулевая подгруппа имеет вид  $m\mathbb{Z}$  и является бесконечной циклической, т.е. свободной ранга 1.

**Следствие 2.** *Любой гомоморфный образ  $\varphi(A)$  свободной абелевой группы  $A$  ранга  $n$  изоморчен группе*

$$\mathbb{Z}^{n-k} \oplus Z_{m_1} \oplus \dots \oplus Z_{m_k}, \quad 0 \leq k \leq n,$$

причём  $m_{i-1} | m_i$ ,  $2 \leq i \leq k$ .

**Доказательство.** Пусть  $B = \text{Ker } \varphi$  — ядро гомоморфизма  $\varphi$ . По теореме о гомоморфизмах (теорема 2 из § 4 гл. 1)  $\varphi(A) \cong A/B$ . Опишем эту факторгруппу, для чего в соответствии с теоремой 2 выберем в  $A$  и  $B$  согласованные базисы. Пусть

$$A = A_1 \oplus \dots \oplus A_n, \quad B = B_1 \oplus \dots \oplus B_n,$$

где

$$A_i = \mathbb{Z}a_i, \quad B_i = B \cap A_i = \begin{cases} n_i \mathbb{Z}a_i & \text{при } i \leq k, \\ 0 & \text{при } i > k. \end{cases}$$

Факторизация бесконечной циклической группы  $\langle a_i \rangle = \mathbb{Z}a_i$  по подгруппе  $m_i a_i \mathbb{Z}$  приводит либо к той же группе  $\langle a_i \rangle$  при  $i > k$ , либо к циклической группе  $\langle \bar{a}_i \mid m_i \bar{a}_i = 0 \rangle$  порядка  $m_i$ , изоморфной  $Z_{m_i}$ ,  $i \leq k$ .

По теореме 7 из § 4 гл. 1 имеем

$$\begin{aligned} A/B &\cong A_1/B_1 \oplus \dots \oplus A_k/B_k \oplus A_{k+1}/B_{k+1} \oplus \dots \oplus A_n/B_n \cong \\ &\cong Z_{m_1} \oplus \dots \oplus Z_{m_k} \oplus \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n-k}. \quad \square \end{aligned}$$

**4. Строение конечно порождённых абелевых групп.** Последнее следствие теоремы 2 даёт фактически ответ на основной вопрос о конечно порождённых абелевых группах. Предварительно докажем одно универсальное свойство свободной абелевой группы.

**Лемма 3.** Пусть  $X$  — множество образующих абелевой группы  $F$ ,  $|X| = n$ . Тогда эквивалентны следующие утверждения:

i)  $F = F_n^{ab}$  — свободная абелева группа и  $X$  — множество её свободных образующих;

ii) каждое однозначное отображение  $\varphi$  множества  $X$  в некоторую абелеву группу  $A$  индуцирует гомоморфизм  $\tilde{\varphi}: F \rightarrow A$ .

**Доказательство.** i)  $\Rightarrow$  ii). Имеем  $X = \{x_1, \dots, x_n\}$ ,  $\varphi: X \rightarrow A$ . Так как каждый элемент из  $F$  однозначно записывается в виде  $\sum_i s_i x_i$ , то, очевидно, отображение

$$\tilde{\varphi}: \sum_i s_i x_i \mapsto \sum_i s_i \varphi(x_i)$$

является гомоморфизмом из  $F$  в  $A$ .

ii)  $\Rightarrow$  i). В этой импликации мы убедимся сразу, взяв в качестве  $A$  свободную группу со множеством образующих  $\{a_1, \dots, a_n\}$  той же мощности, что и  $X$ . Если  $\varphi: x_i \mapsto a_i$  — существующее по условию однозначное отображение, которое продолжается до гомоморфизма  $\tilde{\varphi}: F \rightarrow A$ , то

$$\sum_i s_i x_i = 0 \implies \sum_i s_i a_i = 0 \implies s_i = 0,$$

т.е.  $x_1, \dots, x_n$  — свободные образующие и  $F = F_n^{ab}$ .  $\square$

Понятно, что в лемме 3 условие конечности множества  $X$  не играет никакой роли, но и бесконечные множества нам рассматривать ни к чёму.

**Теорема 3.** *Каждая абелева группа с  $n$  образующими является гомоморфным образом свободной абелевой группы  $F_n^{ab}$ .*

**Доказательство** — непосредственное следствие леммы 3.  $\square$

Соединяя следствие 2 теоремы 2 и теорему 3, мы приходим к основному результату этого параграфа.

**Теорема 4.** 1) *Всякая конечно порождённая абелева группа  $A$  является прямой суммой свободной абелевой группы  $F_r^{ab}$  некоторого ранга  $r \geq 0$  и конечной абелевой группы.*

2) *Всякая конечная абелева группа является прямой суммой некоторого числа  $k$  циклических групп порядков  $m_1, \dots, m_k$ , где  $m_{i-1} | m_i$ ,  $1 < i \leq k$ .*

**5. Другие подходы к проблеме классификации.** Свободные группы проявляют себя и в других обстоятельствах, на которых мы вкратце остановимся.

**Лемма 4.** *Пусть факторгруппа*

$$A/B = \bigoplus_{i=1}^n (A_i/B)$$

— прямая сумма, причём  $B$  — прямое слагаемое в каждой подгруппе  $A_i : A_i = B \oplus J_i$ . Тогда  $B$  — прямое слагаемое в  $A$  и

$$A = B \oplus \left( \bigoplus_{i=1}^n J_i \right).$$

**Доказательство.** Очевидно, что  $B$  и все подгруппы  $J_i$  порождают  $A$ . Предположим, что  $b + x_1 + \dots + x_n = 0$  с какими-то элементами  $b \in B$  и  $x_i \in J_i$ . Переходя к факторгруппе по модулю  $B$ , мы получаем соотношение

$$\bar{x}_1 + \dots + \bar{x}_n = 0 \quad (\bar{x} = x + B).$$

Но так как по условию  $A_i/B$  — прямое слагаемое в  $A/B$ , то  $\bar{x}_i = \bar{0}$ . Стало быть,  $x_i \in B$ , т.е.  $x_i \in (B \cap J_i) = 0$ , а это приводит к заключению, что  $b = 0$ , и, значит, любая линейная зависимость  $b + x_1 + \dots + x_n = 0$  — тривиальная.  $\square$

**Теорема 5.** *Пусть  $A$  — абелева группа,  $B$  — её подгруппа. Если факторгруппа  $A/B$  свободная, то  $A$  — прямая сумма  $B$  и свободной группы  $F^{ab}$ :  $A = B \oplus F^{ab}$ .*

**Доказательство.** Так как  $A/B$  — прямая сумма бесконечных циклических групп, то по лемме 4 достаточно рассмотреть случай, когда  $A/B \cong \mathbb{Z}$ . Итак,

$$A/B = \langle \bar{a} \rangle \cong \mathbb{Z}.$$

Возьмём  $0 \neq a \in \bar{a}$  (элемент смежного класса  $\bar{a}$ , не содержащийся в  $B$ ). Тогда элементы  $ka$  будут представителями смежных классов  $k\bar{a}$ ,  $k = 0, \pm 1, \pm 2, \dots$ , т.е.  $A = B \oplus \langle a \rangle$ .  $\square$

**Определение.** *Периодической частью* (или *подгруппой кручения* — от английского torsion subgroup) абелевой группы  $A$  называется подгруппа  $T(A)$  всех элементов из  $A$  конечного порядка.

В том, что  $T(A)$  — подгруппа, легко убедиться непосредственно: если  $sa = 0, tb = 0$ ;  $a, b \in T(A)$ , то  $st(va + \mu b) = vt(sa) + \mu s(tb) = 0$  и, значит,  $va + \mu b \in T(A)$ .

**Лемма 5.** *Факторгруппа  $A/T(A)$  — группа без кручения.*

**Доказательство.** Предположим, что  $\bar{a} = a + T(A)$  — элемент конечного порядка в  $A/T(A)$ , т.е.  $m\bar{a} = ma + T(A) = \bar{0}$ , или, что то же самое,  $ma \in T(A)$ . Значит,  $n(ma) = 0$  для некоторого  $n \in \mathbb{Z}$ . Но если  $(nm)a = 0$ , то по определению периодической части  $a \in T(A)$  и  $\bar{a} = \bar{0}$ .  $\square$

Пусть теперь  $A$  — абелева группа с  $n$  образующими. Как утверждает лемма,  $A/T(A)$  — группа без кручения. Число её образующих, очевидно, не превосходит  $n$ . Согласно теореме 1  $A/T(A) \cong F_r^{ab}$ ,  $r \leq n$ , — свободная группа. По теореме 5 имеем разложение

$$A = T(A) \oplus F_r^{ab}.$$

Теперь видно, что  $T(A) \cong A/F_r^{ab}$ , и, значит, число образующих подгруппы  $T(A)$  тоже не превосходит  $n$ . Если  $a_1, \dots, a_s$  — её образующие и  $m_1 a_1 = \dots = m_s a_s = 0$ , то, очевидно,  $T(A)$  — конечная группа порядка  $\leq m_1 \dots m_s$ . Мы пришли к следующему утверждению.

**Теорема 6.** *Всякая конечно порождённая абелева группа  $A$  является прямой суммой конечной абелевой группы  $T(A)$  и свободной абелевой группы  $F_r^{ab}$  некоторого ранга  $r$ .*

Фактически мы уже знаем (теорема 4), что  $T(A)$  — прямая сумма циклических групп, но мы хотим пойти другим путём.

**Теорема 7.** *Всякая периодическая абелева группа  $A$  может быть записана в виде прямой суммы  $p$ -групп  $A(p)$ , отвечающих различным простым  $p$ . Прямые слагаемые  $A(p)$  однозначно определяются группой  $A$ .*

**Доказательство.** Пусть  $A(p)$  состоит из всех элементов  $x \in A$ , порядки которых являются степенями простого числа  $p$  (воз-

можно, что  $A(p) = 0$ ). Тогда  $A(p)$  — подгруппа в  $A$ , поскольку

$$p^k x = 0 = p^l y; \quad x, y \in A, \quad m = \max(k, l) \implies$$

$$\implies p^m(x - y) = 0 \implies x - y \in A(p).$$

Каждый элемент из  $A(p_1) + \dots + A(p_s)$  имеет порядок, который не может делиться на простое  $q$ , отличное от  $p_1, \dots, p_s$ . Следовательно,

$$A(q) \cap (A(p_1) + \dots + A(p_s)) = 0.$$

А это значит, что подгруппы  $A(p)$  порождают прямую сумму  $\bigoplus_p A(p)$  (суммирование по всем простым  $p$ ).

Остаётся лишь доказать, что группа  $A$  порождается своими  $p$ -компонентами  $A(p)$ . Пусть  $a \in A$  и  $|\langle a \rangle| = n = p_1^{k_1} \dots p_r^{k_r}$  с различными простыми  $p_i$ . Целые числа  $n_i$ , определённые равенствами  $n = n_i p_i^{k_i}$ ,  $i = 1, \dots, r$ , взаимно просты и, следовательно,

$$t_1 n_1 + \dots + t_r n_r = 1$$

для некоторых  $t_i \in \mathbb{Z}$ . Таким образом,

$$a = \sum_{i=1}^r t_i(n_i a),$$

где  $n_i a \in A(p_i)$  (действительно,  $p_i^{k_i}(n_i a) = na = 0$ ). Получаем, что  $a \in A(p_1) + \dots + A(p_r)$ .

Единственность  $A(p)$  получается сразу, если заметить, что в любом прямом разложении  $A = \bigoplus_p A'(p)$  ни один элемент, не лежащий в  $A'(p)$ , не может быть порядка  $p^t$ . Стало быть,  $A'(p) \supseteq A(p)$ . Обратное включение очевидно.  $\square$

**Теорема 8** (Фробениус–Штикельбергер). *Каждая конечная абелева группа является прямой суммой конечного числа примарных циклических групп.*

**Доказательство.** В силу теоремы 7 можно ограничиться конечными  $p$ -группами. Докажем утверждение, представляющее независимый интерес.

Пусть  $A$  — конечная абелева  $p$ -группа,  $a \in A$  — её элемент максимального порядка  $p^k$ . Тогда циклическая группа  $\langle a \rangle$  — прямое слагаемое в  $A$ .

Действительно, пусть  $B$  — максимальная подгруппа в  $A$ , обладающая свойством  $B \cap \langle a \rangle = \{0\}$ . Тогда, очевидно,

$$H := \langle B, a \rangle = B \oplus \langle a \rangle.$$

Предположим, что  $H$  — собственная подгруппа в  $A$ . Тогда мы можем найти элемент  $x \in A$  такой, что  $x \notin H$ , но  $px \in H$  (если  $p^i x \in H$ ,  $p^{i-1} x \notin H$ , то следует заменить  $x$  на  $p^{i-1} x$ ). Имеем

$$px = b + la \quad (b \in B, l \in \mathbb{Z})$$

и в силу максимальности  $p^k$

$$p^{k-1}b + p^{k-1}la = p^kx = 0.$$

Отсюда  $p^{k-1}la = 0$ , а в таком случае  $p^{k-1}l$  делится на  $p^k$ , т.е.  $l = pj$  для некоторого  $j \in \mathbb{Z}$ . Теперь для  $y = x - ja$  имеем  $py = b \in B$ ; но  $y \notin H$ , так что  $\langle B, y \rangle$  содержит (в силу максимальности  $B$ ) ненулевой элемент  $ra \in \langle a \rangle$ .

Итак,  $ra = b' + sy$ ;  $b' \in B, s \in \mathbb{Z}$ . Отсюда  $sy \in B + \langle a \rangle = H$ . Если  $p \mid s$ , то  $sy \in B$ ,  $b' + sy = b'' \in B$  и  $0 \neq ra = b'' \implies B \cap \langle a \rangle \neq 0$  — противоречие. Значит,  $(s, p) = 1$ , причём  $sy \in H$  и  $py \in H$ , откуда  $y \in H$  — снова противоречие. Таким образом,  $A = H$ ,  $A = \langle a \rangle \oplus B$ , и утверждение доказано.

Теперь доказательство теоремы 8 очевидно. Мы выбираем в  $A$  элемент максимального порядка  $p^k$  и записываем  $A = \langle a \rangle \oplus B$ . Тот же процесс, применённый к  $B$ ,  $|B| < |A|$ , завершает доказательство.  $\square$

Важным дополнением к теореме 8 служит

**Теорема 9.** *Если конечная абелева  $p$ -группа  $A$  разложена двумя способами в прямую сумму циклических подгрупп:*

$$A_1 \oplus \dots \oplus A_r = A = B_1 \oplus \dots \oplus B_s,$$

то  $r = s$  и порядки  $|A_i|$  совпадают с порядками  $|B_j|$  при некотором упорядочении последних.

**Доказательство.** При  $|A| = p$  теорема, очевидно, верна. Используем индукцию по  $|A|$ . Удобно с самого начала упорядочить компоненты  $A_i$  и  $B_j$  так, чтобы их порядки не возрастили:

$$\begin{aligned} A_i &= \langle a_i \rangle, & |\langle a_i \rangle| &= p^{\mu_i}, \\ \mu_1 &\geq \mu_2 \geq \dots \geq \mu_q > \mu_{q+1} = \dots = \mu_r = 1; \end{aligned} \tag{3}$$

$$\begin{aligned} B_j &= \langle b_j \rangle, & |\langle b_j \rangle| &= p^{\nu_j}, \\ \nu_1 &\geq \nu_2 \geq \dots \geq \nu_t > \nu_{t+1} = \dots = \nu_s. \end{aligned} \tag{4}$$

Множество  $pA = \{px \mid x \in A\}$  является в  $A$  подгруппой, не зависящей от какого-либо разложения. С другой стороны, если

$$i_1a_1 + \dots + i_qa_q + \dots + i_ra_r = x = j_1b_1 + \dots + j_tb_t + \dots + j_sb_s,$$

то с учётом (3) и (4) имеем

$$i_1(pa_1) + \dots + i_q(pa_q) = x = j_1(pb_1) + \dots + j_t(pb_t).$$

Стало быть,

$$\langle \tilde{a}_1 \rangle + \dots + \langle \tilde{a}_q \rangle = pA = \langle \tilde{b}_1 \rangle + \dots + \langle \tilde{b}_t \rangle,$$

где  $\tilde{a}_i = pa_i$ ,  $\tilde{b}_j = pb_j$  — элементы порядков  $p^{\mu_i-1}$  и  $p^{\nu_j-1}$  соответственно. Так как  $|pA| < |A|$ , то по предположению индукции  $q = t$

и  $\mu_1 - 1 = \nu_1 - 1, \dots, \mu_q - 1 = \nu_q - 1$ , откуда  $\mu_1 = \nu_1, \dots, \mu_q = \nu_q$ . Замечая ещё, что

$$|A_{q+1} + \dots + A_r| = p^{r-q}, \quad |B_{t+1} + \dots + B_s| = p^{s-t}, \quad q = t,$$

мы получаем

$$p^{\mu_1 + \dots + \mu_q} p^{r-q} = A = p^{\mu_1 + \dots + \mu_q} p^{s-q}.$$

Значит,  $s = r$ , и все утверждения теоремы доказаны.  $\square$

**6. Основная теорема о конечных абелевых группах.** Для разнообразия перейдём к мультиплекативной записи, заменяя суммы на произведения, слагаемые на множители и т.д. Опираясь на теоремы 7-9, мы непосредственно приходим к следующему основному утверждению.

**Теорема 10.** *Всякая конечная абелева группа  $A$  является прямым произведением примарных циклических подгрупп. Любые два таких разложения имеют по одинаковому числу множителей каждого порядка.*

Заимствуя терминологию из теории векторных пространств, мы скажем, что элементы  $a_1, \dots, a_r$  порядков  $d_1, \dots, d_r$  составляют *базис* абелевой группы  $A$ , если каждый элемент  $x \in A$  единственным образом записывается в виде

$$x = a_1^{i_1} a_2^{i_2} \dots a_r^{i_r}, \quad 0 \leq i_k < d_k, \quad k = 1, \dots, r.$$

Разумеется, в таком случае

$$A = \langle a_1 \rangle \times \langle a_2 \rangle \times \dots \times \langle a_r \rangle, \quad |A| = d_1 d_2 \dots d_r, \quad (5)$$

и теорема 10 эквивалентна утверждению о существовании во всякой конечной абелевой группе  $A$  базиса, элементы которого примарны (т.е. их порядки  $d_i$  являются степенями простых  $p$ , делящих  $|A|$ ), причём система  $\{d_1, d_2, \dots, d_r\}$  не зависит от выбора базиса. По этой причине числа  $d_1, \dots, d_r$  называют *инвариантными* или *элементарными делителями* группы  $A$ . Иногда говорят ещё, что  $\{d_1, \dots, d_r\}$  — *тип* конечной абелевой группы  $A$ .

Выпишем все инварианты, расположив их в строки, которые отвечают различным простым делителям порядка  $|A|$ :

$$p_1^{m_{11}}, p_1^{m_{12}}, \dots, p_1^{m_{1k}}; \quad m_{11} \leq m_{12} \leq \dots \leq m_{1k};$$

$$p_2^{m_{21}}, p_2^{m_{22}}, \dots, p_2^{m_{2k}}; \quad m_{21} \leq m_{22} \leq \dots \leq m_{2k};$$

.....

$$p_s^{m_{s1}}, p_s^{m_{s2}}, \dots, p_s^{m_{sk}}; \quad m_{s1} \leq m_{s2} \leq \dots \leq m_{sk};$$

Можно считать, что все строки из инвариантов имеют одинаковую длину  $k$ , если дополнить некоторые из них единицами.

Целые числа

$$m_i = p_1^{m_{1i}} p_2^{m_{2i}} \dots p_s^{m_{si}}, \quad i = 1, 2, \dots, k,$$

называются *инвариантными факторами* (или *множителями*) абелевой группы  $A$ . По построению

$$|A| = m_1 m_2 \dots m_k, \quad m_{i-1} | m_i; \quad 1 < i \leq k. \quad (6)$$

Достаточно вернуться к формулировке следствия 2 из теоремы 2, чтобы убедиться: инвариантные факторы нам уже встречались. От разложения (5), переписанного в виде

$$A = (\langle a_{11} \rangle \times \dots \times \langle a_{s1} \rangle) \times \dots \times (\langle a_{1k} \rangle \times \dots \times \langle a_{sk} \rangle),$$

мы перейдём теперь к разложению

$$A = \langle u_1 \rangle \times \langle u_2 \rangle \times \dots \times \langle u_k \rangle \quad (6)$$

с прямыми циклическими множителями порядков  $m_1, m_2, \dots, m_k$ . Для этого достаточно положить

$$u_i = a_{1i} a_{2i} \dots a_{si}, \quad 1 < i \leq k,$$

и сослаться на предложение 2 или на импликацию (1).

Для примарной группы  $A$  прямые разложения (5) и (6), очевидно, совпадают, но в общем случае разложение (6) более экономно по сравнению с (5) ( $k \leq r \leq sk$ ), причём в (6) выделен элемент  $u_k$  наивысшего порядка  $m := m_k$ ; порядки всех других элементов группы  $A$  делят  $m$ . Целое число  $m$  называют ещё *показателем* (или *экспонентой*) группы  $A$ . Абелева группа  $A$  является циклической тогда и только тогда, когда её показатель совпадает с порядком  $|A|$ .

Последняя фраза играет ключевую роль в доказательстве следующего полезного утверждения о полях.

**Теорема 11.** *Пусть  $F$  — произвольное поле и  $A$  — конечная подгруппа мультипликативной группы  $F^*$ . Тогда  $A$  циклическая.*

**Доказательство.** Если бы группа  $A$  не была циклической, то в соответствии с вышеизложенным было бы  $m < |A|$ , где  $m$  — её показатель:  $a^m = 1 \forall a \in A$ . В таком случае многочлен  $X^m - 1$  имел бы в поле  $F$  более  $m$  корней, а это невозможно. Значит, группа  $A$  циклическая.  $\square$

Остается добавить, что вопрос о существовании абелевой группы  $A$  с заданными инвариантными факторами  $m_1, m_2, \dots, m_k$  не возникает: как и ранее, достаточно рассмотреть (в аддитивной записи) прямую сумму циклических групп  $Z_{m_1}, \dots, Z_{m_k}$ . Число попарно неизоморфных абелевых групп данного порядка  $N$  может быть оценено в довольно явной форме. Так, *число неизоморфных абелевых групп порядка  $N = p^n$  ( $p$  простое) равно числу  $p(n)$  упорядоченных разбиений*

$$n = n_1 + n_2 + \dots + n_l, \quad n_1 \geq n_2 \geq \dots \geq n_l, \quad 1 \leq l \leq n.$$

Целочисленная функция  $p(n)$  встречалась нам при описании классов сопряжённых элементов в симметрической группе  $S_n$  (см. упр. 4

из § 3 гл.1). Абелева группа порядка  $p^n$  и показателя  $p$  (т.е. с инвариантами  $p, \dots, p$ ) обычно называется *элементарной абелевой группой*. Вновь отдав предпочтение аддитивной записи, мы замечаем, что абелева группа  $A$  с  $pA = 0$  ( $p$  — простое число) является векторным пространством над конечным полем  $\mathbb{F}_p$  из  $p$  элементов. Действительно, если отождествить элементы из  $\mathbb{F}_p$  с классами вычетов  $\bar{k}$  по модулю  $p$  ( $\mathbb{F}_p = Z_p$ ) и положить  $\bar{k}a := ka$ ,  $a \in A$ , то мы придём к заданию действия  $\mathbb{F}_p$  на  $A$ , превращающее  $A$  в векторное пространство над  $\mathbb{F}_p$ . Это действие определено правильно, потому что из  $\bar{k} = \bar{k}'$  следует  $(k - k')a = l(pa) = 0$ . Разложению  $A$  в прямую сумму циклических подпространств соответствует разложение векторного пространства в прямую сумму одномерных подпространств [ВА II, гл.1, теорема о базисе]. Итак,

$$A \cong Z_p^n = Z_p \oplus \dots \oplus Z_p.$$

Насколько велик произвол в выборе одномерных базисных подпространств даже при  $n = 2$ , видно из примера в гл. 1:  $Z_p^2$  допускает  $p(p + 1)$  различных разложений.

Пример 4. В качестве примера перечислим все абелевы группы порядков 16 и 36:

$$|A| = 16 = 2^4, \quad p(4) = 5,$$

$$Z_{16}, \quad Z_8 \oplus Z_2, \quad Z_4 \oplus Z_4, \quad Z_4 \oplus Z_2 \oplus Z_2, \quad Z_2^4 = Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2,$$

$ A  = 36 = 2^2 \cdot 3^2$	Элементарные делители	Инвариантные факторы
$Z_4 \oplus Z_9 \cong Z_{36}$	4, 9	36
$Z_2 \oplus Z_2 \oplus Z_9 \cong Z_2 \oplus Z_{18}$	2, 2, 9	18, 2
$Z_4 \oplus Z_3 \oplus Z_3 \cong Z_3 \oplus Z_{12}$	4, 3, 3	12, 3
$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3 \cong Z_6 \oplus Z_6$	2, 2, 3, 3	6, 6

Пример 5. Запишем группу  $Z_{72} \oplus Z_{84}$  в терминах инвариантных факторов. Сначала каждое из циклических слагаемых мы выразим через циклические примарные компоненты:

$$Z_{72} = Z_8 \oplus Z_9, \quad Z_{84} = Z_4 \oplus Z_3 \oplus Z_7.$$

Далее, соберём все примарные компоненты, отвечающие заданному  $p$ :

$$Z_{72} \oplus Z_{84} = (Z_4 \oplus Z_8) \oplus (Z_3 \oplus Z_9) \oplus Z_7$$

(прямая сумма силовских  $p$ -подгрупп). Теперь осталось выделить по одному циклическому слагаемому минимального порядка в каждой примарной компоненте и повторить этот процесс с оставшимися слагаемыми:

$$Z_{72} \oplus Z_{84} = (Z_4 \oplus Z_3) \oplus (Z_8 \oplus Z_9 \oplus Z_7) = Z_{12} \oplus Z_{504}.$$

Если проделать то же самое с группой  $Z_{36} \oplus Z_{168}$ , то получится аналогичный результат. Значит,

$$Z_{72} \oplus Z_{84} = Z_{36} \oplus Z_{168}$$

(строго говоря, всюду следовало бы ставить  $\cong$  вместо знака равенства). В частности, отметим, что показатели обеих групп равны 504.

### УПРАЖНЕНИЯ

1. Показать, что в конечной абелевой группе  $A$  для любого  $d \mid |A|$  существует по крайней мере одна подгруппа порядка  $d$  (обращение теоремы Лагранжа).
2. Показать, что при надлежащем упорядочении инварианты любой подгруппы являются делителями инвариантов абелевой группы.
3. Если  $A \oplus A \cong B \oplus B$ , где  $A$  и  $B$  — конечные абелевые группы, то  $A \cong B$ .
4. Если  $A, B, C$  — конечные абелевые группы и  $A \oplus C \cong B \oplus C$ , то  $A \cong B$ .
5. Всякая конечная абелева группа порядка  $n$ , не делящегося на квадрат целого числа  $> 1$ , является циклической.
6. Перечислить все неизоморфные абелевые группы порядка 72.
7. Изоморфны ли группы  $Z_{12} \oplus Z_{72}$  и  $Z_{18} \oplus Z_{48}$ ?
8. Сформулировать и доказать теорему о конечно порождённых абелевых группах на языке целочисленных матриц (матриц с коэффициентами в  $\mathbb{Z}$ ). Использовать надлежащим образом элементарные преобразования над такими матрицами.
9. Доказать, что индекс подгруппы  $A \subseteq F_n^{ab}$  свободной абелевой группы  $F_n^{ab}$  ранга  $n$  конечен тогда и только тогда, когда  $\text{rank } A = n$ .

## § 4. Линейные группы Ли

**1. Определения и примеры.** Формально говоря, группой Ли  $G$  называется *дифференцируемое* ( $C^2$  или даже *класса*  $C^\infty$ , гладкое) многообразие, наделённое структурой группы с гладкими отображениями — умножением  $(x, y) \mapsto xy$  и взятием обратного элемента  $x \mapsto x^{-1}$ .

От *гомоморфизма*  $\Phi: G \rightarrow H$  группы Ли  $G$  в группу Ли  $H$  также требуется гладкость отображения одного многообразия в другое. То же самое относится к более частным понятиям *изоморфизма* групп Ли и *автоморфизма* группы Ли. Чаще всего имеют дело с *вещественными* или *комплексными* многообразиями и соответственно с *вещественными* или *комплексными* группами Ли.

Задание структуры многообразия предполагает, в частности, наличие топологии, поэтому группы Ли являются *топологическими*. Это означает, что произведение  $gh$  и взятие обратного  $g^{-1}$  являются в данной топологии непрерывными операциями. Считаются известными понятия связности, локальной связности, компактности топологического пространства. В частности, группа называется *компактной*, если для соответствующего топологического пространства справедлива теорема Бореля–Лебега.

Строгое определение группы Ли, объединяющее понятия обычной группы, топологического пространства и дифференцируемого

многообразия, довольно сложно. К тому же определение *подгруппы Ли*  $H \subset G$  предполагает, что  $H$  — *подмногообразие* (новое понятие), задаваемое в окрестности нейтрального элемента (единицы  $e \in H$ ) локальными координатами  $x_1, \dots, x_n$  на  $G$ , которые удовлетворяют системе уравнений

$$f_i(x_1, \dots, x_n) = 0, \quad 1 \leq i \leq m. \quad (1)$$

Считается, что

$$\operatorname{rank} \left\| \frac{\partial f_i}{\partial x_j} \right\|_e = m.$$

Это условие на систему (1), перенесённое левыми сдвигами в любую точку  $h \in H$ , снабжает  $H$  структурой  $(n-m)$ -мерного многообразия. Заметим ещё, что группу Ли  $G$  часто рассматривают локально, в надлежащей окрестности единицы  $e \in G$ . Входить в детали было бы рискованно. Так как нас интересуют классические линейные группы, то с самого начала можно считать их группами Ли, закрыв глаза на многие общие определения.

Пример 1.  $(\mathbb{R}^n, +)$  — группа Ли.

Пример 2. Пусть  $V$  — конечномерное векторное пространство над  $\mathfrak{K}$  ( $\mathfrak{K} = \mathbb{R}$  или  $\mathfrak{K} = \mathbb{C}$ ). Известная нам группа  $\operatorname{Aut} V$  автоморфизмов пространства  $V$  суть открытое подмножество в  $\operatorname{Hom}(V, V)$ , заданное условием  $\det \neq 0$ . Стало быть,  $\operatorname{Aut} V$  — гладкое многообразие. Естественная композиция автоморфизмов — гладкое отображение: если  $A = (a_{ij})$ ,  $B = (b_{jk})$ , то  $AB = C = (c_{ik})$ , где  $c_{ik} = \sum_j a_{ij} b_{jk}$ . Аналогично, отображение  $x \mapsto x^{-1}$  гладко: достаточно вспомнить о формулах Крамера. Итак,  $\operatorname{Aut} V$  — группа Ли размерности  $n^2$ . Её матричную реализацию над  $\mathfrak{K}$  мы условились обозначать  $\operatorname{GL}(n, \mathfrak{K})$  или  $\operatorname{GL}_n(\mathfrak{K})$ .

Пример 3. Для группы  $\operatorname{SL}(n, \mathfrak{K})$  система (1) сводится к одному уравнению

$$\det X = 1, \quad X = (x_{ij}) \in \operatorname{GL}(n, \mathfrak{K}),$$

с явно выполненным условием  $\partial(\det X)/\partial x_{11}|_{X=E} = 1$ . Поэтому  $\operatorname{SL}(n, \mathfrak{K})$  является  $(n^2 - 1)$ -мерной группой Ли.

Пример 4. Из [ВА II, гл. 3] известно, что ортогональная группа  $\operatorname{O}(n) \subset \operatorname{GL}(n, \mathbb{R})$  задаётся билинейными соотношениями

$$f_{ij}(X) = \sum_k x_{ik} x_{jk} = \delta_{ij}$$

в количестве  $m = n(n+1)/2$  штук. Легко проверяется, что минор порядка  $m$  матрицы  $\|\partial f_{ij}/\partial x_{st}\|$ , отвечающий переменным  $x_{st}$ ,  $s \leq t$ , в точке  $E$  отличен от нуля. Это значит, что  $\operatorname{O}(n)$  — группа Ли размерности  $n^2 - m = n(n-1)/2$ .

Такую же размерность имеет подгруппа  $\operatorname{SO}(n)$ , в окрестности единицы совпадающая с  $\operatorname{O}(n)$ . Точнее, как топологическое пространство  $\operatorname{O}(n)$  распадается на две связные компоненты: одна содержит  $E$ , другая  $-E$ . Очевидно,  $\det X = 1$  для всякой матрицы  $X \in \operatorname{O}(n)$ , близкой к  $X$ .

Пример 5. Определение унитарной группы  $\operatorname{U}(n) \subset \operatorname{GL}(n, \mathbb{C})$  в [ВА II, гл. 3] аналогично определению группы  $\operatorname{O}(n)$ , если на  $\operatorname{GL}(n, \mathbb{C})$  смотреть как на вещественную группу, зависящую от  $2n^2$  параметров. Разделение вещественных и мнимых частей  $n(n+1)/2$  полуторалинейных соотношений приведёт к  $2n(n-1)/2 + n = n^2$  гладким функциям. Ранг соответствующей матрицы в точке  $X = E$  также равен  $n^2$ . Поэтому  $\operatorname{U}(n)$  — группа Ли размерности  $2n^2 - n^2 = n^2$ .

Так как  $\det X = e^{i\varphi}$ ,  $X \in \mathrm{U}(n)$ ,  $\varphi \in \mathbb{R}$ , то  $\mathrm{SU}(n)$  — группа Ли размерности  $n^2 - 1$ .

**2. Кривые в матричных группах.** В топологических линейных пространствах имеет смысл говорить о кривых, касательных векторах и т.п. вещах. Так, в анализе и в геометрии под *кривой* в конечномерном вещественном векторном пространстве  $V$  понимают непрерывное отображение (функцию)  $\Gamma: (\alpha, \beta) \rightarrow V$ , где  $(\alpha, \beta)$  — интервал в  $\mathbb{R}$ . Скажем, окружность  $S^1$  единичного радиуса с центром в начале прямоугольной системы координат суть кривая  $\varphi \mapsto (\cos \varphi, \sin \varphi)$ ,  $\varphi \in [0, 2\pi]$ . Разумеется,  $V$  чаще всего снабжается структурой аффинного или евклидова пространства. Пусть  $V = \langle \mathbf{e}_1, \dots, \mathbf{e}_n \rangle$ . Зададим кривую в параметрической форме  $\Gamma_t = (\gamma_1(t), \dots, \gamma_n(t))$ , где  $\gamma_i(t)$  — вещественнозначная функция при любом  $i = 1, \dots, n$ . Кривая  $\Gamma$  *дифференцируема* в точке  $t \in (\alpha, \beta)$ , если дифференцируемы все  $\gamma_i(t)$ , т.е. существуют производные  $\gamma'_1(t), \dots, \gamma'_n(t)$  и

$$\Gamma'_t := \frac{d\Gamma_t}{dt} = (\gamma'_1(t), \dots, \gamma'_n(t))$$

— однозначно определённый вектор в  $V$ , называемый *касательным вектором* к  $\Gamma$  в точке  $\Gamma_t$  или *вектором скорости* в момент времени  $t$ . В дальнейшем будем для простоты говорить о гладкой кривой  $\Gamma_t$ , отождествляя функцию с её значением.

Пусть теперь  $V = M_n(\mathbb{R})$  или  $M_n(\mathbb{C})$ , рассматриваемые как векторные пространства размерностей  $n^2$  и  $2n^2$  соответственно. Будем считать, что кривая  $\Gamma_t$  на пространстве  $M_n(\mathfrak{K})$  ( $\mathfrak{K} = \mathbb{R}$  или  $\mathfrak{K} = \mathbb{C}$ ) на самом деле целиком лежит в матричной группе  $G \subset M_n(\mathfrak{K})$ , т.е.  $\Gamma_t \in G \quad \forall t \in (\alpha, \beta)$ . Тогда естественно говорить о *кривой в группе* или *на группе*  $G$ . При любом  $t = t_0$  надо чётко представлять себе, что  $A_{t_0}$  есть точка кривой в  $n^2$ -мерном пространстве, реализованная в виде матрицы. Если  $A_t = (a_{ik}(t))$ ,  $B_t = (b_{kj}(t)): (\alpha, \beta) \rightarrow G$  — две параметрические кривые в группе  $G$ , то можно определить их произведение  $C_t = A_t B_t$ , полагая

$$C_t = (c_{ij}(t)), \quad c_{ij}(t) := \sum_{k=1}^n a_{ik}(t) b_{kj}(t), \quad t \in (\alpha, \beta). \quad (2)$$

Наша ближайшая задача — рассмотреть в классических матричных группах множество всех дифференцируемых кривых, проходящих через единичный элемент  $E$ , и множество всех касательных векторов к кривым в этой избранной точке.  $M_n(\mathbb{C})$  трактуется как вещественное пространство размерности  $2n^2$ .

**Теорема 1.** Пусть  $G \subset \mathrm{GL}(n, \mathfrak{K})$  — матричная группа. Справедливы следующие утверждения.

i) Если  $A_t, B_t: (\alpha, \beta) \rightarrow G$  — две дифференцируемые кривые в  $G$ ,

то их произведение  $C_t = A_t B_t$  также дифференцируемо и

$$\frac{dC_t}{dt} = (A_t B_t)' = A'_t B_t + A_t B'_t.$$

ii) Пусть  $T = L(G)$  — множество всех касательных векторов  $A'_0$  к кривым  $A_t$  в  $G$  (в малой окрестности параметра  $t = 0$ ), для которых  $A_0 = E$ . Тогда  $L(G)$  — векторное подпространство в  $M_n(\mathbb{K})$ .

**Доказательство.** Утверждение i) получается прямым дифференцированием определяющего соотношения (2).

ii) Пусть  $A'_0, B'_0 \in T$ . Тогда  $(AB)_0 = A_0 B_0 = EE = E$  и согласно i) в  $T$  содержится вектор

$$(AB)'_0 = A'_0 B_0 + A_0 B'_0 = A'_0 E + E B'_0 = A'_0 + B'_0.$$

Следовательно,  $T$  — аддитивная группа.

Если теперь  $\lambda$  — произвольный скаляр и  $A'_0 \in T$ , то рассмотрим кривую  $B_t = A_{\lambda t}$  в окрестности  $t = 0$ . Очевидно, что  $B_0 = A_0 = E$ , причём  $B_t$  дифференцируема и  $B'_0 = \lambda A'_0$ . Так как по условию  $B'_0 \in T$ , то и  $\lambda A'_0 \in T$ .  $\square$

**Определение.** Векторное пространство  $T = L(G)$  называется *касательным пространством к группе  $G$  в точке  $E$* .

**Пример 6.** Пусть  $G = \mathrm{GL}(n, \mathbb{R})$ . Так как  $\det : G \rightarrow \mathbb{R}$  — непрерывная функция и  $\det E = 1$ , то можно указать столь малое  $\varepsilon > 0$  и шар радиуса  $\varepsilon$  с центром в  $E$ , что для каждой матрицы  $A$  из этого шара будет выполняться неравенство  $\det A \neq 0$ , т.е.  $A \in G$ . Теперь для любой матрицы  $B \in M_n(\mathbb{R})$  (т.е. для любого вектора из вещественного векторного пространства размерности  $n^2$ ) определим кривую  $B_t$  в  $M_n(\mathbb{R})$  равенством

$$B_t = tB + E.$$

Мы видим, что  $B_0 = E$ ,  $B'_0 = B$ , а при малых  $t$  матрицы  $B_t$  лежат в  $G$ . Стало быть, касательное пространство  $L(\mathrm{GL}(n, \mathbb{R}))$  совпадает с  $M_n(\mathbb{R})$  и имеет размерность  $n^2$ . Аналогично показывается, что касательное пространство  $L(\mathrm{GL}(n, \mathbb{C}))$  имеет над  $\mathbb{R}$  размерность  $2n^2$ .

**Пример 7.** Имея дело с группой  $\mathrm{SL}(n, \mathbb{R})$ , мы должны выбирать в  $\varepsilon$ -шаре с центром в  $E$  матрицы  $A$  с  $\det A = 1$ , а для любой матрицы  $B \in M_n(\mathbb{R})$  с нулевым следом и малого параметра  $t$  определять кривую  $B_t$ , используя экспоненту матрицы [BA II, гл. 7, § 1] :

$$B_t = \exp(tB).$$

Тогда  $B_0 = E$ ,  $B'_0 = B \exp(tB)$ ,  $B'_0 = B$ ,  $\det B_t = \exp(\mathrm{tr}(tB)) = 1$ . Это и означает, что касательное пространство  $L(\mathrm{SL}(n, \mathbb{R}))$  имеет размерность  $n^2 - 1$ .

**Пример 8.** Из примера 4 видно, что касательные пространства к многообразиям (группам Ли)  $O(n)$  и  $\mathrm{SO}(n)$  в точке  $E$  совпадают. Пусть теперь  $B_t$  — произвольная кривая в  $\mathrm{SO}(n)$  с касательным вектором  $B'_0$  в  $E$ . Так как по определению  $B_s {}^t B_s = E$ , то дифференцирование приводит к соотношению  $B_0 + {}^t B_0 = 0$ , показывающему, что любой касательный вектор кососимметричен.

С другой стороны, если  $A$  — любая кососимметричная матрица, то кривая  $A_s = \exp(sA)$ , выходящая из  $E$  ( $A_0 = E$ ), имеет в  $E$  касательный вектор  $A'_0 = A$ . Каждая точка кривой  $A_s$  — ортогональная матрица с определителем 1 [BA II,

гл. 7]. Таким образом,  $L(\mathrm{SO}(n)) = \mathfrak{so}(n)$  — пространство размерности  $n(n-1)/2$ , состоящее из всех кососимметричных матриц.

**Пример 9.** В случае унитарной группы  $\mathrm{U}(n)$ , заменяя  $\mathfrak{so}(n)$  на пространство  $\mathfrak{su}(n)$  косоэрмитовых матриц (над  $\mathbb{R}$ ) и обращаясь к соображениям, использованным в примере 8, мы убеждаемся в том, что  $L(\mathrm{U}(n))$  имеет размерность  $n^2$ .

Размерность линейной группы Ли определялась ранее по числу независимых параметров, задающих базисное дифференцируемое многообразие. Теперь мы видим, что справедлива

**Теорема 2.** *Пусть  $G$  — одна из классических линейных групп Ли  $\mathrm{GL}(n, \mathfrak{K})$ ,  $\mathrm{SL}(n, \mathfrak{K})$ ,  $\mathrm{O}(n)$ ,  $\mathrm{SO}(n)$ ,  $\mathrm{U}(n)$ ,  $\mathrm{SU}(n)$ ;  $\mathfrak{K} = \mathbb{R}$  или  $\mathfrak{K} = \mathbb{C}$ ,  $L(G)$  — её касательное пространство в  $E$ .*

*Тогда  $\dim G = \dim L(G)$ .*

**Доказательство** получается сопоставлением примеров 2–5, 6–9.  $\square$

К указанным в теореме группам следовало бы добавить симплексическую группу, но ради простоты изложения мы условились её опускать.

**3. Дифференциал гомоморфизма.** Всякому гомоморфизму  $\Phi : G \rightarrow H$  матричных групп  $G$ ,  $H$  и всякой гладкой кривой  $A_t$  в группе  $G$  отвечает кривая  $(\Phi \circ \Gamma)_t = \Phi(\Gamma_t)$  в группе  $H$ . Гомоморфизм  $\Phi$  естественно называть *гладким*, если все кривые  $\Phi \circ \Gamma_t$  гладкие.

**Определение.** Гладкому гомоморфизму  $\Phi : G \rightarrow H$  матричных групп Ли и касательному вектору  $\Gamma'_0$  к  $G$  в точке  $E$  можно поставить в соответствие касательный вектор  $d\Phi(\Gamma'_0)$  к  $H$  в  $E$ , полагая

$$d\Phi(\Gamma'_0) = (\Phi \circ \Gamma)'_0. \quad (3)$$

Отображение  $d\Phi : L(G) \rightarrow L(H)$ , заданное равенством (3), называется *дифференциалом* или *касательным отображением* гомоморфизма  $\Phi$ .

**Теорема 3.** *В матричных группах справедливы следующие утверждения.*

i) *Дифференциал гомоморфизма групп является линейным отображением касательных пространств.*

ii) *Если  $\Phi : G \rightarrow H$ ,  $\Psi : H \rightarrow K$  — гладкие гомоморфизмы, то*

$$d(\Psi \Phi) = d\Psi \cdot d\Phi.$$

iii) *Гладкому изоморфизму  $\Phi : G \rightarrow H$  отвечает линейный изоморфизм  $d\Phi : L(G) \rightarrow L(H)$ , причём  $\dim G = \dim H$ .*

**Доказательство.** Пусть  $A'_0, B'_0 \in L(G)$ ,  $\mu, \nu \in \mathbb{R}$ . Тогда

$$\begin{aligned} d\Phi(\mu A'_0 + \nu B'_0) &= (\Phi \circ (\mu A + \nu B))'_0 = \\ &= (\mu(\Phi \circ A) + \nu(\Phi \circ B))'_0 = \mu(\Phi \circ A)'_0 + \nu(\Phi \circ B)'_0 = \\ &= \mu d\Phi(A'_0) + \nu d\Phi(B'_0). \end{aligned}$$

Это доказывает утверждение i).

Что касается ii), то заметим сначала, что композиция  $\Psi\Phi$  является гладким гомоморфизмом, поэтому выражение  $d(\Psi\Phi)$  имеет смысл. Далее,

$$d(\Psi\Phi)(A'_0) = ((\Psi\Phi) \circ A)'_0 = d\Psi(\Phi \circ A)'_0 = d\Psi \cdot d\Phi(A'_0).$$

Наконец, изоморфность  $d\Phi$  вытекает из следующих соображений. Так как  $\Phi^{-1}\Phi$  — тождественное отображение, то в соответствии с ii) имеем тождественное отображение  $d\Phi^{-1} \cdot d\Phi : L(G) \rightarrow L(G)$ , и поэтому  $d\Phi$  — инъективное отображение, а  $d\Phi^{-1}$  — сюръективное. Но и  $\Phi\Phi^{-1}$  — тождественное отображение, поэтому  $d\Phi^{-1}$  инъективно, а  $d\Phi$  сюръективно. Это даёт всё, что нужно.  $\square$

Отсылая к [34] за деталями, приведём без доказательства следующую содержательную теорему о группах Ли.

**Теорема 4.** *Гомоморфизм связной группы Ли в произвольную группу Ли однозначно определяется своим дифференциалом.*

**4. Алгебра Ли группы Ли.** Что такое алгебра Ли  $\mathcal{L}$ , нам известно из [ВА II]. Так как произведение элементов  $x, y \in \mathcal{L}$  принято обозначать  $[x, y]$ , то для коммутатора элементов  $g, h \in G$  в группе Ли используем обычное обозначение  $(g, h) = ghg^{-1}h^{-1}$ . Напомним, что коммутирование в алгебре Ли линейно по каждому аргументу, кососимметрично и удовлетворяет тождеству Якоби

$$[[x, y], z] + [[y, z], x] + [[z, x], y] = 0. \quad (4)$$

Из примеров 6–9 и из [ВА II, гл. 7] видно, что касательные пространства классических линейных групп Ли наделены структурой алгебры Ли. Однако поучительно посмотреть на связь между операциями умножения в группе и коммутированием в соответствующей алгебре Ли, причём в более общей ситуации любых связных групп Ли.

Итак, пусть  $G$  — связная группа Ли с нейтральным элементом  $e$ ,  $L(G)$  — её касательное пространство в  $e$ . Коммутатор  $[g'_0, h'_0]$  касательных векторов  $g'_0, h'_0 \in L(G)$  к кривым  $g_t, h_s$ ,  $0 \leq s, t \leq 1$ , на группе  $G$ , выходящим из  $e$ :  $g_0 = e = h_0$ , определим соотношением

$$[g'_0, h'_0] := \frac{\partial^2}{\partial t \partial s} (g_t, h_s) \Big|_{t=s=0}. \quad (5)$$

Положив

$$f(t, s) = (g_t, h_s),$$

мы видим, что  $f(t, 0) = e$  и

$$q'_t = \frac{\partial}{\partial s} f(t, s) \Big|_{s=0} \in L(G)$$

суть касательный вектор к кривой  $q$ :  $s \rightarrow f(t, s)$ , а

$$\frac{\partial^2}{\partial t \partial s} f(t, s) \Big|_{t=s=0}$$

— касательный вектор к кривой  $q'_t$  в пространстве  $L(G)$ . Коммутатор  $(\Gamma_t, \Delta_s)$  элементов  $n$ -мерной группы  $G$  с координатами  $(x_1, \dots, x_n)$  и  $(y_1, \dots, y_n)$  выражается через дифференцируемые функции  $f_i(x_1, \dots, x_n, y_1, \dots, y_n)$ ,  $1 \leq i \leq n$ . Вид функций  $f_i$ , целиком определённый группой, не зависит от конкретных элементов, поэтому для коммутатора  $[g'_0, h'_0]$  получаем следующее явное выражение:

$$[g'_0, h'_0]_i = \sum_{j,k} \frac{\partial^2 f_i}{\partial x_j \partial y_k} \Big|_{(e,e)} (g'_0)_j (h'_0)_k. \quad (6)$$

Из (6) видно, что частная производная в (5) не зависит от выбора координат, а коммутатор линеен по каждому аргументу.

Если воспользоваться легко проверяемым соотношением  $(a, b) = (b, a)^{-1}$ , то можно убедиться, что коммутатор (5) кососимметричен. Тождество (4) доказать несколько труднее, но если перейти к линейным группам Ли, не обязательно классическим, то ситуация упрощается. Именно, пусть  $L(G) \subset M_n(\mathbb{K})$ ;  $\mathbb{K} = \mathbb{R}$  или  $\mathbb{K} = \mathbb{C}$ . Для любых двух матриц  $X, Y \in L(G)$ , являющихся касательными векторами к кривым  $\exp(tX), \exp(sY) \in G$ , прямые вычисления со степенными рядами показывают, что с точностью до членов степени  $\geq 3$

$$\exp(tX) \exp(sY) = E + tX + sY + tsXY + \frac{t^2}{2} X^2 + \frac{s^2}{2} Y^2 + \dots \in G,$$

и, значит,

$$\begin{aligned} (\exp(tX), \exp(sY)) &= \\ &= (E + tX + sY + tsXY + \frac{t^2}{2} X^2 + \frac{s^2}{2} Y^2 + \dots) \times \\ &\quad \times (E - tX - sY + tsXY + \frac{t^2}{2} X^2 + \frac{s^2}{2} Y^2 + \dots) = \\ &= E + ts(XY - YX) + t^2 sU(X, Y, t, s) + ts^2 V(X, Y, t, s), \end{aligned}$$

где  $\deg_{X,Y} U(X, Y, t, s) \geq 3$ ,  $\deg_{X,Y} V(X, Y, t, s) \geq 3$ . Теперь по формуле (5) находим

$$\begin{aligned} [X, Y] &= \\ &= \frac{\partial^2}{\partial t \partial s} (E + ts(XY - YX) + t^2 sU(X, Y, t, s) + ts^2 V(X, Y, t, s)) \Big|_{t=s=0} = \\ &= XY - YX, \end{aligned}$$

т.е. для коммутатора  $[X, Y]$ , определённого абстрактным образом, получается естественное выражение  $[X, Y] = XY - YX$ , которым мы пользовались ранее. Тождество Якоби при таком коммутировании очевидным образом выполняется. Тем самым получена

**Теорема 5.** Касательная алгебра всякой линейной группы Ли снабжена структурой алгебры Ли с операцией коммутирования  $[X, Y] = XY - YX$ .

**5. Логарифм.** Экспоненциальному отображению  $\exp: L(G) \rightarrow G$  в случае матричных групп отвечает антипод — логарифмическое отображение

$$\log X = (X - E) - \frac{(X - E)^2}{2} + \frac{(X - E)^3}{3} - \frac{(X - E)^4}{4} + \dots, \quad (7)$$

определенное для любой вещественной  $n \times n$ -матрицы  $X$ , достаточно близкой к  $E$ . Чтобы убедиться в этом, положим  $Y := X - E = (y_{ij})$ , считая  $|y_{ij}| < \varepsilon$ . Простая индукция по  $k$  приводит к оценке  $|(Y^k)_{ij}| \leqslant n^{k-1}\varepsilon^k$ , и поэтому для отношения модулей двух соседних членов в (7) находим

$$\frac{|(Y^{k+1})_{ij}|}{|(Y^k)_{ij}|} \frac{k}{k+1} \frac{n^k \varepsilon^{k+1}}{n^{k-1} \varepsilon^k} = \frac{k}{k+1} n\varepsilon.$$

Таким образом, ряд (7) сходится для любой матрицы  $X$  с  $|(X - E)_{ij}| < 1/n$ .

**Теорема 6.** Пусть  $U_E$  — окрестность  $E$  в  $M_n(\mathbb{R})$ , где определено отображение  $\log$ , а  $U_0$  — окрестность нуля, в которой  $\exp(U_0) \subset U_E$ . Тогда:

- i)  $\exp \log X = X$ ,  $X \in U_E$ ;  $\log \exp Y = Y$ ,  $Y \in U_0$ .
- ii) если  $A, B$  коммутируют и близки к  $E$ , то

$$\log(AB) = \log A + \log B.$$

**Доказательство i)** ничем не отличается от числового случая. Что касается ii), то  $\exp(\log(AB)) = AB = (\exp(\log A))(\exp(\log B)) = \exp(\log A + \log B)$ . Осталось воспользоваться биективностью  $\exp$  вблизи 0.  $\square$

**Отдельные замечания.** 1) Назовём однопараметрической подгруппой линейной группы Ли  $G$  гладкий гомоморфизм  $\sigma: \mathbb{R} \rightarrow G$ . Так как  $\sigma(t) = (\sigma(t/n))^n$ , то  $\sigma$  определяется своими значениями вблизи 0  $\in \mathbb{R}$ . Пример в [ВА II, гл. 7], однопараметрической группы  $\sigma: t \mapsto \exp(tA)$ , определённой квадратной матрицей  $A$ , является в некотором смысле общим, поскольку локально  $G$  порождается кривыми  $\exp(tA)$ ,  $A \in L(G)$ .

2) Под линейным представлением группы Ли  $G$  понимается дифференцируемый гомоморфизм  $\Phi: G \rightarrow \mathrm{GL}(V)$ , где  $V$  — векторное пространство над  $\mathbb{R}$  или  $\mathbb{C}$ . Коэффициенты матриц  $\Phi_g$  являются по определению дифференцируемыми функциями от  $g \in G$ . Наличие вещественной или комплексной структуры в  $G$  и  $V$  проявляется в нескольких вариантах (см., например, [1]). Линейные представления компактных групп Ли фактически определяются представлениями

соответствующих алгебр Ли. Хорошой иллюстрацией служит описание неприводимых представлений группы  $SU(2)$  в гл. 3 и её алгебры Ли  $\mathfrak{su}(2)$  в гл. 4.

### УПРАЖНЕНИЯ

**1.** Показать, что для каждой однопараметрической подгруппы  $\sigma$  группы  $GL(n, \mathbb{R})$  существует матрица  $A \in M_n(\mathbb{R})$ , такая, что  $\sigma(t) = \exp(tA)$ .

**2.** Автоморфизмы алгебры Ли  $L(G)$  данной линейной группы Ли  $G$  в свою очередь образуют линейную группу Ли  $\text{Aut}(L(G))$ . Если  $\Gamma_t$  — некоторая кривая в  $\text{Aut}(L(G))$ , то  $\Gamma_t[\mathbf{a}, \mathbf{b}] = [\Gamma_t\mathbf{a}, \Gamma_t\mathbf{b}]$ . Дифференцирование при  $t = 0$  приводит в обозначении  $\mathcal{D} = (\frac{d}{dt}\Gamma_t)_{t=0}$  (считаем  $\Gamma_0 = E$ ) к соотношению

$$\mathcal{D}[\mathbf{a}, \mathbf{b}] = [\mathcal{D}\mathbf{a}, \mathbf{b}] + [\mathbf{a}, \mathcal{D}\mathbf{b}],$$

которое позволяет называть  $\mathcal{D}$  *дифференцированием* алгебры Ли  $L(G)$ . С этим понятием мы уже встречались в [ВА II].

Доказать, что если  $\mathcal{D}$  — дифференцирование алгебры Ли  $L(G)$ , то  $\exp \mathcal{D}$  — её автоморфизм.

## Глава 3

# ЭЛЕМЕНТЫ ТЕОРИИ ПРЕДСТАВЛЕНИЙ

---

Точным определениям теории линейных представлений групп мы предшествуют две близкие по духу задачи.

**Задача 1.** В  $(m+1)$ -мерном пространстве  $V_m$  вещественных однородных многочленов

$$f(x, y) = a_0x^m + a_1x^{m-1}y + \dots + a_{m-1}xy^{m-1} + a_my^m$$

(или, скорее, полиномиальных функций  $(x, y) \mapsto f(x, y)$ ) степени  $m$  выделяется множество решений двумерного *уравнения Лапласа*

$$\frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2} = 0 \quad (*)$$

в частных производных (см. [ВА I, упр. 9 из § 1 гл. 6]). Оператор Лапласа  $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$  линеен:

$$\Delta(\alpha f + \beta g) = \alpha \Delta f + \beta \Delta g \quad \forall \alpha, \beta \in \mathbb{R}.$$

Поэтому решения уравнения (\*) образуют некоторое подпространство  $H_m$  пространства  $V_m$ . Непосредственно проверяется, что

$$\Delta f = \sum_{k=0}^{m-2} [(m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2}] x^{m-k-2} y^k.$$

Следовательно,

$$\Delta f = 0 \iff$$

$$\iff (m-k)(m-k-1)a_k + (k+2)(k+1)a_{k+2} = 0, \quad 0 \leq k \leq m-2,$$

и все коэффициенты  $a_k$  выражаются через два из них, скажем, через  $a_0$  и  $a_1$ . Таким образом,  $\dim H_m \leq 2$ .

Но два линейно независимых решения можно указать сразу. Действительно, распространив по линейности действие оператора  $\Delta$  на многочлены с комплексными коэффициентами, будем иметь

$$\begin{aligned} \Delta(x + iy)^m &= m(m-1)(x + iy)^{m-2} + imi(m-1)(x + iy)^{m-2} = 0, \\ i^2 &= -1. \end{aligned}$$

Выделяя вещественную и мнимую части, получим

$$z_m(x, y) = (x + iy)^m = u_m(x, y) + iv_m(x, y),$$

откуда

$$\Delta u_m + i\Delta v_m = \Delta z_m = 0 \implies \Delta u_m = 0, \Delta v_m = 0.$$

Итак,

$$H_m = \langle u_m(x, y), v_m(x, y) \rangle_{\mathbb{R}}.$$

Интерпретируя теперь  $x, y$  как координаты вектора в евклидовой плоскости  $\mathbb{R}^2$  с фиксированной прямоугольной системой координат, посмотрим, что произойдёт при ортогональной замене координат — повороте плоскости  $\mathbb{R}^2$  вокруг начальной точки на произвольный угол  $\theta$ :

$$x' = \Phi_\theta(x) = x \cos \theta - y \sin \theta,$$

$$y' = \Phi_\theta(y) = x \sin \theta + y \cos \theta.$$

Известное из анализа (и легко проверяемое для многочленов) правило дифференцирования сложных функций даёт

$$\begin{aligned}\frac{\partial^2 f}{\partial x'^2} &= \frac{\partial^2}{\partial x^2} - 2 \frac{\partial^2 f}{\partial x \partial y} \cos \theta \cdot \sin \theta + \frac{\partial^2 f}{\partial y^2} \sin^2 \theta, \\ \frac{\partial^2 f}{\partial y'^2} &= \frac{\partial^2}{\partial x^2} + 2 \frac{\partial^2 f}{\partial x \partial y} \cos \theta \cdot \sin \theta + \frac{\partial^2 f}{\partial y^2} \cos^2 \theta,\end{aligned}$$

откуда

$$\frac{\partial^2 f}{\partial x'^2} + \frac{\partial^2 f}{\partial y'^2} = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}.$$

Это значит, что уравнение (\*) остаётся инвариантным при ортогональной замене переменных, или, как мы ещё могли бы сказать, при действии группы  $\mathrm{SO}(2) = \{\Phi_\theta\}$ . В частности, многочлены  $u_m(x', y')$ ,  $v_m(x', y')$  будут решениями уравнения (\*) и как таковые будут линейно выражаться через  $u_m(x, y)$ ,  $v_m(x, y)$ . Таким образом, группа  $\mathrm{SO}(2)$  действует на пространстве решений уравнения Лапласа. При этом говорят о двумерном вещественном линейном представлении

$$\Phi^{(m)} : \Phi_\theta \mapsto \Phi^{(m)}(\theta)$$

группы  $\mathrm{SO}(2)$ .

Обратившись опять к комплексным многочленам, мы замечаем, что

$$x' + iy' = xe^{i\theta} + iye^{i\theta} = e^{i\theta}(x + iy),$$

$$(x' + iy')^m = e^{im\theta}(x + iy)^m.$$

Сохранив за комплексифицированным линейным оператором  $\Phi^{(m)}(\theta)$  его прежнее обозначение, будем иметь

$$\Phi^{(m)}(\theta) : z_m \mapsto z'_m = e^{im\theta} z_m.$$

Так называемые одномерные унитарные представления  $\Phi^{(m)} : \Phi_\theta \mapsto e^{im\theta}$ ,  $m \in \mathbb{Z}$ , группы  $\mathrm{SO}(2)$  играют важную роль в анализе.

Заметим, что действие  $\Phi$  индуцирует действие группы  $\mathrm{SO}(2)$  на всём пространстве  $V_m$ , и с этой точки зрения  $H_m$  — инвариантное подпространство в  $V_m$ .

**Задача 2.** Оценка числа возможных органических соединений,

например, в химии циклических углеводородов, сводится к следующей отвлечённо-житейской задаче. Сколько можно изготовить различных ожерелий длины  $n$  из неограниченного запаса жемчужин  $q$  различных цветов?

Попытаемся (вслед за Г. Полиа) ответить на этот вопрос, считая, что ожерелья ориентированы, т.е. перевёрнутое ожерелье, вообще говоря, не отождествляется с исходным.

Рис. 4.

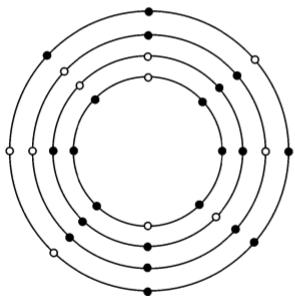
Заметим, что нитяных отрезков с нанизанными на них  $n$  жемчужинами имеется всего  $q^n$  (число слов длины  $n$  в свободной полугруппе с  $q$  образующими). На множестве  $\Omega_n$  этих отрезков действует циклическая группа порядка  $n$  с образующей  $\sigma = (12 \dots n) \in S_n$ , циклически переставляющей жемчужины на каждом отрезке. Ожерельем естественно считать  $\langle \sigma \rangle$ -орбиту отрезка или, если угодно, некоторое множество концентрических окружностей (рис. 4). Вторая интерпретация более наглядна. Она связана с изоморфизмом

$$\Phi : \sigma \mapsto \Phi(\sigma) = \begin{vmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{vmatrix},$$

который уже встречался нам ранее и который будет назван позднее двумерным линейным вещественным представлением группы  $\langle \sigma \rangle$ . Искомое число  $r$  ожерелий выражается формулой из упр. 8 § 3 гл. 1. Если  $d | n$ , то элемент  $\sigma^d$  порядка  $n/d$  оставляет на месте те отрезки (и ожерелья), которые распадаются на  $d$  периодов длины  $n/d$  (см. в этой связи [ВА I, гл. 4, § 2, упр. 12, 13]). Поэтому  $N(\sigma^d) = q^d$ , а  $N(\sigma^k) = q^m$ ,  $m = \mathrm{НОД}(n, k)$ . Величине  $N(\sigma^k)$  с  $\mathrm{НОД}(n, k) = d$  в сумме  $\sum_k N(\sigma^k)$  отвечает ровно  $\varphi(n/d)$  слагаемых ( $\varphi$  — функция Эйлера). Это означает, что

$$r = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) q^d. \quad (**)$$

Переход к физически различным (неориентируемым) ожерельям связан с дополнительными отождествлениями элементов в  $\Omega_n$  посредством обычного двумерного линейного представления группы диэд-



ра  $D_n$ ). Попытайтесь сделать это самостоятельно.

Не только в рассмотренных примерах, но и в реальных физических задачах линейные представления групп возникают самопротивожно как отражение той или иной симметрии. Соответственно идеи и язык теории представлений весьма естественны. Так, примеры, приводимые в § 1, касаются хорошо известных задач и не дают, как будто, ничего нового. Между тем сам факт появления их “под одной крышей” должен наводить на полезные размышления.

Цель, преследуемая теорией представлений, двоякая: 1) чисто математическая, диктуемая отчасти желанием использовать дополнительный аппарат для исследования самих групп; 2) прикладная, иллюстрируемая, скажем, ярким её вкладом в кристаллографию и в квантовую механику. Ни один из этих аспектов по существу не отражён в настоящей главе, цель которой более чем скромная — сказать нечто содержательное о теории представлений, основываясь исключительно на доступном нам материале из линейной алгебры и из теории групп.

## § 1. Определения и примеры линейных представлений

**1. Основные понятия.** Строго говоря, мы уже занимались теорией представлений, когда рассматривали в § 2 гл. 1 действие групп на множествах. Возьмём теперь в качестве множества векторное пространство  $V$  размерности  $n$  над полем  $K$  и выделим в группе  $S(V)$  всех биективных преобразований  $V \rightarrow V$  подгруппу  $GL(V)$  — группу обратимых линейных операторов на  $V$  (или группу автоморфизмов пространства  $V$ ). Ясно, что при любом выборе базиса  $(e_1, \dots, e_n)$  в  $V$  группа  $GL(V)$  становится обычной матричной группой  $GL(n, K)$ , которую можно считать группой автоморфизмов арифметического линейного пространства  $K^n$ . Каждому линейному оператору  $A \in GL(V)$  при этом отвечает матрица  $A = (a_{ij})$  такая, что

$$Ae_j = \sum_{i=1}^n a_{ij}e_i, \quad a_{ij} \in K, \quad \det A \neq 0.$$

**Определение 1.** Пусть  $G$  — какая-то группа. Всякий гомоморфизм  $\Phi : G \rightarrow GL(V)$  называется линейным *представлением* группы  $G$  в пространстве  $V$ . Представление называется *точным*, если ядро представления  $\text{Ker } \Phi$  состоит только из единичного элемента группы  $G$ , и *тривиальным* (или *единичным*), если  $\Phi(g) = E$  — единичный оператор для всех элементов  $g \in G$ . Размерность  $\dim_K V$  называется также *степенью представления*. При  $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$  говорят

рят соответственно о рациональном, вещественном или комплексном представлении группы  $G$ .

Таким образом, линейное представление — это пара  $(\Phi, V)$ , состоящая из *пространства представления*  $V$  (или  $G$ -*пространства*) и гомоморфизма  $\Phi : G \rightarrow \mathrm{GL}(V)$ . По определению

$$\begin{aligned}\Phi(e) &= \mathcal{E} \text{ — единичный оператор,} \\ \Phi(gh) &= \Phi(g)\Phi(h) \text{ для всех } g, h \in G.\end{aligned}$$

Условившись в обозначении  $g * v$  для действия линейного оператора  $\Phi(g)$  на вектор  $v \in V$ , мы придём к соотношениям

$$\begin{aligned}g * (u + v) &= g * u + g * v, \quad u, v \in V, \\ g * (\lambda v) &= \lambda(g * v), \quad \lambda \in K, \\ e * v &= v, \\ (gh) * v &= g * (h * v),\end{aligned}\tag{1}$$

имитирующими свойства линейных операторов, причём последние два соотношения заменяют то, что выражено выше посредством  $\Phi$  (сравнить с i), ii) в § 2 гл. 1). Соотношениями (1) в линейном представлении  $(\Phi, V)$  на первое место выдвигается  $G$ -пространство  $V$ , что бывает удобно делать по тем или иным причинам (например, когда  $V$  — не абстрактное линейное пространство, а какая-то его конкретная реализация).

С другой стороны, пространство  $V$  можно и не упоминать, если под линейным представлением понимать попросту гомоморфизм  $\Phi$  группы  $G$  в матричную группу  $\mathrm{GL}(n, K)$ . По-прежнему  $\Phi_{gh} = \Phi_g \Phi_h$ , но здесь  $\Phi_g$  — невырожденная матрица, причём  $\Phi_e = E$  — единичная матрица. Матричная интерпретация более приемлема с вычислительной точки зрения, но она менее инвариантна и лишена пространственной наглядности. На самом деле важно владеть (несложным) искусством свободного перехода от  $G$ -пространств к матричным представлениям, и обратно.

Напомним в этой связи хорошо известный из курса линейной алгебры [ВА II] факт, что две матрицы  $A, B$ , отвечающие одному и тому же линейному оператору в различных базисах, подобны:  $B = CAC^{-1}$  ( $C$  — матрица перехода от одного базиса к другому). В случае представлений, когда речь идёт о группе линейных операторов, зависимость от выбора базиса учитывается следующим образом.

**Определение 2.** Два линейных представления  $(\Phi, V)$ ,  $(\Psi, W)$  группы  $G$  называются *эквивалентными* (*изоморфными* или *подобными*), если существует изоморфизм векторных пространств  $\sigma : V \rightarrow W$ , делающий диаграмму

$$\begin{array}{ccc} V & \xrightarrow{\sigma} & W \\ \Phi(g) \downarrow & & \downarrow \Psi(g) \\ V & \xrightarrow{\sigma} & W \end{array}$$

коммутативной при всех  $g \in G$ , т. е.

$$\Psi(g)\sigma = \sigma\Phi(g), \quad g \in G,$$

или, что равносильно,

$$\Psi(g) = \sigma\Phi(g)\sigma^{-1} \quad (2)$$

(сравнить с определением эквивалентности действий группы на множествах, данным в упр. 1 из § 2 гл. 1). Будем иногда писать  $\Phi \approx \Psi$  для эквивалентных и  $\Phi \not\approx \Psi$  для неэквивалентных представлений.

Приведём ещё два варианта определения 2.

а) Терминология  $G$ -пространств. Пусть  $G$  — группа и  $V : (g, v) \mapsto g * v$ ,  $W : (g, w) \mapsto g \diamond w$  — два  $G$ -пространства с действиями  $*$ ,  $\diamond$ , удовлетворяющими условиям (1). Изоморфизм  $\sigma : V \rightarrow W$  векторных пространств является *изоморфизмом  $G$ -пространств*, если

$$g \diamond \sigma(v) = \sigma(g * v) \quad (2')$$

для всех  $g \in G$  и  $v \in V$ . Говорят ещё, что отображение  $\sigma$  перестановочно с действием  $G$ .

б) Матричная терминология. Если  $V = \langle v_1, \dots, v_n \rangle$ ,  $W = \langle w_1, \dots, w_n \rangle$  и  $\Phi_g, \Psi_g$  — матрицы линейных операторов  $\Phi(g), \Psi(g)$  относительно выбранных базисов, то условие эквивалентности (2) выражается в виде

$$\Psi_g = C\Phi_g C^{-1}, \quad (2'')$$

где  $C$  — некоторая невырожденная матрица, одна и та же для всех  $g \in G$ . Коэффициенты всех рассматриваемых матриц принадлежат одному полю  $K$ .

Отношение подобия матриц, выраженное условием (2''), есть отношение эквивалентности, разбивающее множество  $M_n(K)$  на непересекающиеся классы. Соответственно и представления группы  $G$  разбиваются на классы эквивалентных представлений. Из дальнейшего будет ясно, что для теории представлений интересны и существенны именно классы эквивалентных представлений.

Обращаясь вновь к курсу линейной алгебры, попытаемся более наглядно представить себе действие группы  $\Phi(G)$  на пространстве  $V$ . Относительно линейного оператора  $\mathcal{A} : V \rightarrow V$  в  $V$  может существовать инвариантное подпространство  $U : u \in U \implies \mathcal{A}u \in U$ . Дополнив произвольный базис  $(e_1, \dots, e_k)$  в  $U$  до базиса всего пространства  $V = \langle e_1, \dots, e_k, e_{k+1}, \dots, e_n \rangle$ , мы увидим, что матрица опе-

ратора  $A$  в базисе  $(e_1, \dots, e_n)$  примет блочно-треугольный вид:

$$A_1 = \begin{vmatrix} A_1 & A_0 \\ 0 & A_1 \end{vmatrix}.$$

Блок  $A_1$  соответствует инвариантному подпространству  $U$ , а блок  $A_2$  — факторпространству  $V/U$ . Если  $A_0$  — нулевая матрица, то  $A = A_1 + A_2$  — прямая сумма блоков и  $V = U \oplus W$  — прямая сумма инвариантных подпространств.

Существование собственного инвариантного подпространства относительно  $\mathcal{A}$  всегда обеспечено, коль скоро основное поле  $K$  алгебраически замкнуто (см. [ВА II]). Если, например,  $K = \mathbb{C}$ , то найдётся вектор  $v \in V$ ,  $v \neq 0$ , для которого  $\mathcal{A}v = \lambda v$ . Здесь  $\lambda$  — корень характеристического многочлена

$$f_{\mathcal{A}}(t) = |tE - A| = t^n - (\text{tr } A)t^{n-1} + \dots + (-1)^n \det A$$

( $A$  — произвольная матрица линейного оператора  $\mathcal{A}$ ). Это соображение позволяет выбрать в  $V$  базис, относительно которого  $A$  принимает треугольный вид:

$$A = \begin{vmatrix} \lambda_1 & & * & & \\ & \lambda_2 & & & \\ & & \ddots & & \\ 0 & & & \lambda_n & \end{vmatrix},$$

с характеристическими корнями  $\lambda_1, \lambda_2, \dots, \lambda_n$  по диагонали. Несколько более тонкий анализ заканчивается приведением  $A$  к *жордановой нормальной форме*  $J(A)$  (см. [ВА II]) — прямой сумме *жордановых клеток*

$$J_{m,\lambda} = \begin{vmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \dots & 0 \\ \dots & & & & \\ 0 & 0 & 0 & \dots & \lambda \end{vmatrix}$$

( $m \times m$  — размер клетки,  $\lambda$  — один из характеристических корней).

Заметим, что если  $A^q = E$ , то  $J_{m,\lambda}^q = E$  — единичная  $m \times m$ -матрица для каждой жордановой клетки  $J_{m,\lambda}$  матрицы  $A$ , а это, очевидно, возможно только тогда, когда  $m = 1$  и  $\lambda$  — корень степени  $q$  из 1 (по-прежнему считаем  $K = \mathbb{C}$ ). Значит,

$$A^q = E \implies CAC^{-1} = \begin{vmatrix} \lambda_1 & & 0 & & \\ & \lambda_2 & & & \\ & & \ddots & & \\ 0 & & & \lambda_n & \end{vmatrix}, \quad \lambda_i^q = 1, \quad (3)$$

для некоторой обратимой матрицы  $C$ . То же самое следует из более простого критерия диагональности линейного оператора  $\mathcal{A}$  с матри-

цей  $A$  и характеристическим многочленом  $f_A(t) = t^q - 1$  без кратных корней.

Все эти соображения, относящиеся к изолированному линейному оператору  $\mathcal{A}: V \rightarrow V$ , полезно иметь в виду при переходе к группе  $\{\Phi(g) \mid g \in G\}$  линейных операторов.

**Определение 3.** Пусть  $(\Phi, V)$  — линейное представление группы  $G$ . Подпространство  $U \subset V$  называется *инвариантным* (или *устойчивым*) относительно  $G$ , если  $\Phi(g)u \in U$  для всех  $u \in U$  и всех  $g \in G$ . Нулевое подпространство и само пространство  $V$  представления  $\Phi$  относятся к *тривиальным* инвариантным подпространствам. Представление, обладающее лишь тривиальными инвариантными подпространствами, называется *неприводимым*. Представление *приводимо*, если у него имеется хотя бы одно нетривиальное инвариантное подпространство.

Согласно сказанному выше в случае приводимого представления  $(\Phi, V)$  с инвариантным подпространством  $U$  пространство  $V$  обладает базисом, относительно которого

$$\Phi_g = \begin{vmatrix} \Phi'_g & \Phi_g^0 \\ 0 & \Phi''_g \end{vmatrix} \quad (4)$$

для всех  $g \in G$ . Так как  $\Phi'_{gh} = \Phi'_g \Phi'_h$ ,  $\Phi'_e = E_k$  и  $\Phi'_g(U) \subset U$ , то отображение  $\Phi': g \mapsto \Phi'_g$  определяет представление на  $U$ , называемое *подпредставлением* в  $\Phi$ . На факторпространстве  $V/U$  также определено представление. Оно называется *факторпредставлением* и задаётся матрицами  $\Phi''_g$ ,  $g \in G$ .

Если базис в  $V$  можно выбрать так, что все матрицы  $\Phi_g^0$  в (4) нулевые, то говорят о *разложимом* представлении  $\Phi$ , а точнее, о *прямой сумме представлений*  $\Phi = \Phi' + \Phi''$ . Разложение  $(\Phi, V)$  в прямую сумму осуществимо в точности тогда, когда инвариантное подпространство  $U \subset V$  имеет *дополнительное инвариантное подпространство*  $W$ , так что  $V = U \oplus W$  — разложение в прямую сумму подпространств и  $\Phi(U) \subset U$ ,  $\Phi(W) \subset W$ . Если это так, то  $\Phi' = \Phi|_U$ ,  $\Phi'' = \Phi|_W$  — ограничения  $\Phi$  на  $U$  и на  $W$  соответственно.

Линейное представление  $(\Phi, V)$  называется *неразложимым*, если его нельзя выразить в виде прямой суммы двух нетривиальных подпредставлений. Говорят также о *неразложимом G-пространстве*  $V$ .

Последовательно расщепляя, если это возможно,  $V, U, W$  и т. д. в прямые суммы инвариантных подпространств, мы придём к прямой сумме  $V = V_1 \oplus \dots \oplus V_r$  нескольких инвариантных подпространств (соответственно к прямой сумме  $\Phi = \Phi^{(1)} + \dots + \Phi^{(r)}$  нескольких представлений). При надлежащем выборе базиса в  $V$  матрицы ли-

нейных операторов примут вид

$$\Phi_g = \begin{vmatrix} \Phi_g^{(1)} & 0 & \dots & 0 \\ 0 & \Phi_g^{(2)} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \Phi_g^{(r)} \end{vmatrix}.$$

**Определение 4.** Линейное представление  $(\Phi, V)$  группы  $G$ , являющееся прямой суммой неприводимых представлений, называется *вполне приводимым*. Аналогичная терминология применяется по отношению к  $G$ -пространствам.

Интуитивно ясно, что неприводимые представления играют роль строительных блоков, из которых конструируются произвольные линейные представления. Вполне приводимые представления получаются в результате применения простейшей конструкции — прямой суммы. Из дальнейшего будет видно, что во многих случаях этого достаточно для описания всех представлений. Заметим, что некоторые важные для физики группы, такие, как группа Лоренца, имеют *бесконечномерные неприводимые представления*. Естественно, что они никак не сводятся к конечномерным и должны изучаться отдельно.

**2. Примеры линейных представлений.** Мы ввели все существенные понятия теории представлений. Осталось наполнить их реальным содержанием, для чего на первых порах весьма полезно познакомиться (и основательно разобраться) с приводимой ниже серией примеров.

**Пример 1.** Полная линейная группа  $\mathrm{GL}(n, K)$  над полем  $K$  имеет по определению точное неприводимое линейное представление степени  $n$  с пространством представления  $V = K^n$ . На этом же пространстве действует любая линейная группа  $H \subset \mathrm{GL}(n, K)$  — точно, но, возможно, приводимо.

Аналогичные замечания относятся к другим классическим группам, указанным в § 1 гл. 1. Скажем, унитарная группа  $U(n)$  действует неприводимым образом на эрмитовом пространстве, а ортогональная  $O(n)$  — на евклидовом. Это непосредственно следует из доказанного в [ВА II] более сильного утверждения, что группы  $U(n)$  и  $O(n)$  действуют транзитивно (в смысле примера 3 из п. 3 § 2 гл. 1) на множестве векторов единичной длины.

**Пример 2.** Заставив действовать  $\mathrm{GL}(n, K)$  на векторном пространстве  $M_n(K)$  матриц порядка  $n$  по правилу  $\Psi_A : X \mapsto AX$  ( $A \in \mathrm{GL}(n, K)$ ,  $X \in M_n(K)$ ), мы без труда убеждаемся в том, что  $\Psi_A(\alpha X + \beta Y) = \alpha\Psi_A(X) + \beta\Psi_A(Y)$  и  $\Psi_{AB} = \Psi_A\Psi_B$ . Поэтому  $(\Psi, M_n(K))$  — линейное представление степени  $n^2$ . Пусть  $M_n^{(i)}$  — подпространство матриц

$$\begin{vmatrix} 0 & \dots & x_{1i} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & x_{ni} & \dots & 0 \end{vmatrix}$$

с единственным отличным от нуля столбцом  $X^{(i)}$ . Как легко проверить, это подпространство инвариантно относительно  $\Psi_A$ ,  $A \in \mathrm{GL}(n, K)$ , неприводимо

и изоморфно (как  $\mathrm{GL}(n, K)$ -пространство) естественному пространству  $K^n$ , на котором действует  $\mathrm{GL}(n, K)$ . Таким образом,

$$M_n(K) = M_n^{(1)}(K) \oplus \dots \oplus M_n^{(n)}(K)$$

— разложение в прямую сумму  $n$  изоморфных  $\mathrm{GL}(n, K)$ -подпространств, чему соответствует разложение

$$\Psi = \Psi^{(1)} + \dots + \Psi^{(n)}$$

в прямую сумму  $n$  эквивалентных представлений. Символически этот факт записывают в виде

$$M_n(K) \cong n M_n^{(1)}(K), \quad \Psi \approx n\Psi^{(1)}.$$

**Пример 3.** Определим теперь действие  $\Phi$  группы  $\mathrm{GL}(n, K)$  на  $M_n(K)$ , положив  $\Phi_A : X \mapsto AXA^{-1}$ . Снова  $(\Phi, M_n(K))$  — линейное представление степени  $n^2$ . Если  $X = (x_{ij})$ , то, как обычно,  $\mathrm{tr} X = \sum_{i=1}^n x_{ii}$  — след матрицы  $X$ . Хорошо известно, что  $\mathrm{tr}(\alpha X + \beta Y) = \alpha \mathrm{tr} X + \beta \mathrm{tr} Y$  (линейность функции  $\mathrm{tr}$ ) и  $\mathrm{tr} \Phi_A(X) = \mathrm{tr} X$ . Отсюда следует, что множество  $M_n^0(K)$  матриц с нулевым следом является инвариантным подпространством относительно  $\Phi$ . С другой стороны,  $\Phi_A(\lambda E) = \lambda E$  и  $\mathrm{tr} \lambda E = n\lambda$ . Таким образом, в случае поля  $K$  нулевой характеристики имеет место разложение в прямую сумму  $\mathrm{GL}(n, K)$ -подпространств

$$M_n(K) = \langle E \rangle \oplus M_n^0(K) \tag{5}$$

размерностей 1 и  $n^2 - 1$  соответственно. Заметим, что при  $n = p$  и  $K = \mathbb{Z}_p$  разложение типа (5) отсутствует, поскольку в этом случае  $\mathrm{tr} E = 0$ .

Согласно определению жорданова нормальная форма  $J(X)$  матрицы  $X$  является не чем иным, как удобным и простейшим представителем  $\mathrm{GL}(n, \mathbb{C})$ -орбиты, содержащей  $X$ . Ограничение  $\Phi$  на любую подгруппу  $H \subset \mathrm{GL}(n, K)$  делает естественным вопрос о канонических представителях  $H$ -орбит.

**Пример 4.** В предыдущем примере положим  $K = \mathbb{R}$  и ограничим  $\Phi$  на ортогональную группу  $O(n)$ . Так как  $A \in O(n) \iff {}^t A = A^{-1}$ , то  ${}^t(AXA^{-1}) = {}^t A^{-1} \cdot {}^t X \cdot {}^t A = A {}^t X A^{-1}$ . Выбирая в качестве  $X$  матрицу  $Y + {}^t Y$  или  $Y - {}^t Y$ , мы видим, что пространство представления  $M_n(\mathbb{R})$  группы  $O(n)$  записывается в виде суммы  $O(n)$ -подпространств

$$M_n(\mathbb{R}) = \langle E \rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R}) \oplus M_n^-(\mathbb{R})$$

— одномерного пространства  $\langle E \rangle_{\mathbb{R}}$  скалярных матриц  $(n+2)(n-1)/2$ -мерного пространства симметричных матриц с нулевым следом и  $n(n-1)/2$ -мерного пространства кососимметричных матриц. Хорошо известно взаимно однозначное соответствие между симметричными (кососимметричными) матрицами и симметричными (соответственно кососимметричными) билинейными формами. Действие  $O(n)$  на  $\langle E \rangle_{\mathbb{R}} \oplus M_n^+(\mathbb{R})$  и на  $M_n^-(\mathbb{R})$  переносится на пространства соответствующих форм. Теорема о приведении квадратичной формы  $q(x)$  к главным осям есть не что иное, как возможность выбора в  $O(n)$ -орбите, содержащей  $q(x)$ , диагональной формы  $\sum_i \lambda_i x_i^2$  с вещественными  $\lambda_i$ , определёнными однозначно с точностью до перестановки.

Заменяя  $\mathbb{R}$  на  $\mathbb{C}$  и  $O(n)$  на унитарную группу  $U(n)$ , мы придём к разложению

$$M_n(\mathbb{C}) = \langle E \rangle_{\mathbb{C}} \oplus M_n^+(\mathbb{C}) \oplus M_n^-(\mathbb{C})$$

в прямую сумму  $U(n)$ -подпространств скалярных, эрмитовых с нулевым следом и косоэрмитовых матриц. Случай  $n = 2$  был подробно разобран в § 1 гл. 1.

Пример 5. Пусть  $G$  — группа перестановок, действующая на некотором множестве  $\Omega$  с числом элементов  $|\Omega| = n > 1$ , т.е.  $G \subset S_n$ . Векторное пространство

$$V = \langle e_i \mid i \in \Omega \rangle_K$$

над полем  $K$  нулевой характеристики с базисом, занумерованным элементами множества  $\Omega$ , мы превратим в  $G$ -пространство, полагая

$$\Phi(g) \left( \sum_{i \in \Omega} \lambda_i e_i \right) = \sum_{i \in \Omega} \lambda_i \Phi(g)e_i = \sum_{i \in \Omega} \lambda_i e_{g(i)}$$

$(i \mapsto g(i))$  — действие перестановки  $g \in G$  на  $i \in G$ . Так как  $(gh)(i) = g(h(i))$ , то получается линейное представление степени  $n$  группы  $G$ . Оно никогда не является неприводимым, поскольку

$$V = \left\langle \sum_{i \in \Omega} e_i \right\rangle \oplus \left\{ \sum_{\lambda_1 + \dots + \lambda_n = 0} \lambda_i e_i \mid \lambda_i \in K \right\} \quad (6)$$

— разложение в прямую сумму одномерного и  $(n - 1)$ -мерного инвариантных подпространств (если  $\text{char } K = p > 0$  и  $p \mid n$ , то прямой суммы уже не получится). Выделим два частных случая.

а)  $G = S_n$ . Мономорфизм  $S_n \rightarrow \text{GL}(n, \mathbb{R})$ , построенный в упр. 13 из § 4 гл. 1, совпадает с нашим линейным представлением  $\Phi$ , если взять в качестве  $e_i$   $i$ -й координатный столбец  $E^{(i)}$ . Разложение (6) показывает, что для  $S_n$  существует более экономное вложение  $S_n \rightarrow \text{GL}(n - 1, \mathbb{Q})$ . Позднее будет доказана неприводимость этого линейного представления степени  $n - 1$  (даже над полем  $\mathbb{C}$ ).

б) *Регулярное представление*. Пусть  $G$  — произвольная конечная группа. Положив  $\Omega = G$ , мы получим так называемое регулярное  $G$ -пространство  $V = \langle e_g \mid g \in G \rangle$  и соответственно *регулярное представление*  $(\rho, V)$  группы  $G : \rho(a)e_g = e_{ag}$  для всех  $a, g \in G$ . Если угодно, регулярное представление в несколько иных обозначениях нам уже встречалось при доказательстве теоремы Кэли [ВА I, гл. 4], но нас интересовало тогда не пространство  $V$ , а множество  $\{e_g\}$  его базисных векторов. Значение регулярного представления конечной группы  $G$  заключается в том, что оно содержит все неприводимые представления  $G$ , рассматриваемые с точностью до эквивалентности (см. § 5).

Пример 6. Представление степени 1 — это просто гомоморфизм  $\Phi : G \rightarrow K^*$  группы  $G$  в мультиликативную группу поля  $K$  ( $K$  — одномерное векторное пространство над собой). Так как мультиликативная группа поля абелева, то  $\text{Ker } \Phi \supset G'$ , где  $G'$  — коммутант группы  $G$  (теорема 5 из § 4 гл. 1). Заметим, что *эквивалентность двух одномерных представлений*  $\Phi'$ ,  $\Phi''$  (с одинаковым пространством представления) *равносильна их совпадению*, так как

$$a\Phi'(g)a^{-1} = \Phi''(g) \implies \Phi'(g) = \Phi''(g) \implies \Phi' = \Phi''.$$

Пусть  $g^n = e$ . Тогда  $\Phi(g)^n = \Phi(g^n) = \Phi(e) = 1$ , т.е.  $\Phi(g)$  — корень из единицы. Ядро любого одномерного представления может быть нетривиальным даже для циклической группы  $G$ . Если, например,  $G = Z_4$  и  $K = Z_{11}$ , то  $\text{Ker } \Phi \supset 2Z_4$ . С другой стороны, в случае  $K = \mathbb{C}$  любая циклическая группа имеет точное одномерное представление.

а)  $G = (\mathbb{Z}, +)$ . Представление  $k \mapsto \lambda^k$  при  $|\lambda| \neq 1$  точно. Если  $|\lambda| = 1$ , то по формуле Эйлера  $\lambda = e^{2\pi i \theta}$ ,  $\theta \in \mathbb{R}$ , и ядро отображения  $k \mapsto e^{2\pi i \theta k}$  отлично от нуля только при  $\theta \in \mathbb{Q}$ .

Группа  $\mathbb{Z}$  обладает неразложимыми комплексными представлениями сколь угодно высокой степени, которые, однако, не являются неприводимыми. Достаточно сослаться на теорему о жордановой нормальной форме матрицы и рассмотреть отображение

$$k \mapsto J_{m,1}^k = \begin{vmatrix} 1 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 1 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & 1 \end{vmatrix}^k.$$

б)  $G = \langle a \mid a^n = e \rangle$ . Пусть  $\varepsilon = \exp(2\pi i/n)$  — примитивный корень степени  $n$  из 1. Из  $n$  одномерных представлений

$$\Phi^{(m)}: a^k \mapsto \varepsilon^{mk}, \quad m = 0, 1, \dots, n-1, \quad (7)$$

точными будут  $\varphi(n)$ . Отметим интересный факт: циклическая группа порядка  $n$  имеет ровно  $n$  попарно неэквивалентных неприводимых представлений над  $\mathbb{C}$ . Все они одномерны и имеют вид (7).

Действительно, нужно убедиться лишь в том, что у конечной циклической группы нет неприводимых над  $\mathbb{C}$  представлений размерности  $> 1$ . Но перед определением 3 отмечался тот факт, что любой линейный оператор  $\Phi(g)$  конечного порядка диагонализируем над  $\mathbb{C}$ . В данном случае это равносильно полной приводимости представления  $\Phi$ . Если  $\dim \Phi = r$ , то  $\Phi$  распадается в прямую сумму  $r$  одномерных представлений.

Для циклической группы конечного порядка получено по существу описание всех комплексных линейных представлений. С точностью до эквивалентности

$$\Phi_g = \begin{vmatrix} \Phi_g^{(i_1)} & & 0 & & \\ & \ddots & & & \\ 0 & & \Phi_g^{(i_r)} & & \end{vmatrix},$$

где  $\Phi^{(m)}$  — одно из представлений вида (7).

Нашей целью является установление подобных закономерностей в общем случае.

**Пример 7.** Уже в предыдущих примерах чувствовалась сильная зависимость свойств линейного представления  $\Phi$  группы  $G$  от основного поля  $K$ . Внесём дополнительную ясность в этот вопрос.

Циклическая группа  $G = \langle a \mid a^p = e \rangle$  простого порядка  $p$ , действующая на двумерном векторном пространстве  $V = \langle v_1, v_2 \rangle$  над произвольным полем  $K$  характеристики  $p$  по правилу  $a * v_1 = v_1$ ,  $a * v_2 = v_1 + v_2$ , определяет неразложимое представление  $(\Phi, V)$ :

$$a^k \mapsto \Phi_a^k = \begin{vmatrix} 1 & k \\ 0 & 1 \end{vmatrix}, \quad 0 \leq k \leq p-1.$$

В самом деле, матрица  $\Phi_a$  имеет характеристический корень 1 кратности 2. Поэтому разложимость  $\Phi$  в прямую сумму двух одномерных представлений означала бы существование обратимой матрицы  $C$ , для которой  $C\Phi_a C^{-1} = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$ .

Но тогда  $\Phi_a = C^{-1}EC = E$ , что не так.

Пусть, далее,  $G = \langle a \mid a^3 = e \rangle$  — циклическая группа порядка 3 и  $K = \mathbb{R}$ . Двумерное представление  $(\Phi, V)$ ,  $V = \langle v_1, v_2 \rangle$ , заданное в указанном базисе матрицей

$$\Phi_a = \begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix},$$

неприводимо, поскольку характеристический многочлен  $t^3 + t + 1$  этой матрицы не имеет вещественных корней. Если же  $V$  рассматривать над  $\mathbb{C}$ , то, естественно,  $V$  разлагается в прямую сумму одномерных  $G$ -подпространств

$$V = \langle v_1 + \varepsilon^{-1} v_2 \rangle \oplus \langle v_1 + \varepsilon v_2 \rangle$$

и

$$C\Phi_a C^{-1} = \begin{vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{vmatrix}, \quad \varepsilon = \frac{-1 + \sqrt{-3}}{2}, \quad C = \begin{vmatrix} 1 & -\varepsilon^{-1} \\ 1 & -\varepsilon \end{vmatrix}.$$

Таким образом, при расширении поля свойство неприводимости представления может утрачиваться.

В дальнейшем, за редким исключением, основное поле  $K$  будет полем комплексных чисел (наиболее важным с практической точки зрения) или же произвольным алгебраически замкнутым полем нульевой характеристики.

## УПРАЖНЕНИЯ

**1.** Группа  $\mathrm{SO}(2)$  задаётся своим естественным двумерным представлением

$$\Phi'(\theta) = \begin{vmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{vmatrix},$$

неприводимым над  $\mathbb{R}$ . Проверить, что

$$A\Phi'(\theta)A^{-1} = \begin{vmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{vmatrix} \quad \text{для } A = \frac{1}{\sqrt{2}} \begin{vmatrix} 1 & i \\ i & 1 \end{vmatrix} \in \mathrm{GL}(2, \mathbb{C}).$$

Значит,  $\Phi'$  — прямая сумма двух неэквивалентных (в данном случае просто различных) одномерных представлений.

**2.** Неприводимо ли при  $n = 2$  и  $n = 3$   $\mathrm{GL}(n, \mathbb{C})$ -пространство  $M_n^0(\mathbb{C})$  в разложении (5)?

**3.** Пусть  $\Phi$  и  $\Psi$  — неприводимые комплексные представления циклической группы  $\langle a \mid a^n = e \rangle$  порядка  $n$ . Показать, что

$$\frac{1}{n} \sum_{k=0}^{n-1} \Phi(a^k) \overline{\Psi(a^k)} = \begin{cases} 1, & \text{если } \Phi \approx \Psi, \\ 0, & \text{если } \Phi \not\approx \Psi. \end{cases}$$

**4.** Опираясь на упр. 3, убедиться в справедливости следующего утверждения. Любую комплекснозначную функцию  $f$  на конечной циклической группе  $\langle a \mid a^n = e \rangle$  можно записать в виде разложения “по элементарным гармоникам”

$$f(a^k) = \sum_{m=0}^{n-1} c_m \varepsilon^{mk}, \quad \varepsilon = \exp\left(\frac{2\pi i}{n}\right).$$

“Коэффициенты Фурье”  $c_m$  вычисляются по формуле

$$c_m = \frac{1}{n} \sum_{k=0}^{n-1} f(a^k) \varepsilon^{-mk}.$$

**5.** Из формулы для числа ожерелий (см. начало главы) вывести элементарные следствия:

а)  $q^p - q \equiv 0 \pmod{p}$  (малая теорема Ферма, см. § 4 гл. 4);

б)  $\sum_{d|n} \varphi(d) = n$ .

## § 2. Унитарность и приводимость

**1. Унитарные представления.** Напомним (см. [ВА II]), что в курсе линейной алгебры невырожденная форма  $(u, v) \mapsto (u|v)$  на векторном пространстве  $V$  над  $\mathbb{C}$  называется *эрмитовой*, если

$$\begin{aligned} (u|v) &= \overline{(v|u)}, \\ (\alpha u + \beta v|w) &= \alpha(u|w) + \beta(v|w), \\ (v|v) &> 0 \quad \text{для всех } v \neq 0 \end{aligned} \tag{1}$$

(как всегда,  $z \mapsto \bar{z}$  — автоморфизм комплексного сопряжения). Пространство  $V$ , рассматриваемое вместе с невырожденной эрмитовой формой  $(u|v)$ , называется *эрмитовым* пространством. Его вещественным аналогом служит *евклидово* пространство со скалярным произведением, задаваемым невырожденной симметричной билинейной формой. Взяв базис  $e_1, \dots, e_n$  в  $V$ , мы запишем форму  $(u|v)$  для  $u = \sum_i u_i e_i$ ,  $v = \sum_j v_j e_j$  в виде

$$(u|v) = \sum_{i,j} h_{ij} u_i \bar{v}_j.$$

Матрица  $H = (h_{ij})$  удовлетворяет условию  $\bar{h}_{ij} = h_{ji}$  и называется также *эрмитовой*.

Существует ортонормированный базис (определенный условием  $(e_i|e_j) = \delta_{ij}$ ), относительно которого

$$(u|v) = \sum_{i=1}^n u_i \bar{v}_i.$$

Линейный оператор  $\mathcal{A}: V \rightarrow V$ , сохраняющий эту форму, т.е. обладающий свойством  $(\mathcal{A}u|\mathcal{A}v) = (u|v)$ , называется *унитарным оператором*. В вещественном случае ему соответствует *ортогональный оператор*. Условие унитарности, записанное в матричном виде  $A \cdot {}^t \bar{A} = E$  с  $A = (a_{ij})$ ,  ${}^t \bar{A} = A^* = (\bar{a}_{ji})$ , нам уже встречалось в гл. 1. Обозначив (как в [ВА II]) через  $\mathcal{A}^*$  линейный оператор с матрицей  ${}^t \bar{A} = A^*$ , выразим условие унитарности в виде  $\mathcal{A} \cdot \mathcal{A}^* = \mathcal{E} = \mathcal{A}^* \cdot \mathcal{A}$ . Группу всех унитарных матриц (группу унитарных операторов или просто унитарную группу) принято обозначать  $U(n)$ . По определению  $U(n) \subset GL(n, \mathbb{C})$ , и если представление  $\Phi: G \rightarrow GL(n, \mathbb{C})$  таково, что  $\text{Im } \Phi \subset U(n)$ , то  $(\Phi, V)$  называется *унитарным представлением*.

**Теорема 1.** *Всякое линейное представление  $(\Phi, V)$  над  $\mathbb{C}$  конечной группы  $G$  эквивалентно унитарному представлению.*

**Доказательство.** Выберем в пространстве представления  $V$

группы  $G$  какую-нибудь невырожденную эрмитову форму

$$H : (u, v) \mapsto H(u, v) = \sum_{i,j} h_{ij} u_i \bar{v}_j$$

(запись относительно некоторого базиса  $(f_1, \dots, f_n)$  пространства  $V$ ) и рассмотрим форму  $(u|v)$ , получающуюся из  $H(u, v)$  “усреднением” по  $G$ :

$$(u|v) = |G|^{-1} \sum_{g \in G} H(\Phi(g)u, \Phi(g)v). \quad (2)$$

Множитель  $|G|^{-1}$  несуществен и поставлен лишь для того, чтобы в случае унитарности  $\Phi$  имело место равенство  $(u|v) = H(u, v)$ . Так как

$$H(\Phi(g)u, \Phi(g)v) = \overline{H(\Phi(g)v, \Phi(g)u)},$$

$$\begin{aligned} H(\Phi(g)(\alpha u + \beta v), \Phi(g)w) &= H(\alpha \Phi(g)u + \beta \Phi(g)v, \Phi(g)w) = \\ &= \alpha H(\Phi(g)u, \Phi(g)w) + \beta H(\Phi(g)v, \Phi(g)w), \\ H(\Phi(g)v, \Phi(g)v) &> 0 \end{aligned}$$

для  $v \neq 0$  и всех  $g \in G$ , то форма (2) удовлетворяет условиям (1) и является, следовательно, невырожденной эрмитовой формой.

Кроме того (и это самое главное),

$$\begin{aligned} (\Phi(h)u | \Phi(h)v) &= \frac{1}{|G|} \sum_{g \in G} H(\Phi(g)\Phi(h)u, \Phi(g)\Phi(h)v) = \\ &= \frac{1}{|G|} \sum_{g \in G} H(\Phi(gh)u, \Phi(gh)v) = \frac{1}{|G|} \sum_{t \in G} H(\Phi(t)u, \Phi(t)v) = (u|v), \end{aligned}$$

т.е. оператор  $\Phi(g)$  при любом  $g \in G$  оставляет форму  $(u|v)$  инвариантной. Выберем в  $V$  ортонормированный относительно формы  $(u|v)$  базис. Тогда в этом базисе матрицы  $\Phi_g$  операторов  $\Phi(g)$  будут унитарными.  $\square$

**Замечание 1.** Утверждение теоремы 1 не вытекает автоматически из известного нам факта, что каждая отдельная матрица  $\Phi_g$  с  $g^m = e$  подобна унитарной  $\text{diag}(\lambda_1, \dots, \lambda_n)$  с  $\lambda_i^m = 1$ .

**Замечание 2.** В вещественном случае совершенно аналогичное рассуждение показывает, что представление  $(\Phi, V)$  эквивалентно ортогональному.

**Замечание 3.** По многим причинам унитарные представления играют важную роль в приложениях теории представлений, и весьма замечательно, что теорема 1 продолжает оставаться справедливой для гораздо более широкого класса компактных групп таких, как

$U(n)$  и  $O(n)$ . Доказательство то же самое, но суммирование по элементам группы заменяется интегрированием (по некоторой мере) на группе. Вспомним, что компактная группа  $SU(2)$  геометрически не отличима от трёхмерной сферы  $S^3$ , и поэтому имеет смысл говорить, например, о её объеме. Вообще, существует значительный параллелизм в теории представлений конечных и компактных групп, но мы лишиены возможности на этом останавливаться. Из примера 6, а) § 1 видно, что представления некомпактных групп (например,  $G = \mathbb{Z}$ ) унитарными быть не обязаны.

В заключение отметим, что хотя доказательство теоремы 1 конструктивно, было бы не очень практическим использовать его для отыскания унитарной реализации имеющегося представления. Например, для группы  $G$ , порождённой элементами  $a_1, \dots, a_d$ , достаточно добиться унитарности матриц  $\Phi_{a_1}, \dots, \Phi_{a_d}$ . Тогда и группа  $\Phi(G)$  будет унитарной.

Пример 1. Симметрическая группа  $S_3 = \langle (1\ 2), (1\ 2\ 3) \rangle$  обладает двумерным представлением  $\Phi$ , содержащимся в качестве прямого слагаемого в естественном трёхмерном представлении (см. пример 5 из § 1). Именно, если

$$\Phi(\pi)e_i = e_{\pi i}, \quad i = 1, 2, 3, \quad f_1 = e_1 - e_3, \quad f_2 = e_2 - e_3,$$

то

$$\Phi((1\ 2))f_1 = e_2 - e_3 = f_2, \quad \Phi((1\ 2))f_2 = e_1 - e_3 = f_1,$$

$$\Phi((1\ 2\ 3))f_1 = e_2 - e_1 = -f_1 + f_2, \quad \Phi((1\ 2\ 3))f_2 = e_3 - e_1 = -f_1.$$

Так как  $\pi = (1\ 2\ 3)^i(1\ 2)^j$ , где  $i = 0, 1$  или  $2$  и  $j = 0$  или  $1$ , то без труда получаются все матрицы  $\Psi_\pi = \Phi(\pi)|_{\langle f_1, f_2 \rangle}$ :

$$\begin{aligned} e_1 &\mapsto \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}, & (1\ 2) &\mapsto \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, & (1\ 3) &\mapsto \begin{vmatrix} -1 & -1 \\ 0 & 1 \end{vmatrix}, \\ (2\ 3) &\mapsto \begin{vmatrix} 1 & 0 \\ -1 & -1 \end{vmatrix}, & (1\ 2\ 3) &\mapsto \begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix}, & (1\ 3\ 2) &\mapsto \begin{vmatrix} 0 & 1 \\ -1 & -1 \end{vmatrix}. \end{aligned}$$

Из соотношений  $\det \begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix} = 1$  и  $(1\ 2\ 3)^3 = e$  следует, что

$$C \begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix} C^{-1} = \begin{vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{vmatrix}, \quad \varepsilon = \frac{-1 + \sqrt{-3}}{2},$$

для некоторой невырожденной матрицы  $C$ . Сопряжение при помощи  $C$  не должно нарушать свойства унитарности матрицы  $\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$ . Линейным условиям

$$C \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix} C, \quad C \begin{vmatrix} -1 & -1 \\ 1 & 0 \end{vmatrix} = \begin{vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{vmatrix} C$$

удовлетворяет матрица

$$C = \begin{vmatrix} 1 & -\varepsilon^2 \\ -\varepsilon^2 & 1 \end{vmatrix}.$$

Теперь мы имеем возможность выписать известные нам унитарные представления группы  $S_3$ , а именно единичные  $\Phi^{(1)}, \Phi^{(2)} : \pi \mapsto \text{sgn}(\pi) = \pm 1$  и

только что полученное двумерное представление  $\Phi^{(3)} \approx \Psi$ . Для последующих ссылок удобна такая таблица:

$S_3$	$e$	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
$\Phi^{(1)}$	1	1	1	1	1	1
$\Phi^{(2)}$	1	-1	-1	-1	1	1
$\Phi^{(3)}$	$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix}$	$\begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$	$\begin{vmatrix} 0 & \varepsilon \\ \varepsilon^{-1} & 0 \end{vmatrix}$	$\begin{vmatrix} 0 & \varepsilon^{-1} \\ \varepsilon & 0 \end{vmatrix}$	$\begin{vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{vmatrix}$	$\begin{vmatrix} \varepsilon^{-1} & 0 \\ 0 & \varepsilon \end{vmatrix}$

Пример 2. Естественное ортогональное представление бесконечной группы, а именно  $SU(2)$ , доставляет эпиморфизм  $\Phi: SU(2) \rightarrow SO(3)$ , построенный в § 1 гл. 1.

**2. Полная приводимость.** Из определений и замечаний, сделанных в § 1, ясно, насколько фундаментальным является следующее утверждение.

Теорема 2 (теорема Машке). *Каждое линейное представление конечной группы  $G$  над полем  $K$  характеристики, не делящей  $|G|$  (в частности, нулевой), вполне приводимо.*

Напомним, что утверждение теоремы 2 означает разложимость  $(\Phi, V)$  в прямую сумму неприводимых представлений. Собственно говоря, классическая теорема Машке гласит следующее.

(M) *Каждое  $G$ -инвариантное подпространство  $U \subset V$  обладает  $G$ -инвариантным дополнением  $W$ :*

$$V = U \oplus W. \quad (3)$$

Мы будем доказывать именно это утверждение, из которого теорема 2 следует автоматически. Действительно, либо представление  $(\Phi, V)$  неприводимо, и тогда нечего доказывать, либо существует собственное  $G$ -инвариантное подпространство  $U$ , и тогда имеет место разложение (3) с некоторым  $G$ -подпространством  $W$ . В этом случае  $\dim U < \dim V$ ,  $\dim W < \dim V$ . Применяя к  $U$  и  $W$  те же рассуждения и используя индукцию по размерности, получаем требуемое разложение на неприводимые компоненты.

Переходим к доказательству утверждения (M). Нас по-прежнему больше интересует случай поля  $K = \mathbb{C}$ , поэтому полезно привести два независимых рассуждения.

Первое доказательство ( $K = \mathbb{C}$ ). Согласно теореме 1 существует невырожденная эрмитова форма  $(u|v)$  на пространстве представления  $V$ , инвариантная относительно линейных операторов  $\Phi(g)$ . Для каждого подпространства  $U \subset V$  существует *ортогональное дополнение*

$$U^\perp = \{v \in V \mid (u|v) = 0 \quad \forall u \in U\},$$

и по известной теореме из курса линейной алгебры

$$V = U \oplus U^\perp,$$

причём  $(U^\perp)^\perp = U$ . Предположим теперь, что  $U$  —  $G$ -подпространство в  $V$ , т.е.  $\Phi(g)U \subset U$  для всех  $g \in G$ . Так как  $\Phi(g)|_U$  — автоморфизм, то любой элемент  $u \in U$  записывается в виде  $u = \Phi(g)u'$ ,  $u' \in U$ . Остаётся воспользоваться инвариантностью формы

$$v \in U^\perp \implies (u|\Phi(g)v) = (\Phi(g)u'| \Phi(g)v) = (u'|v) = 0.$$

Стало быть,  $v \in U^\perp \implies \Phi(g)v \in U^\perp$ . Положив  $W = U^\perp$ , придём к разложению (3).  $\square$

**Второе доказательство.** Пусть, как и прежде,  $U$  — инвариантное относительно действия  $G$  подпространство в  $V$ . Рассмотрим прямую сумму

$$V = U \oplus U',$$

где  $U'$  — произвольным образом выбранное дополнение к  $U$ . Вообще говоря,  $U'$  не является  $G$ -инвариантным. Рассмотрим оператор проектирования  $\mathcal{P} : V \rightarrow U'$ , определённый соотношением

$$\mathcal{P}v = u'$$

для всякого вектора  $v = u + u'$ . Имеем

$$v - \mathcal{P}v \in U, \quad \mathcal{P}(U) = 0, \quad \mathcal{P}^2 = \mathcal{P}. \quad (4)$$

Введём теперь “усреднённый” линейный оператор

$$\mathcal{P}_G = |G|^{-1} \sum_{h \in G} \Phi(h)\mathcal{P}\Phi(h^{-1})$$

(деление на  $|G|$  по условию возможно). Имеем

$$\Phi(g)\mathcal{P}_G = \mathcal{P}_G \Phi(g) \quad \forall g \in G. \quad (5)$$

Действительно,

$$\begin{aligned} \Phi(g)\mathcal{P}_G\Phi(g^{-1}) &= |G|^{-1} \sum_{h \in G} \Phi(g)\Phi(h)\mathcal{P}\Phi(h^{-1})\Phi(g^{-1}) = \\ &= |G|^{-1} \sum_{h \in G} \Phi(gh)\mathcal{P}\Phi((gh)^{-1}) = |G|^{-1} \sum_{t \in G} \Phi(t)\mathcal{P}\Phi(t^{-1}) = \mathcal{P}_G, \end{aligned}$$

что и приводит к соотношению (5). Положим

$$W = \mathcal{P}_G(V) = \{\mathcal{P}_Gv \mid v \in V\}.$$

Согласно (5)

$$\Phi(g)w = \Phi(g)\mathcal{P}_Gv = \mathcal{P}_G\Phi(g)v = \mathcal{P}_Gv' = w' \in W$$

для всякого  $w \in W$ , так что векторное подпространство  $W \subset V$  является на самом деле  $G$ -подпространством.

Осталось показать, что  $V = U \oplus W$  — прямая сумма  $G$ -подпространств. Так как  $\Phi(h^{-1})v - \mathcal{P}\Phi(h^{-1})v \in U$  (см. (4)), то

$v - \Phi(h)\mathcal{P}\Phi(h^{-1})v = \Phi(h)\{\Phi(h^{-1})v - \mathcal{P}\Phi(h^{-1})v\} \in \Phi(h)U = U$  (инвариантность  $U$ ). Следовательно,

$$v - \mathcal{P}_G v = |G|^{-1} \sum_{h \in G} \{v - \Phi(h)\mathcal{P}\Phi(h^{-1})v\} = u \in U,$$

и мы получаем  $v = u + w$  с  $w = \mathcal{P}_G v \in W$ , т.е.  $V = U \oplus W$ .

Далее,

$$\begin{aligned} \Phi(h^{-1})U \subset U &\implies \mathcal{P}\Phi(h^{-1})U = 0 \text{ (см.(4))} \implies \\ &\implies \Phi(h)\mathcal{P}\Phi(h^{-1})U = 0 \implies \mathcal{P}_G(U) = 0. \end{aligned}$$

Стало быть,

$$v - \mathcal{P}_G v = u \in U \implies \mathcal{P}_G(v - \mathcal{P}_G v) = 0,$$

откуда  $\mathcal{P}_G v = \mathcal{P}_G^2 v$  для всех  $v \in V$ . Это значит, что  $\mathcal{P}_G$  — проектирование на  $W$  вдоль  $U$ :

$$\mathcal{P}_G(U) = 0, \quad \mathcal{P}_G^2 = \mathcal{P}_G. \quad (6)$$

Теперь  $v \in U \cap W \implies \mathcal{P}_G v = 0$ , поскольку  $v \in U$ , и  $v = \mathcal{P}_G v'$ , поскольку  $v \in \mathcal{P}_G(V) = W$ . Используя (6), получаем

$$0 = \mathcal{P}_G v = \mathcal{P}_G(\mathcal{P}_G v') = \mathcal{P}_G^2 v' = \mathcal{P}_G v' = v \implies U \cap W = 0. \square$$

Было бы неосторожным сделать более сильное заключение об однозначности разложения на неприводимые компоненты (неприводимые  $G$ -подпространства):

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_r.$$

Если, например,  $\Phi(g) = \mathcal{E}$  — единичный оператор для всех  $g \in G$ , то любое прямое разложение  $V$  на одномерные подпространства будет разложением на неприводимые компоненты, а таких разложений бесконечно много. Другое дело, если мы сгруппируем все изоморфные неприводимые компоненты:

$$V = U_1 \oplus \dots \oplus U_s.$$

Так как мы не различаем изоморфные  $G$ -пространства, то можно считать

$$U_1 = V_1 \oplus V_1 \oplus \dots \oplus V_1 = n_1 V_1,$$

.....

$$U_s = V_s \oplus V_s \oplus \dots \oplus V_s = n_s V_s,$$

где  $n_i$  — *кратность вхождения* неприводимой компоненты  $V_i$  в разложение  $V$ . Мы увидим, что кратности определяются однозначно.

### УПРАЖНЕНИЯ

**1.** Всякое одномерное непрерывное представление группы  $(\mathbb{R}, +)$  (когда близким числам соответствуют близкие операторы) имеет вид  $\Phi^{(\alpha)} : t \mapsto e^{i\alpha t}$ , где  $\alpha$  — комплексное число. Показать, что  $\Phi^{(\alpha)}$  унитарно тогда и только тогда, когда  $\alpha \in \mathbb{R}$ .

**2.** Ядро гомоморфизма  $f : t \mapsto \begin{vmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{vmatrix}$  группы  $(\mathbb{R}, +)$  на  $\mathrm{SO}(2)$  состоит из чисел  $t = 2\pi m$ ,  $m \in \mathbb{Z}$ . Таким образом,  $\mathrm{SO}(2) \cong \mathbb{R}/(2\pi\mathbb{Z})$ , и каждому неприводимому унитарному представлению  $\Phi$  (согласно результатам § 4 оно обязательно одномерно) группы  $\mathrm{SO}(2)$  отвечает неприводимое унитарное представление

$$\tilde{\Phi} : t + 2\pi m \mapsto \Phi(t), \quad 0 \leq t < 2\pi,$$

группы  $\mathbb{R}$ , для которого  $\tilde{\Phi}(2\pi) = \Phi(0) = 1$ . Вывести из упр. 1, что  $\tilde{\Phi} = \Phi^{(n)}$ ,  $n \in \mathbb{Z}$ . В сочетании с замечанием 3) в п. 1 это означает, что всякое неприводимое представление группы  $\mathrm{SO}(2)$  имеет вид  $\Phi^{(n)}(t) = e^{int}$ ,  $n \in \mathbb{Z}$ . Проверить, что

$$\frac{1}{2\pi} \int_0^{2\pi} e^{ikt} \cdot \overline{e^{ilt}} dt = \delta^{kl}$$

(сравнить с соотношением в упр. 3 из § 1: порядок  $n$  заменён “объёмом”  $2\pi$  группы  $\mathrm{SO}(2)$ ). В анализе система функций  $\{e^{int}\}$  служит классическим примером полной ортонормированной системы периодических функций (или функций на окружности  $S^1 \sim \mathrm{SO}(2)$ ; см., в частности, [ВА II]). С этого начинается обширная теория рядов Фурье.

**3.** При помощи теоремы Машке доказать, что любое точное комплексное двумерное представление неабелевой конечной группы неприводимо.

### § 3. Конечные группы вращений

Со времён античности и вплоть до нашего времени объекты, обладающие богатой симметрией, постоянно привлекают внимание учёных. Наиболее известные и яркие примеры таких объектов — знаменитые пять платоновых тел, красота которых непосредственно, на чувственном уровне, доступна каждому человеку. В разные эпохи эта красота вдохновляла философов, математиков, астрономов, физиков на создание как мистических, так и научных систем, эстетическиозвученных правильным многогранникам по своей стройности и завершённости. В изданном в 1968 г. в русском переводе цикле лекций “Симметрия”, прочитанных великим математиком XX в. Германом Вейлем [8], раскрыто значение исследований различных аспектов симметрии как в становлении всего научного мировоззрения, так и математики в частности. Уже по этой популярной брошюре можно чётко проследить два основных, дополняющих друг друга аспекта в математическом описании симметричных объектов: нахождение необходимых условий существования (в простейших случаях формулируемых в виде одного или нескольких диофантовых уравнений

для основных параметров (см. ниже (1)) и проблема конструктивно-геометрического описания, когда действительно существующие объекты строятся в явном виде (ниже — изображения платоновых тел). С развитием теории групп и теории представлений групп спектр исследований в области симметрии чрезвычайно расширился, затронув самые различные разделы математики, физики, химии, биологии и других научных дисциплин.

В этом параграфе речь пойдёт о конечных подгруппах группы  $\mathrm{SO}(3)$ . Зная их, мы заодно получим ортогональные неприводимые представления таких групп, как  $A_4$ ,  $S_4$ ,  $A_5$ , причём в легко запоминаемой геометрической оболочке. При первом чтении можно опустить п. 1 и доказательство (весьма конспективное) теоремы 2, но тому, кто пожелает проверить прочность усвоения общей идеи “действия группы” (§ 3 гл. 1), будет полезно познакомиться с содержанием всего параграфа.

**1. Порядки конечных подгрупп в  $\mathrm{SO}(3)$ .** Согласно теореме Эйлера из курса линейной алгебры [ВА II] всякий элемент  $\mathcal{A} \in \mathrm{SO}(3)$ ,  $\mathcal{A} \neq \mathcal{E}$ , является вращением (поворотом) в евклидовом пространстве  $\mathbb{R}^3$  вокруг некоторой оси. Другими словами, имеются ровно две точки на единичной двумерной сфере  $S^2$ , остающиеся неподвижными при действии  $\mathcal{A}$ : точки пересечения сферы и оси вращения. Эти две точки называются *полюсами вращения*  $\mathcal{A}$ .

Пусть теперь  $G$  — конечная подгруппа в  $\mathrm{SO}(3)$ , а  $S$  — множество полюсов всех неединичных вращений из  $G$ . Ясно, что  $G$  действует как группа перестановок на множестве  $S$ . Если  $x$  — полюс для некоторого вращения  $\mathcal{A} \neq \mathcal{E}$ ,  $\mathcal{A} \in G$ , то при любом  $\mathcal{B}$  имеем

$$(\mathcal{B}\mathcal{A}\mathcal{B}^{-1})\mathcal{B}x = \mathcal{B} \cdot \mathcal{A}x = \mathcal{B}x,$$

т. е.  $\mathcal{B}x$  — полюс для  $\mathcal{B}\mathcal{A}\mathcal{B}^{-1}$  и, стало быть,  $\mathcal{B}x \in S$ . Обозначим через  $\Omega$  множество всех упорядоченных пар  $(\mathcal{A}, x)$ , где  $\mathcal{A} \in G$ ,  $\mathcal{A} \neq \mathcal{E}$ ,  $x$  — полюс для  $\mathcal{A}$ . Пусть, далее,  $G_x$  — стационарная подгруппа (стабилизатор) точки  $x$ , т. е. подгруппа в  $G$  всех элементов, оставляющих  $x$  на месте. Если

$$G = G_x \cup g_2 G_x \cup \dots \cup g_{m_x} G_x$$

— разложение  $G$  в левые смежные классы по  $G_x$ , то  $G$ -орбитой точки  $x$  будет множество

$$G(x) = \{x, g_2 x, \dots, g_{m_x} x\}$$

с числом элементов  $|G(x)| = m_x$ . По теореме Лагранжа  $N = m_x n_x$ , где  $N = |G|$ ,  $n_x = |G_x|$  (по сравнению с § 3 гл. 1 обозначения несколько изменены). Заметим, что  $n_x$  — порядок циклической подгруппы в  $G$ , каждый из элементов которой является вращением вокруг оси, проходящей через  $x$ . Говорят, что  $n_x$  — *кратность полюса*  $x$  или что  $x$  есть  *$n_x$ -полюс*.

Каждому элементу  $\mathcal{A} \neq \mathcal{E}$  из  $G$  соответствует два полюса, поэтому  $|\Omega| = 2(N - 1)$ . С другой стороны, для каждого полюса  $x$  имеется  $n_x - 1$  элементов из  $G$ , отличных от  $e$  и оставляющих неподвижным полюс  $x$ . Следовательно, число пар  $(\mathcal{A}, x)$  равно сумме

$$|\Omega| = \sum_{x \in S} (n_x - 1).$$

Взяв за  $\{x_1, \dots, x_k\}$  множество полюсов, по одному из каждой орбиты, положив  $n_i := n_{x_i}$ ,  $m_i := m_{x_i}$  и заметив, что  $n_x = n_{x_i} = n_i$  для всех  $x \in G(x_i)$ , мы получим

$$|\Omega| = \sum_{x \in S} (n_x - 1) = \sum_{i=1}^k m_i(n_i - 1) = \sum_{i=1}^k (N - m_i).$$

Таким образом,

$$2N - 2 = \sum_{i=1}^k (N - m_i).$$

Разделив на  $N$  обе части равенства, будем иметь

$$2 - \frac{2}{N} = \sum_{i=1}^k \left(1 - \frac{1}{n_i}\right). \quad (1)$$

Предполагаем  $N > 1$ , так что  $1 \leqslant 2 - 2/N < 2$ . Так как  $n_i \geqslant 2$ , то  $1/2 \leqslant 1 - 1/n_i < 1$ , а поэтому  $k$  должно равняться 2 или 3.

Случай 1.  $k = 2$ . Тогда

$$2 - \frac{2}{N} = \left(1 - \frac{1}{n_1}\right) + \left(1 - \frac{1}{n_2}\right),$$

или, что равносильно,

$$2 = \frac{N}{n_1} + \frac{N}{n_2} = m_1 + m_2,$$

откуда  $m_1 = m_2 = 1$ ,  $n_1 = n_2 = N$ . Стало быть,  $G$  имеет в точности одну ось вращения и  $G = C_N$  — циклическая группа порядка  $N$ .

Случай 2.  $k = 3$ . Пусть для определённости  $n_1 \leqslant n_2 \leqslant n_3$ . Если  $n_1 \geqslant 3$ , то мы имели бы

$$\sum_{i=1}^3 \left(1 - \frac{1}{n_i}\right) \geqslant \sum_{i=1}^3 \left(1 - \frac{1}{3}\right) = 2,$$

что невозможно. Таким образом,  $n_1 = 2$ , и уравнение (1) записывается в виде  $1/2 + 2/N = 1/n_2 + 1/n_3$ . Очевидно,  $n_2 \geqslant 4 \implies 1/n_2 + 1/n_3 \leqslant 1/2$  — противоречие. Поэтому  $n_2 = 2$  или  $n_2 = 3$ .

Если  $n_2 = 2$ , то  $n_3 = N/2 = m$  (т.е.  $N$  должно быть чётным) и  $m_1 = m_2 = m$ ,  $m_3 = 2$ . Эти данные соответствуют группе диздра

$D_m$  (см. пример 1 из п. 5 § 4 гл. 1). Если  $n_2 = 3$ , то  $1/6 + 2/N = 1/n_3$ , и мы имеем лишь три возможности:

2')  $n_3 = 3$ ,  $N = 12$ ,  $m_1 = 6$ ,  $m_2 = 4$ ,  $m_3 = 4$ ;

2'')  $n_3 = 4$ ,  $N = 24$ ,  $m_1 = 12$ ,  $m_2 = 8$ ,  $m_3 = 6$ ;

2''')  $n_3 = 5$ ,  $N = 60$ ,  $m_1 = 30$ ,  $m_2 = 20$ ,  $m_3 = 12$ .

Соберём все эти данные в табл. 1.

Таблица 1

$N$	Число орбит	$ S $	Порядки централизаторов		
			$n$	$n$	—
$n$	2	2	$n$	$n$	—
$2m$	3	$2m + 2$	2	2	$m$
12	3	14	2	3	3
24	3	26	2	3	4
60	3	62	2	3	5

Нами доказано следующее утверждение.

**Теорема 1.** Пусть  $G$  — конечная подгруппа в  $\mathrm{SO}(3)$ , отличная от циклической и диэдralьной. Тогда для её порядка  $N$  имеют ся лишь три возможности:  $N = 12, 24, 60$ . Другие ограничения на группу  $G$  содержатся в таб. 1.

**2. Группы правильных многогранников.** Существование групп порядков 12, 24 и 60, содержащихся в  $\mathrm{SO}(3)$ , доказывается совсем просто. С точностью до подобия существует лишь пять (известных с античных времён) правильных выпуклых многогранников в евклидовом пространстве  $\mathbb{R}^3$  (см. рис. 5): тетраэдр  $\Delta_4$ , куб  $\square_6$ , октаэдр  $\Delta_8$ , додекаэдр  $\star_{12}$  и икосаэдр  $\Delta_{20}$ :

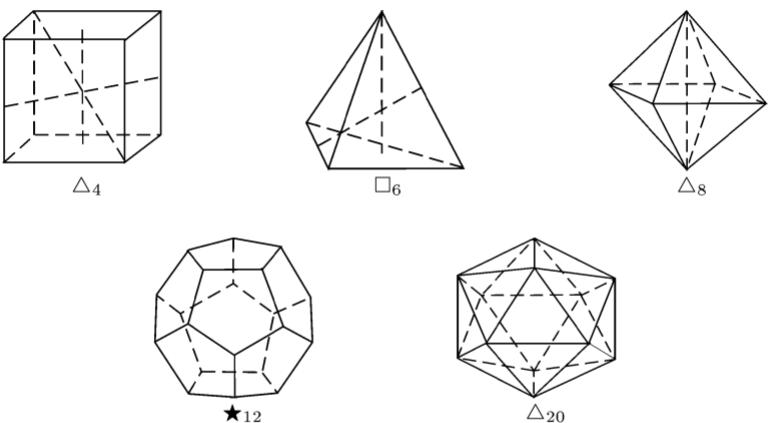


Рис. 5

Если центр правильного многогранника  $M$  поместить в начальную точку пространства  $\mathbb{R}^3$ , то вращения из  $\mathrm{SO}(3)$ , совмещающие

$M$  с собой, составят конечную подгруппу. При этом, однако, возникает не пять, а всего лишь три различные (неизоморфные) группы вращений, поскольку для куба и октаэдра, а также для додекаэдра и икосаэдра они одинаковы. Это очень легко объяснить геометрически. Если соединить отрезками середины смежных граней куба, то эти отрезки будут рёбрами вписанного в куб октаэдра. Всякое вращение в  $\mathbb{R}^3$ , оставляющее куб инвариантным, переводит в себя вписанный октаэдр, и обратно. Аналогичное замечание относится к паре додекаэдр–икосаэдр.

В табл. 2  $N_0$  — число вершин многогранника,  $N_1$  — число рёбер,  $N_2$  — число граней,  $\mu$  — число сторон (рёбер) каждой грани, а  $\nu$  — число граней, сходящихся к одной вершине. Как и ранее,  $N$  — порядок соответствующей группы.

Таблица 2

	$N_0$	$N_1$	$N_2$	$\mu$	$\nu$	$N$
Тетраэдр	4	6	4	3	3	12
Куб	8	12	6	4	3	24
Октаэдр	6	12	8	3	4	24
Додекаэдр	20	30	12	5	3	60
Икосаэдр	12	30	20	3	5	60

В соответствии с геометрической теоремой Эйлера о многогранниках

$$N_0 - N_1 + N_2 = 2.$$

Общее число полюсов равно

$$N_0 + N_1 + N_2 = 2N_1 + 2.$$

При любом вращении, переводящем многогранник в себя, данное ребро  $a_1 b_1$  совмещается с любым другим: с  $a_i b_i$  или с  $b_i a_i$ , так что  $N = 2N_1$ . Заметим ещё, что  $\{\mu, \nu\} = \{n_2, n_3\}$ , где  $n_2, n_3$  — введённые в п. 1 кратности полюсов.

Пусть, далее, **T** — группа тетраэдра, **O** — группа куба (октаэдра) и **I** — группа икосаэдра (додекаэдра).

Элементами **T** являются вращения на углы вокруг четырёх осей, соединяющих вершины с центрами противоположных граней, вращения на угол  $\pi$  вокруг каждой из трёх осей, соединяющих середины противоположных рёбер, и единичное вращение.

В группе **O**, кроме единичного, имеются вращения на углы  $\pi/2$ ,  $\pi$ ,  $3\pi/2$  вокруг трёх осей, соединяющих центры противоположных граней куба, вращения на углы  $2\pi/3$ ,  $4\pi/3$  вокруг четырёх осей, соединяющих экстремально противоположные вершины, и вращения на угол  $\pi$  вокруг каждой из шести осей, соединяющих середины диагонально-противоположных рёбер.

Правильный тетраэдр вписывается в куб и остаётся инвариантным относительно некоторых вращений из  $\mathbf{O}$  порядка 3 и 2. Вместе с единицей их набирается 12 штук и они составляют как раз группу  $\mathbf{T}$ . Следовательно,  $\mathbf{T} \subset \mathbf{O}$ , а так как  $|\mathbf{O} : \mathbf{T}| = 2$ , то  $\mathbf{T} \triangleleft \mathbf{O}$ .

Каждому элементу из  $\mathbf{O}$  соответствует ровно одна перестановка на множестве, состоящем из четырёх больших диагоналей куба. Из равенства порядков групп  $|\mathbf{O}| = |S_4| = 24$  следует их изоморфизм:  $\mathbf{O} \cong S_4$ .

Соответственно  $\mathbf{T} \cong A_4$ .

Упр. 2 показывает, что  $\mathbf{I} \cong A_5$ .

Возвращаясь к доказательству теоремы 1, заметим, что при  $n_1 = 2$ ,  $n_2 = n_3 = 3$  имеются две четырёхэлементные орбиты

$$G(p_1) = \{p_1, p_2, p_3, p_4\},$$

$$G(q_1) = \{q_1, q_2, q_3, q_4\}$$

полюсов, где  $p_i$  и  $q_i$  — противоположные точки на сфере  $S^2$ . Если  $\Delta_4^0$  — тетраэдр с вершинами  $p_i$ , то его группа преобразований симметрии  $\mathbf{T}^0$  содержит  $G$ . Из  $|G| = 12$  следует, что  $\Delta_4^0$  — правильный тетраэдр, т.е.  $\Delta_4^0 = \Delta_4$  и  $\mathbf{T}^0 = G = \mathbf{T}$ .

При  $n_2 = 3$ ,  $n_3 = 4$  берём шестиэлементную орбиту  $G(p_1) = \{p_1, \dots, p_6\}$  полюсов, которые разбиваются на пары, поскольку  $i \neq 3 \implies n_i \neq 4$ . Эти три пары точек на сфере  $S^2$  мы берём за три пары противоположных вершин октаэдра  $\Delta_8^0$ . Как и в предыдущем случае,  $|G| = 24 \implies \Delta_8^0$  (в том смысле, что  $\Delta_8^0$  — правильный октаэдр) и  $\mathbf{O}^0 = G = \mathbf{O}$ .

Наконец, при  $n_1 = 2$ ,  $n_2 = 3$ ,  $n_3 = 5$  строится икосаэдр  $\Delta_{20}^0$  с вершинами  $p_i$ , взятыми из орбиты  $G(p_i) = \{p_1, \dots, p_{20}\}$ . Снова  $|G| = 60$  влечёт правильность икосаэдра  $\Delta_{20}^0$  и совпадение групп:  $\mathbf{I}^0 = G = \mathbf{I}$ . Осталось заметить, что любые два правильных многогранника одного и того же типа, вписанные в сферу  $S^2$ , получаются друг из друга некоторым вращением (замена системы координат). Этим устанавливается сопряжённость в  $\mathrm{SO}(3)$  изоморфных подгрупп.

Соберём полученные результаты в виде теоремы.

**Теорема 2.** *Все конечные подгруппы в  $\mathrm{SO}(3)$  исчерпываются с точностью до изоморфизма группами*

$$C_n, D_n, \quad n \in \mathbb{N};$$

$$\mathbf{T} \cong A_4, \quad \mathbf{O} \cong S_4 \quad \text{и} \quad \mathbf{I} \cong A_5.$$

*Любые две изоморфные конечные подгруппы сопряжены в  $\mathrm{SO}(3)$ .*

*Следствие. Указанные в теореме 2 изоморфизмы дают не-приводимые трёхмерные ортогональные представления групп  $A_4$ ,  $S_4$  и  $A_5$ .*

Используя теорему 2 и эпиморфизм  $\Phi : \mathrm{SU}(2) \rightarrow \mathrm{SO}(3)$  (теорема 1 из § 1 гл. 1), мы легко придём к описанию всех конечных

подгрупп группы  $SU(2)$  (можно действовать и в обратном порядке). Любая такая группа  $G^*$ , отличная от циклической, является прообразом некоторой конечной подгруппы  $G \subset SO(3)$ . Возникают так называемые *бинарные группы*

$$\begin{aligned} D_n^8 &= \Phi^{-1}(D_n), & \mathbf{T}^* &= \Phi^{-1}(\mathbf{T}), \\ \mathbf{O}^* &= \Phi^{-1}(\mathbf{O}), & \mathbf{I}^* &= \Phi^{-1}(\mathbf{I}) \end{aligned}$$

— бинарная группа диэдра, бинарная группа тетраэдра, бинарная группа октаэдра и бинарная группа икосаэдра. Бинарные группы, равно как и ортогональные представления

$$\Phi: SU(2) \longrightarrow SO(3)$$

в целом возникают естественным образом при описании состояний физической системы частиц со спином.

### УПРАЖНЕНИЯ

**1.** В группе икосаэдра  $\mathbf{I}$ , помимо единичной подгруппы, имеется 15 сопряжённых циклических подгрупп порядка 2, 10 сопряжённых циклических подгрупп порядка 3 и 6 сопряжённых циклических подгрупп порядка 5. Доказать, что  $\mathbf{I}$  — простая группа.

**2.** Установить изоморфизм между группами  $\mathbf{I}$  и  $A_5$ .

**3.** Показать, что если  $H$  — конечная подгруппа нечётного порядка в  $SU(2)$  или  $SO(3)$ , то  $H$  циклическая.

**4.** Если конечная подгруппа  $H \subset SU(2)$  не является прообразом какой-либо подгруппы  $G \subset SO(3)$ , то  $|H| \equiv 1 \pmod{2}$ . Убедиться в этом.

**5.** Показать, что с точностью до сопряжения

$$D_3^* = \left\langle \left\| \begin{array}{cc} 0 & 1 \\ -1 & 0 \end{array} \right\|, \quad \left\| \begin{array}{cc} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{array} \right\|; \quad \varepsilon^2 + \varepsilon + 1 = 0 \right\rangle.$$

**6.** Что общего между собой имеют бинарная группа икосаэдра  $\mathbf{I}^*$  и группа

$$SL(2, Z_5) = \left\{ \left\| \begin{array}{cc} a & b \\ c & d \end{array} \right\| \mid ad - bc = 1; \quad a, b, c, d \in Z_5 \right\}?$$

**7.** Пусть атомы  $q$  различных сортов ( $q < 200$ ) располагаются всевозможными способами (без учёта каких-либо химических связей) в вершинах правильного многогранника  $M$ . “Молекулы”, получающиеся друг из друга поворотом вокруг некоторой оси, не различаются. Пусть  $f(M, q)$  — число различных молекул. Получить формулы

$$\begin{aligned} f(\Delta_4, q) &= \frac{q^2}{12}(q^2 + 11), \\ f(\square_6, q) &= \frac{q^2}{24}(q^6 + 17q^2 + 6), \\ f(\Delta_8, q) &= \frac{q^2}{24}(q^4 + 3q^2 + 12q + 8). \end{aligned}$$

**8.** Показать, что подсчёт числа различных раскрасок граней многогранника  $M$  красками  $q$  сортов приводит в случае тетраэдра  $\Delta_4$  к той же формуле, что и в упр. 7, а в случае куба и октаэдра формулы поменяются местами.

## § 4. Характеры линейных представлений

**1. Лемма Шура и её следствие.** В основе всякой содержательной математической теории лежит обычно несколько сравнительно несложных (но тонких) соображений. Одним из краеугольных камней теории представлений является следующее утверждение.

Теорема 1 (лемма Шура). Пусть  $(\Phi, V)$ ,  $(\Psi, W)$  — два неприводимых комплексных представления группы  $G$  и  $\sigma: V \rightarrow W$  — линейное отображение такое, что

$$\Psi(g)\sigma = \sigma\Phi(g) \quad \forall g \in G. \quad (1)$$

Тогда:

- i) если представления  $\Phi$ ,  $\Psi$  неэквивалентны, то  $\sigma = 0$ ;
- ii) если  $V = W$ ,  $\Phi = \Psi$ , то  $\sigma = \lambda E$ .

Доказательство. При  $\sigma = 0$  доказывать нечего. Считаем поэтому  $\sigma \neq 0$  и полагаем  $V_0 = \text{Ker } \sigma \subset V$ .

Так как  $\sigma\Phi(g)v_0 = \Psi(g)\sigma v_0$  при любом  $v_0 \in V_0$ , то  $\Phi(g)V_0 = V_0$ , т.е. подпространство  $V_0$  инвариантно относительно  $G$ . Ввиду неприводимости  $(\Phi, V)$  имеем  $V_0 = 0$  или  $V_0 = V$ . Равенство  $V_0 = V$  невозможно, поскольку  $\sigma \neq 0$ . Стало быть,  $\text{Ker } \sigma = 0$ .

Аналогично, полагая  $W_1 = \text{Im } \sigma \subset W$ , будем иметь

$$w_1 \in W, \implies \Psi(g)w_1 = \Psi(g)\sigma(v_1) = \sigma(\Phi(g)v_1) = w'_1 \in W_1,$$

так что  $W_1$  — инвариантное подпространство в  $W$ . Снова  $\sigma \neq 0 \implies W_1 \neq 0$ , а поскольку  $(\Psi, W)$  — неприводимое представление, остаётся единственная возможность  $W_1 = W$ .

i) Так как  $\text{Ker } \sigma = 0$ ,  $\text{Im } \sigma = W$ , то  $\sigma: V \rightarrow W$  — изоморфизм, и условие i) есть не что иное, как условие эквивалентности представлений  $\Phi$ ,  $\Psi$  (см. § 1, определение 2). Утверждение i) доказано.

ii) По условию  $\sigma: V \rightarrow W$  — линейный оператор на  $V$ . Пусть  $\lambda$  — одно из его собственных значений; оно существует, поскольку основное поле  $\mathbb{C}$  алгебраически замкнуто. Линейный оператор  $\sigma_0 = \sigma - \lambda E$  имеет нетривиальное ядро (в нём содержится собственный вектор) и удовлетворяет равенству  $\Psi(g)\sigma_0 = \sigma_0\Phi(g)$ . По ранее доказанному  $\sigma_0 = 0$ , т.е.  $\sigma = \lambda E$ .  $\square$

Следствие. Пусть  $(\Phi, V)$ ,  $(\Psi, W)$  — два неприводимых представления над  $\mathbb{C}$  конечной группы  $G$  порядка  $|G|$  и  $\sigma: V \rightarrow W$  — произвольное линейное отображение.

Тогда усреднённое отображение

$$\tilde{\sigma} = \frac{1}{|G|} \sum_{g \in G} \Psi(g)\sigma\Phi(g)^{-1}$$

обладает следующими свойствами:

- i)  $\Phi \not\cong \Psi \implies \tilde{\sigma} = 0$ ;

$$\text{ii}) \ V = W, \ \Phi = \Psi \implies \tilde{\sigma} = \lambda \mathcal{E}, \ \lambda = \frac{\operatorname{tr} \sigma}{\dim V}.$$

Доказательство. Имеем

$$\begin{aligned} \Psi(g)\tilde{\sigma}\Phi(g)^{-1} &= |G|^{-1} \sum_{h \in G} \Psi(g)\Psi(h)\sigma\Phi(h)^{-1}\Phi(g)^{-1} = \\ &= |G|^{-1} \sum_h \Psi(gh)\sigma\Phi(gh)^{-1} = |G|^{-1} \sum_{t \in G} \Psi(t)\sigma\Phi(t)^{-1} = \tilde{\sigma}, \end{aligned}$$

так что  $\Psi(g)\tilde{\sigma} = \tilde{\sigma}\Phi(g) \quad \forall g \in G$ . По лемме Шура сразу получаются оба утверждения, причём уточнение, касающееся константы  $\lambda$ , вытекает из соотношений

$$\begin{aligned} (\dim V)\lambda = \operatorname{tr} \lambda \mathcal{E} &= \operatorname{tr} \tilde{\sigma} = |G|^{-1} \sum_{g \in G} \operatorname{tr} \Phi(g)\sigma\Phi(g)^{-1} = \\ &= |G|^{-1} \sum_{g \in G} \operatorname{tr} \sigma = \operatorname{tr} \sigma. \end{aligned}$$

Здесь мы воспользовались известным свойством функции следа:  $\operatorname{tr} CAC^{-1} = \operatorname{tr} A$ .  $\square$

Нам понадобится матричная формулировка следствия. С этой целью выберем в пространствах  $V, W$  какие-нибудь базисы:

$$V = \langle e_i \mid i \in I \rangle, \quad W = \langle f_j \mid j \in J \rangle.$$

Запишем в этих базисах наши отображения (отождествляя их с соответствующими матрицами):

$$\begin{aligned} \Phi_g &= (\varphi_{ii'}(g)), \quad \Psi_g = (\psi_{jj'}(g)), \\ \sigma &= (\sigma_{ji}), \quad \tilde{\sigma} = (\tilde{\sigma}_{ji}); \quad i, i' \in I, \quad j, j' \in J. \end{aligned}$$

Согласно определению  $\tilde{\sigma}$

$$\tilde{\sigma}_{ji} = |G|^{-1} \sum_{g \in G, i' \in I, j' \in J} \psi_{jj'}(g)\sigma_{j'i'}\varphi_{i'i}(g^{-1}). \quad (2)$$

Отображение  $\sigma: V \rightarrow W$  у нас совершенно произвольное. Мы можем взять

$$\sigma_{ji} = 0 \quad \forall (j, i) \neq (j_0, i_0); \quad \sigma_{j_0 i_0} = 1. \quad (3)$$

Утверждению i) следствия тогда отвечает соотношение

$$|G|^{-1} \sum_{g \in G} \psi_{jj_0}(g) \cdot \varphi_{i_0 i(g^{-1})} = 0 \quad \forall i, i_0, j, j_0 \quad (4)$$

( $\Phi$  и  $\Psi$  — неэквивалентные представления).

Если теперь  $V = W$  и  $\Phi = \Psi$ , то

$$\operatorname{tr} \sigma = \sum_i \sigma_{ii} = \sum_{i', j'} \delta_{j'i'}\sigma_{j'i'},$$

$$\tilde{\sigma} = \frac{\operatorname{tr} \sigma}{\dim V} \mathcal{E} \implies \tilde{\sigma}_{ji} = \delta_{ji} \frac{\operatorname{tr} \sigma}{\dim V} = \frac{\delta_{ji}}{\dim V} \sum_{i',j'} \delta_{j'i'} \sigma_{j'i'}.$$

Сравнивая полученное выражение с (2), получаем

$$|G|^{-1} \sum_{g \in G, i', j'} \varphi_{jj'}(g) \sigma_{j'i'} \varphi_{i'i}(g^{-1}) = \frac{1}{\dim V} \sum_{i', j'} \delta_{ji} \delta_{j'i'} \sigma_{j'i'},$$

откуда в силу произвола в выборе  $\sigma$  (см. (3)) приходим к выводу, что утверждению ii) следствия отвечает соотношение

$$|G|^{-1} \sum_{g \in G} \varphi_{jj_0}(g) \varphi_{i_0 i}(g^{-1}) = \begin{cases} \frac{\delta_{ji}}{\dim V}, & \text{если } j_0 = i_0, \\ 0 & \text{в противном случае.} \end{cases} \quad (5)$$

В соотношениях (4) и (5) заключена вся нужная нам информация. □

**2. Характеры представлений.** С каждым комплексным конечномерным линейным представлением  $(\Phi, V)$  группы  $G$  связывается функция

$$\chi_\Phi : G \longrightarrow \mathbb{C},$$

определенная соотношением

$$\chi_\Phi(g) = \operatorname{tr} \Phi(g), \quad g \in G,$$

и называемая *характером представления*. Её обозначают также символом  $\chi_V$  или просто  $\chi$ , если ясно, о каком представлении идёт речь.

Пусть  $\Phi_g = (\varphi_{ij}(g))$  — матрица, отвечающая оператору  $\Phi(g)$  в некотором базисе пространства  $V$ , а  $\lambda_1, \dots, \lambda_n$ , ( $n = \dim V$ ) — её характеристические корни, взятые с учётом кратностей. По определению

$$\chi_\Phi(g) = \chi_V(g) = \sum_{i=1}^n \varphi_{ii}(g) = \sum_{i=1}^n \lambda_i.$$

Если  $C$  — любая обратимая матрица, то

$$\operatorname{tr} C \Phi_g C^{-1} = \operatorname{tr} \Phi_g.$$

Но мы знаем, что всякое представление  $\Psi$ , эквивалентное  $\Phi$ , имеет вид  $g \mapsto C \Phi_g C^{-1}$ . Поэтому *характеры изоморфных (эквивалентных) представлений совпадают*. Это замечание показывает, что понятие характера определено правильно.

Отметим ещё ряд элементарных свойств характеров.

**Предложение.** Пусть  $\chi_\Phi$  — характер комплексного линейного представления  $(\Phi, V)$  группы  $G$ . Тогда:

- i)  $\chi_\Phi(e) = \dim V$ ;
- ii)  $\chi_\Phi(hgh^{-1}) = \chi_\Phi(g) \quad \forall g, h \in G$ , т.е.  $\chi_\Phi$  — функция, постоянная на классах сопряжённых элементов группы  $G$ ;

iii)  $\chi_\Phi(g^{-1}) = \overline{\chi_\Phi(g)}$  для любого элемента  $g \in G$  конечного порядка (чертка означает комплексную сопряжённость);

iv) прямой сумме  $\Phi = \Phi' + \Phi''$  представлений отвечает характер  $\chi_\Phi = \chi_{\Phi'} + \chi_{\Phi''}$ .

**Доказательство.** Действительно,  $\chi_\Phi(e) = \text{tr } \Phi(e) = \text{tr } \mathcal{E} = \dim V$ . Далее,

$$\chi_\Phi(hgh^{-1}) = \text{tr } \Phi(hgh^{-1}) = \text{tr } \Phi(h)\Phi(g)\Phi(h)^{-1} = \text{tr } \Phi(g) = \chi_\Phi(g).$$

Для доказательства iii) заметим, что

$$g^m = e \implies \Phi(g)^m = \mathcal{E},$$

и если  $\lambda_1, \dots, \lambda_n$  — характеристические корни оператора  $\Phi(g)$ , то  $\lambda_1^k, \dots, \lambda_n^k$  — характеристические корни оператора  $\Phi(g)^k$ . В частности,  $\lambda_i^m = 1$ ,  $1 \leq i \leq n$ , и, стало быть,  $|\lambda_i| = 1$ ,  $\bar{\lambda}_i = \lambda_i^{-1}$ . Поэтому

$$\chi_\Phi(g^{-1}) = \text{tr } \Phi(g^{-1}) = \sum_i \lambda_i^{-1} = \sum_i \bar{\lambda}_i = \overline{\sum_i \lambda_i} = \overline{\chi_\Phi(g)}.$$

Наконец, в случае  $\Phi = \Phi' + \Phi''$  мы знаем, что при надлежащем выборе базиса в пространстве представления  $V$  все матрицы  $\Phi_g$ ,  $g \in G$ , примут вид

$$\Phi_g = \begin{vmatrix} \Phi'_g & 0 \\ 0 & \Phi''_g \end{vmatrix},$$

откуда  $\text{tr } \Phi_g = \text{tr } \Phi'_g + \text{tr } \Phi''_g$ . Это и значит, что  $\chi_\Phi(g) = \chi_{\Phi'}(g) + \chi_{\Phi''}(g)$ .  $\square$

Заметим, что при  $n = \dim V = 1$  будет  $\chi_\Phi(g) = \Phi(g)$ , но при  $n > 1$  характер  $\chi_\Phi$  не является гомоморфизмом  $G$  в  $\mathbb{C}^*$ .

**Пример 1.** Рассмотрим группу  $SU(2)$  в её естественном двумерном представлении. Пусть  $\chi$  — соответствующий характер. Согласно (5) из § 1 гл. 1 любая матрица  $g \in SU(2)$  сопряжена с матрицей

$$b_\varphi = \begin{vmatrix} e^{i\varphi/2} & 0 \\ 0 & e^{-i\varphi/2} \end{vmatrix}, \quad 0 \leq \varphi < 2\pi,$$

так что классы сопряжённых элементов группы  $SU(2)$  параметризуются вещественными числами  $\varphi$  из указанного интервала. В соответствии со свойством ii) характеров имеем

$$\chi(g) = \chi(hb_\varphi h^{-1}) = \chi(b_\varphi) = e^{i\varphi/2} + e^{-i\varphi/2} = 2 \cos \frac{\varphi}{2}.$$

При каноническом представлении  $\Phi: SU(2) \rightarrow SO(3)$  матрица  $b_\varphi$  переходит в матрицу

$$B_\varphi = \begin{vmatrix} \cos \varphi & -\sin \varphi & 0 \\ \sin \varphi & \cos \varphi & 0 \\ 0 & 0 & 1 \end{vmatrix},$$

которая также служит удобным представителем в классе сопряжённых ортогональных матриц группы  $SO(3)$ . Очевидно, что

$$\chi_\Phi(B_\varphi) = 1 + 2 \cos \varphi. \tag{6}$$

Формулой (6) мы воспользуемся позднее.

Множество  $\mathbb{C}^G = \{G \rightarrow \mathbb{C}\}$  всех функций из  $G$  в  $\mathbb{C}$  наделено естественной структурой векторного пространства над  $\mathbb{C}$ : для  $\alpha_1, \alpha_2 \in \mathbb{C}$ ,  $\chi_1, \chi_2 \in \mathbb{C}^G$  под  $\alpha_1\chi_1 + \alpha_2\chi_2$  понимается функция со значениями

$$(\alpha_1\chi_1 + \alpha_2\chi_2)(g) = \alpha_1\chi_1(g) + \alpha_2\chi_2(g).$$

Функция из  $\mathbb{C}^G$  называется *центральной*, если она постоянна на сопряжённых классах группы  $G$ . Центральные функции образуют, очевидно, векторное подпространство в  $\mathbb{C}^G$ , которое мы обозначим  $X_{\mathbb{C}}(G)$ . Вообще говоря,  $X_{\mathbb{C}}(G)$  — бесконечномерное пространство, но если в группе  $G$  имеется лишь конечное число классов сопряжённых элементов  $\mathcal{K}_1, \mathcal{K}_2, \dots, \mathcal{K}_r$  (так будет всегда для конечной группы  $G$ ), то пространство  $X_{\mathbb{C}}(G)$  конечномерно. Например,

$$X_{\mathbb{C}}(G) = \langle \Gamma_1, \Gamma_2, \dots, \Gamma_r \rangle_{\mathbb{C}},$$

где

$$\Gamma_i(g) = \begin{cases} 1, & \text{если } g \in \mathcal{K}_i, \\ 0, & \text{если } g \notin \mathcal{K}_i. \end{cases} \quad (7)$$

По доказанному (предложение ii)) характеристы группы  $G$  принадлежат пространству  $X_{\mathbb{C}}(G)$ . Мы увидим, что натянутое на них подпространство на самом деле совпадает с  $X_{\mathbb{C}}(G)$ , по крайней мере для конечной группы  $G$ .

Далее предполагаем, что группа  $G$  конечна. Превратим  $\mathbb{C}^G$  в эрмитово пространство со скалярным произведением

$$(\sigma, \tau)_G = \frac{1}{|G|} \sum_{g \in G} \sigma(g) \overline{\tau(g)}, \quad \sigma, \tau \in \mathbb{C}^G. \quad (8)$$

Легко проверяется, что форма  $(\sigma, \tau) \mapsto (\sigma, \tau)_G$  удовлетворяет всем свойствам невырожденной эрмитовой формы. Её сужение на подпространство  $X_{\mathbb{C}}(G) \subset \mathbb{C}^G$  оказывается весьма полезным инструментом, в особенности при изучении характеров линейных представлений.

**Теорема 2.** *Пусть  $\Phi, \Psi$  — неприводимые комплексные представления конечной группы  $G$ . Тогда*

$$(\chi_{\Phi}, \chi_{\Psi})_G = \begin{cases} 1, & \text{если } \Phi \approx \Psi, \\ 0, & \text{если } \Phi \not\approx \Psi. \end{cases} \quad (9)$$

**Доказательство.** В матричных обозначениях имеем

$$\chi_{\Phi}(g) = \sum_{i=1}^n \varphi_{ii}(g), \quad \chi_{\Psi}(g) = \sum_{i=1}^n \psi_{ii}(g).$$

Полагая  $i_0 = i$ ,  $j_0 = j$  в соотношении (4), а затем суммируя по  $i$  и  $j$

(в допустимых для  $i$  и  $j$  пределах), получим

$$\begin{aligned} 0 &= |G|^{-1} \sum_{g,i,j} \psi_{jj}(g) \varphi_{ii}(g) |G|^{-1} = \sum_g \left( \sum_j \psi_{jj}(g) \right) \left( \sum_i \varphi_{ii}(g^{-1}) \right) = \\ &= |G|^{-1} \sum_{g \in G} \chi_\Psi(g) \chi_\Phi(g^{-1}) = |G|^{-1} \sum_{g \in G} \chi_\Psi(g) \overline{\chi_\Phi(g)} = (\chi_\Psi, \chi_\Phi)_G \end{aligned}$$

для любых неэквивалентных неприводимых представлений  $\Phi$ ,  $\Psi$  группы  $G$ .

Используем теперь (при  $i_0 = i, j_0 = j$ ) соотношение (5):

$$\begin{aligned} 1 &= \frac{\sum_{j,i} \delta_{ji}}{\dim V} = \frac{1}{|G|} \sum_{g \in G} \left( \sum_j \varphi_{jj}(g) \right) \left( \sum_i \varphi_{ii}(g^{-1}) \right) = \\ &= |G|^{-1} \sum_{g \in G} \chi_\Phi(g) \chi_\Phi(g^{-1}) = (\chi_\Phi, \chi_\Phi)_G. \end{aligned}$$

Так как характеристы изоморфных представлений совпадают, то и  $(\chi_\Phi, \chi_\Psi)_G = 1$  при  $\Phi \approx \Psi$ .  $\square$

Соотношение (9) называется (*первым*) *соотношением ортогональности* для характеров.

**Следствие.** Пусть

$$V = V_1 \oplus \dots \oplus V_k \tag{10}$$

— разложение комплексного  $G$ -пространства  $V$  в прямую сумму неприводимых  $G$ -подпространств  $V_i$ . Если  $W$  — какое-то неприводимое  $G$ -пространство с характером  $\chi_W$ , то число слагаемых  $V_i$  в (10), изоморфных  $W$ , равно  $(\chi_V, \chi_W)_G$  и не зависит от способа разложения (кратность вхождения  $W$  в  $G$ -пространство  $V$ ). Два представления (два  $G$ -пространства) с одним и тем же характером изоморфны.

**Доказательство.** Как мы уже отмечали ранее (предложение iv)),  $\chi_V = \chi_{V_1} + \dots + \chi_{V_k}$ , и поэтому

$$(\chi_V, \chi_W)_G = (\chi_{V_1}, \chi_W)_G + \dots + (\chi_{V_k}, \chi_W)_G.$$

По теореме 2 справа стоит сумма из  $k$  нулей и единиц, причём число единиц совпадает с числом  $G$ -подпространств  $V_i$ , изоморфных  $W$ . Но скалярное произведение  $(\chi_V, \chi_W)_G$  вообще не зависит от какого-либо разложения (см. определяющее соотношение (8)), так что одновременно нами доказана инвариантность кратности вхождения  $W$  в  $G$ -пространство  $V$ .

Два  $G$ -пространства  $V, V'$  с одним и тем же характером  $\chi = \chi_V = \chi_{V'}$  содержат в своих разложениях любое слагаемое, изоморфное данному неприводимому  $G$ -пространству  $W$ , одинаковое число раз,

а именно  $(\chi, \chi_W)_G$ . Поэтому в разложениях

$$V = \bigoplus_{i=1}^k V_i, \quad V' = \bigoplus_{j=1}^l V'_j$$

на неприводимые прямые слагаемые мы можем считать  $l = k$ ,  $V'_i \cong \cong V_i$ ,  $1 \leq i \leq k$ . Следовательно, изоморфны и сами  $G$ -пространства  $V, V'$ .  $\square$

Замечания, сделанные после доказательства теоремы Машке, и следствие теоремы 2 дают возможность выразить характер  $\chi_\Phi$  любого комплексного линейного представления  $(\Phi, V)$  конечной группы  $G$  в виде целочисленной линейной комбинации

$$\chi_\Phi = \sum_{i=1}^s m_i \chi_i.$$

Здесь  $m_i$  — кратность, с которой неприводимое представление  $(\Phi_i, V_i)$  входит в разложение  $(\Phi, V)$ , так что  $\Phi_i \not\cong \Phi_j$  при  $i \neq j$ . Используя соотношение ортогональности (9), мы можем написать

$$(\chi_\Phi, \chi_\Phi)_G = \sum_{i=1}^s m_i^2. \quad (11)$$

Стало быть, скалярный квадрат  $(\chi_\Phi, \chi_\Phi)_G$  характера  $\chi_\Phi$  любого комплексного представления  $\Phi$  всегда является целым числом, равным 1 в точности тогда, когда  $\Phi$  — неприводимое представление.  $\square$

Мы пришли к замечательному результату. Характеры, или “следы представлений”, несущие скучные сведения о каждом отдельном линейном операторе  $\Phi(g)$ , выражают существенные свойства их совокупности  $\{\Phi(g) \mid g \in G\}$ , т.е. свойства самого представления  $\Phi$ .

**Пример 2.** Убедимся в неприводимости над  $\mathbb{C}$  представлений групп  $A_4, S_4$ , и  $A_5$  вращениями трёхмерного пространства. Для этого надо вернуться к следствию теоремы 2 из § 3 и воспользоваться формулами (6) и (11). Представление  $\Phi$ , описанное в § 3, показывает, что если  $\pi$  — перестановка порядка  $q$ , то  $\Phi(\pi)$  — поворот на угол  $k \cdot 2\pi/q$ ,  $\text{НОД}(k, q) = 1$ , вокруг некоторой оси. Поэтому значения характера  $\chi = \chi_\Phi$  вычисляются непосредственно по формуле (6):

$$\chi(\pi) = 1 + 2 \cos k \frac{2\pi}{q} = 3, -1, 0, 1, \frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2},$$

если соответственно  $q = 1, 2, 3, 4, 5 (k = \pm 1), 5 (k = \pm 2)$ . Заметим, что

$$\frac{1+\sqrt{5}}{2} = \text{tr} \begin{vmatrix} \varepsilon & 0 & 0 \\ 0 & \varepsilon^{-1} & 0 \\ 0 & 0 & 1 \end{vmatrix} = \varepsilon + \varepsilon^{-1} + 1, \quad \frac{1-\sqrt{5}}{2} = \varepsilon^2 + \varepsilon^{-2} + 1,$$

$$\varepsilon = \exp\left(\frac{2\pi i}{5}\right).$$

Вычисление порядка перестановки  $\pi$  по её разложению на независимые циклы описано в [ВА I, гл. 4, § 2, упр. 13]. Распределение элементов по классам сопряжённости приводилось ранее в виде таблиц. Вот те же таблицы, дополненные значениями характера  $\chi$ :

12	1	3	4	4
$A_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$\chi$	3	-1	0	0

24	1	3	6	8	6
$S_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$
$\chi$	3	-1	-1	0	1

60	1	15	20	12	12
$A_5$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4\ 5)$	$(1\ 2\ 3\ 5\ 4)$
$\chi$	3	-1	0	$(1 + \sqrt{5})/2$	$(1 - \sqrt{5})/2$

Соотношения

$$(\chi, \chi)_{A_4} = \frac{1}{12} \{1 \cdot 3^2 + 3(-1)^2 + 4 \cdot 0^2 + 4 \cdot 0^2\} = 1,$$

$$(\chi, \chi)_{S_4} = \frac{1}{24} \{1 \cdot 3^2 + 3(-1)^2 + 6(-1)^2 + 8 \cdot 0^2 + 6 \cdot 1^2\} = 1,$$

$$(\chi, \chi)_{A_5} = \frac{1}{60} \left\{ 1 \cdot 3^2 + 15(-1)^2 + 20 \cdot 0^2 + 12 \left( \frac{1 + \sqrt{5}}{2} \right)^2 + 12 \left( \frac{1 - \sqrt{5}}{2} \right)^2 \right\} = 1$$

показывают, что представление  $\Phi$  с характером  $\chi$  неприводимо над  $\mathbb{C}$  (см. (11)).

## УПРАЖНЕНИЯ

1. Пусть  $\Phi, \Psi$  — неприводимые комплексные представления конечной группы  $G$ . Получить обобщение теоремы 2

$$|G|^{-1} \sum_g \chi_\Psi(hg) \overline{\chi_\Phi(g)} = \delta_{\Phi, \Psi} \frac{\chi_\Phi(h)}{\chi_\Phi(e)}.$$

Здесь  $h$  — произвольный элемент группы  $G$ ;  $\delta_{\Phi, \Psi} = 1$  или  $\delta_{\Phi, \Psi} = 0$  в зависимости от эквивалентности или неэквивалентности  $\Phi$  и  $\Psi$ .

2. Применить критерий неприводимости, основанный на характеристиках, к представлению  $\Phi^{(3)}$  группы  $S_3$  из примера 1 п. 1 § 2.

3. Доказать при помощи леммы Шура, что все неприводимые представления над  $\mathbb{C}$  абелевой группы  $G$  одномерны.

4. Если группа  $G$  обладает автоморфизмом  $\tau$ , то с каждым линейным представлением  $(\Phi, V)$  этой группы ассоциируется ещё одно представление  $(\Phi^\tau, V)$ , определённое по правилу  $\Phi^\tau(g) = \Phi(\tau(g))$ . Проверить, что это действительно так, и показать, что неприводимость  $\Phi$  влечёт неприводимость  $\Phi^\tau$ . Как правило,  $\Phi^\tau \approx \Phi$ , но бывают случаи, когда получается новое представление. Что следует ожидать в случае внутреннего автоморфизма?

Пусть  $G = A_5$  и  $\Phi$  — представление, рассмотренное в примере 2. Отображение  $\tau : \pi \mapsto (12)\pi(12)^{-1}$  является (внешним) автоморфизмом группы  $A_5$ , представляющим классы с представителями  $(1\ 2\ 3\ 4\ 5)$  и  $(1\ 2\ 3\ 5\ 4)$ . Множества значений

характеров  $\chi$  и  $\chi^\tau$  получаются друг из друга перестановкой местами  $(1 + \sqrt{5})/2$  и  $(1 - \sqrt{5})/2$ . Показать, что характеры  $\chi^\tau$  и  $\chi$  неэквивалентны.

5. Пусть  $\Phi: G \rightarrow U(n)$ ,  $\Psi: G \rightarrow U(n)$  — эквивалентные унитарные неприводимые представления конечной группы  $G$ . Доказать, что найдётся унитарная матрица  $C$ , для которой  $C\Phi_g C^{-1} = \Psi_g \quad \forall g \in G$ .

6. Доказать, что центр  $Z(G)$  конечной группы  $G$ , обладающей точным неприводимым представлением над  $\mathbb{C}$ , всегда тривиальный или циклический.

7. Пусть  $g \mapsto \Phi_g$ ,  $g \mapsto \Psi_g$  — два матричных комплексных представления конечной группы  $G$ . Предположим, что для каждого  $g \in G$  найдётся невырожденная матрица  $C_g$  такая, что  $C_g \Phi_g C_g^{-1} = \Psi_g$ . Доказать, что существует невырожденная матрица  $C$ , не зависящая от  $g$ , для которой  $C\Phi_g C^{-1} = \Psi_g$ .

## § 5. Неприводимые представления конечных групп

**1. Число неприводимых представлений.** В случае конечных групп предыдущие рассмотрения позволяют ответить на принципиальные вопросы теории представлений. Одной из основных является следующая

Теорема 1. Число неприводимых попарно неэквивалентных представлений конечной группы  $G$  над  $\mathbb{C}$  равно числу её классов сопряжённых элементов.

Доказательство теоремы содержится в леммах 1 и 2, если заметить, что число  $r$  классов сопряжённости группы  $G$  мы интерпретируем как размерность пространства  $X_{\mathbb{C}}(G)$  центральных комплекснозначных функций на  $G$  (см. (7) из § 4). Так как характеры линейных представлений — центральные функции, то они порождают в  $X_{\mathbb{C}}(G)$  линейное подпространство некоторой размерности  $s \leq r$ . По теореме 2 из § 4 характеры неприводимых представлений составляют ортонормированный базис (в метрике  $(*, *)_G$  этого подпространства. Стало быть, интересующее нас число совпадает с  $s$ , и оно не превосходит  $r$ . Осталось установить равенство  $s = r$ .

Лемма 1. Пусть  $\Gamma$  — центральная функция на конечной группе  $G$  и  $(\Phi, V)$  — неприводимое представление над  $\mathbb{C}$  с характером  $\chi_\Phi$ .

Тогда для линейного оператора

$$\Phi_\Gamma = \sum_{h \in G} \overline{\Gamma}(h)\Phi(h): V \longrightarrow V$$

имеем  $\Phi_\Gamma = \lambda \mathcal{E}$ , где

$$\lambda = \frac{|G|}{\chi_\Phi(e)} (\chi_\Phi, \Gamma)_G$$

( $\overline{\Gamma}$  — центральная функция, определённая равенством  $\overline{\Gamma}(g) = \overline{\Gamma(g)}$ ).

**Доказательство.** Так как  $\Gamma$  — центральная функция, то

$$\begin{aligned}\Phi(g)\Phi_\Gamma\Phi(g)^{-1} &= \sum_{h \in G} \bar{\Gamma}(h)\Phi(g)\Phi(h)\Phi(g^{-1}) = \\ &= \sum_{h \in G} \bar{\Gamma}(ghg^{-1})\Phi(ghg^{-1}) = \sum_{t \in G} \bar{\Gamma}(t)\Phi(t) = \Phi_\Gamma.\end{aligned}$$

Итак,  $\Phi_\Gamma\Phi(g) = \Phi(g)\Phi_\Gamma \forall g \in G$ . Лемма Шура (теорема 1 из § 4), применённая к случаю  $\sigma = \Phi_\Gamma$ , показывает, что  $\Phi_\Gamma = \lambda \mathcal{E}$ . Вычисляя след операторов, стоящих в обеих частях этого равенства, находим

$$\begin{aligned}\lambda\chi_\Phi(e) &= \lambda \dim V = \operatorname{tr} \lambda \mathcal{E} = \operatorname{tr} \Phi_\Gamma = \sum_{h \in G} \bar{\Gamma}(h)\operatorname{tr} \Phi(h) = \\ &= |G| \left\{ |G|^{-1} \sum_{h \in G} \chi_\Phi(h)\bar{\Gamma}(h) \right\} = |G|(\chi_\Phi, \Gamma)_G. \quad \square\end{aligned}$$

**Лемма 2.** Характеры  $\chi_1, \dots, \chi_s$  всех попарно неэквивалентных неприводимых представлений группы  $G$  над  $\mathbb{C}$  образуют ортонормированный базис пространства  $X_{\mathbb{C}}(G)$ .

**Доказательство.** По теореме 2 из § 4 система  $\chi_1, \dots, \chi_s$  ортонормирована, и её можно включить в ортонормированный базис пространства  $X_{\mathbb{C}}(G)$ . Пусть  $\Gamma$  — произвольная центральная функция, ортогональная ко всем  $\chi_i$ :  $(\chi_i, \Gamma)_G = 0$ . Тогда по лемме 1 линейный оператор  $\Phi_\Gamma^{(i)}$ , отвечающий представлению  $\Phi^{(i)}$  с характером  $\chi_i$ , равен нулю.

По теореме Машке всякое комплексное представление  $\Phi$  можно разложить в прямую сумму

$$\Phi = m_1\Phi^{(1)} + \dots + m_s\Phi^{(s)}$$

с некоторыми кратностями  $m_1, \dots, m_s$ . В соответствии с этим разложением для оператора  $\Phi_\Gamma$ , определённого соотношением

$$\Phi_\Gamma = \sum_{h \in G} \bar{\Gamma}(h)\Phi(h),$$

имеем

$$\Phi_\Gamma = m_1\Phi_\Gamma^{(1)} + \dots + m_s\Phi_\Gamma^{(s)} = 0.$$

В частности, это относится к линейному оператору  $\rho_\Gamma$ , где  $\rho$  — регулярное представление (см. пример 5 из § 1). Но в таком случае будем иметь (обозначая временно единичный элемент группы  $G$  символом 1, чтобы избежать сочетания  $e_e$ )

$$0 = \rho_\Gamma(e_1) = \sum_{h \in G} \bar{\Gamma}(h)\rho(h)e_1 = \sum_{h \in G} \bar{\Gamma}(h)e_h \implies \bar{\Gamma}(h) = 0.$$

Это верно при любом  $h \in G$ , поэтому  $\bar{\Gamma} = 0$  и, следовательно,  $\Gamma = 0$ .  $\square$

Пример 1. Теорема 1, применённая к симметрической группе  $S_3$ , утверждает, что эта группа обладает ровно тремя неприводимыми комплексными представлениями. Искать их не нужно: таблица в конце п. 1 из § 2 содержит всю необходимую информацию. Заметим, между прочим, что квадраты степеней представлений  $\Phi^{(1)}, \Phi^{(2)}, \Phi^{(3)}$  удовлетворяют соотношению  $1^2 + 1^2 + 2^2 = 6 = |S_3|$ . Сейчас мы увидим, что и в общем случае выполняется аналогичное соотношение.

**2. Степени неприводимых представлений.** Рассмотрим несколько более подробно регулярное представление  $(\rho, \langle e_g \mid g \in G \rangle_{\mathbb{C}})$ . Обозначим через  $R_h$  матрицу линейного оператора  $\rho(h)$  в данном базисе  $\{e_g \mid g \in G\}$ . Так как  $\rho(h)e_g = e_{hg}$ , то все диагональные элементы матрицы  $R_h$  при  $h \neq e$  равны нулю и  $\text{tr } R_h = 0$ . Стало быть,

$$\chi_{\rho}(e) = |G|, \quad \chi_{\rho}(h) = 0 \quad \forall h \neq e. \quad (1)$$

Пусть теперь  $(\Phi, V)$  — произвольное неприводимое представление группы  $G$  над  $\mathbb{C}$ . Как показывает следствие теоремы 2 из § 4, кратность вхождения  $\Phi$  в  $\rho$  равна скалярному произведению  $(\chi_{\rho}, \chi_{\Phi})_G$ . Согласно (1)

$$\begin{aligned} (\chi_{\rho}, \chi_{\Phi})_G &= |G|^{-1} \sum_{h \in G} \chi_{\rho}(h) \overline{\chi_{\Phi}(h)} = \\ &= |G|^{-1} \chi_{\rho}(e) \overline{\chi_{\Phi}(e)} = |G|^{-1} |G| \chi_{\Phi}(e) = \dim V. \end{aligned} \quad (2)$$

Мы видим, что каждое неприводимое представление (рассматриваемое с точностью до эквивалентности) входит в регулярное с кратностью, равной своей степени. По теореме 1 имеется  $r$  попарно неэквивалентных неприводимых представлений

$$\Phi^{(1)}, \Phi^{(2)}, \dots, \Phi^{(r)}$$

( $r$  — число классов сопряжённости группы  $G$ ), которым соответствуют характеристики

$$\chi_1, \chi_2, \dots, \chi_r, \quad \chi_i = \chi_{\Phi}^{(i)},$$

степеней

$$n_1, n_2, \dots, n_r, \quad n_i = \chi_i(e).$$

Обычно за  $\Phi^{(1)}$  берут единичное представление, так что  $\chi_1(g) = 1 \forall g \in G$ . Соотношение (2) показывает, что

$$\rho = n_1 \Phi^{(1)} + \dots + n_r \Phi^{(r)},$$

откуда

$$\chi_{\rho} = n_1 \chi_1 + \dots + n_r \chi_r.$$

В частности,

$$|G| = \chi_{\rho}(e) = n_1 \chi_1(e) + \dots + n_r \chi_r(e) = n_1^2 + \dots + n_r^2.$$

**Теорема 2.** Каждое неприводимое представление  $\Phi^{(i)}$  входит в разложение регулярного представления  $\rho$  с кратностью, равной

своей степени  $n_i$ . Порядок  $|G|$  конечной группы  $G$  и степени  $n_1, \dots, n_r$  всех её неприводимых представлений связаны соотношением

$$\sum_{i=1}^r n_i^2 = |G|. \quad (3)$$

Для групп небольшого порядка красивого соотношения (3) достаточно, чтобы найти все степени  $n_1, \dots, n_r$ , хотя в общем случае нужны, конечно, дополнительные соображения.

Сведения о характеристиках неприводимых представлений (или короче: о *неприводимых характеристиках*) удобно записывать в виде таблицы

$G$	$e$	$g_2$	$g_3$	$\dots$	$g_r$
$\chi_1$	$n_1$	$\chi_1(g_2)$	$\chi_1(g_3)$	$\dots$	$\chi_1(g_r)$
$\chi_2$	$n_2$	$\chi_2(g_2)$	$\chi_2(g_3)$	$\dots$	$\chi_2(g_r)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\chi_r$	$n_r$	$\chi_r(g_2)$	$\chi_r(g_3)$	$\dots$	$\chi_r(g_r)$

называемой *таблицей характеристик*. В её верхней строке стоят представители всех  $r$  классов сопряжённости  $\mathcal{K}_i = g_i^G$  группы  $G$ . Например, таблица характеристик группы  $S_3$  имеет вид

$S_3$	$e$	(1 2)	(1 2 3)
$\chi_1$	1	1	1
$\chi_2$	1	-1	1
$\chi_3$	2	0	-1

(сравнить с таблицей в конце п. 1 из § 2). Как всегда, обозначим символом  $C(g) = C_G(g)$  централизатор в группе  $G$  элемента  $g \in G$ . Мы знаем, что  $|C(g)| |g^G| = |G|$  (см. п. 2 из § 3 гл. 1). Поэтому соотношение (9) из § 4 (первое соотношение ортогональности), переписанное в виде

$$\begin{aligned} \sum_{j=1}^r \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \frac{\overline{\chi_k(g_j)}}{\sqrt{|C(g_j)|}} &= \frac{1}{|G|} \sum_{j=1}^r \frac{|G|}{|C(g_j)|} \chi_i(g_j) \overline{\chi_k(g_j)} = \\ &= \frac{1}{|G|} \sum_{j=1}^r |g_i^G| \chi_i(g_j) \overline{\chi_k(g_j)} = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \overline{\chi_k(g)} = \\ &= (\chi_i, \chi_k)_G = \delta_{ik}, \end{aligned}$$

означает, что  $r \times r$ -матрица

$$M = \left( \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \right)$$

унитарна по строкам. Но унитарность по строкам равносильна унитарности по столбцам ( $M \cdot {}^t \bar{M} = E = {}^t \bar{M} \cdot M$ ), так что

$$\sum_i \frac{\chi_i(g_j)}{\sqrt{|C(g_j)|}} \frac{\overline{\chi_i(g_k)}}{\sqrt{|C(g_k)|}} = \delta_{jk},$$

или, в более подробной записи,

$$\sum_{i=1}^r \chi_i(g) \overline{\chi_i(h)} = \begin{cases} 0, & \text{если } g \text{ и } h \text{ не сопряжены,} \\ |C_G(g)| & \text{в противном случае.} \end{cases} \quad (4)$$

Соотношение (4) называется *вторым соотношением ортогональности* для характеров.

**3. Представления абелевых групп.** Описание неприводимых представлений циклических групп в примере 6 из § 1 допускает следующее естественное обобщение.

**Теорема 3.** *Каждое неприводимое представление конечной абелевой группы  $A$  над  $\mathbb{C}$  имеет степень 1. Число таких попарно независимых представлений равно порядку  $|A|$ . Обратно, если каждое неприводимое представление группы  $A$  имеет степень 1, то  $A$  — абелева группа.*

**Доказательство.** Число  $r$  классов сопряжённости абелевой группы  $A$  совпадает с её порядком, поэтому первые два утверждения вытекают из теоремы 2 (см. также упр. 3 из § 4). Положив, далее, в соотношении (3) все  $n_i$  равными 1, мы получим  $r = |A|$ , что равносильно коммутативности группы.  $\square$

**Определение.** Пусть  $A$  — абелева группа. Множество

$$\hat{A} = \text{Hom}(A, \mathbb{C}^*)$$

гомоморфизмов группы  $A$  в мультиликативную группу  $\mathbb{C}^*$  поля комплексных чисел, рассматриваемое вместе с поточечной операцией умножения

$$(\chi_1 \chi_2)(a) = \chi_1(a) \chi_2(a)$$

$(\chi_i \in \hat{A}, a \in A)$ , называется *группой характеров* группы  $A$  над  $\mathbb{C}$  ( $\chi^{-1} = \bar{\chi}$ ).

**Теорема 4.** *Группы  $A$  и  $\hat{A}$  изоморфны.*

**Доказательство.** Из теоремы 3 мы знаем во всяком случае, что  $|A| = |\hat{A}|$ . Согласно результатам § 3 из гл. 2 группа  $A$  допускает разложение

$$A = A_1 \times A_2 \times \dots \times A_k$$

в прямое произведение циклических групп  $A_i = \langle a_i \rangle$  (неважно каких, примарных или нет; мы выбираем мультиликативную запись закона умножения в  $A$ ). Если  $|A_i| = s_i$  и  $\varepsilon_i$  — примитивный корень  $s_i$ -й степени из 1, то каждому элементу  $a = a_1^{t_1} a_2^{t_2} \dots a_k^{t_k}$  из  $A$  отвечает характер  $\chi_a \in \hat{A}$ , определённый соотношением

$$\chi_a(a_1^{r_1} a_2^{r_2} \dots a_k^{r_k}) = \varepsilon_1^{r_1 t_1} \varepsilon_2^{r_2 t_2} \dots \varepsilon_k^{r_k t_k}.$$

Очевидно, что  $\chi_a \chi_{a'} = \chi_{aa'}$  (см. определение). Если

$$a = a_1^{t_1} a_2^{t_2} \dots a_k^{t_k} \neq a_1^{t'_1} a_2^{t'_2} \dots a_k^{t'_k} = a',$$

то существует индекс  $i$  с  $t_i \neq t'_i$ . Тогда

$$\chi_a(a_i) = \varepsilon_i^{t_i} \neq \varepsilon_i^{t'_i} = \chi_{a'}(a_i).$$

Следовательно, все характеристы  $\chi_a$  попарно различны и отображение  $a \mapsto \chi_a$  устанавливает требуемый изоморфизм между  $A$  и  $\hat{A}$ .  $\square$

Метод доказательства теоремы 4 даёт, очевидно, явную конструкцию всех неприводимых представлений абелевой группы.

**Пример.** Пусть  $V_{2^n}$  — элементарная абелева группа порядка  $2^n$ ,  $\chi$  — её неприводимый комплексный характер, отличный от единичного, т.е.  $\chi(a) \neq 1$  для некоторого  $a \in V_{2^n}$ . Тогда  $\text{Ker } \chi = B \cong V_{2^{n-1}}$  и имеет место разложение  $V_{2^n} = B \cup aB$  на смежные классы по  $B$ , так что

$$\chi(a^i b) = (-1)^i, \quad i = 0, 1.$$

В частности, четверная группа (Клейна)  $V_4$ , о представлениях которой упоминалось в задаче 2 из § 2 гл. 1, имеет следующую таблицу характеров:

$V_4$	$e$	$a$	$b$	$ab$
$\chi_1$	1	1	1	1
$\chi_2$	1	-1	1	-1
$\chi_3$	1	1	-1	-1
$\chi_4$	1	-1	-1	1

Результаты о представлениях абелевых групп позволяют получить некоторую информацию и о представлениях произвольных конечных групп.

**Теорема 5.** *Представления степени 1 конечной группы  $G$  над  $\mathbb{C}$  находятся в биективном соответствии с неприводимыми представлениями факторгруппы  $G/G'$  ( $G'$  — коммутант группы  $G$ ). Их число равно индексу  $(G : G')$ .*

**Доказательство.** Сделаем сначала общее замечание. Пусть  $G$  — произвольная группа,  $K$  — её нормальная подгруппа. Если  $\Phi$  — представление группы  $G$  с ядром  $\text{Ker } \Phi \supset K$ , то можно определить представление  $\bar{\Phi}$  факторгруппы  $G/K$ , полагая

$$\bar{\Phi}(gK) = \Phi(g), \quad g \in G.$$

Корректность этого определения очевидна (см. доказательство теоремы 1 из § 4 гл. 1). Далее,  $\text{Ker } \bar{\Phi} = (\text{Ker } \Phi)/K$ . В частности, при  $K = \text{Ker } \Phi$  получается точное представление  $\bar{\Phi}$ .

Обратно: всякое линейное представление  $\Psi$  группы  $H$  индуцирует представление  $\Phi$  группы  $G$ , допускающей эпиморфизм  $\pi : G \rightarrow H$ . Достаточно положить

$$\Phi(g) = \Psi(\pi(g)).$$

Так как  $\pi$  — эпиморфизм, то  $\Phi(G) = \Psi(H)$  и  $\Phi$ ,  $\Psi$  одновременно приводимы или неприводимы. По теореме о соответствии (теорема 3 из § 4 гл. 1)  $\text{Ker } \Phi = \pi^{-1}(\text{Ker } \Psi)$ . С любым одномерным представлением

$\Phi$  группы  $G$  ассоциируется абелева (а точнее, циклическая) группа  $\text{Im } \Phi$ , так что  $\text{Ker } \Phi \supset G'$ . Доказательство теоремы получается теперь в результате простого соединения теоремы 3, сделанного выше замечания, и теоремы 4 из § 4 гл. 1.  $\square$

**4. Представления некоторых специальных групп.** Хотя в принципе для получения всех неприводимых представлений конечной группы  $G$  достаточно разложить её регулярное представление (теорема 2), на практике это вызывает значительные трудности и приходится избирать обходные пути. Обычно бывает проще построить сначала таблицу характеров, а затем уже конструировать сами представления (см. в этой связи § 4 из гл. 4). Впрочем, в тех сравнительно несложных примерах, которые приводятся ниже, прибегать к каким-либо ухищрениям нет необходимости.

А) Пусть  $G$  — произвольная 2-транзитивная группа перестановок, действующая на множестве  $\Omega = \{1, 2, \dots, n\}$  (см. пример 3 из § 3 гл. 1). Пусть, далее,  $\Phi$  — естественное представление группы  $G$  на пространстве  $V = \langle e_1, e_2, \dots, e_n \rangle$  с действием  $\Phi(g)e_i = e_{g(i)}$  (см. пример 5 из § 1). Как нетрудно понять, значение  $\chi_\Phi(g)$  совпадает с числом  $N(g)$  точек  $i \in \Omega$  (базисных векторов  $e_i$ ), остающихся неподвижными при действии  $g$ . По теореме 3 из § 3 гл. 1 имеем

$$\sum_{g \in G} \chi_\Phi(g) \overline{\chi_\Phi(g)} = \sum_{g \in G} \chi_\Phi(g)^2 = \sum_{g \in G} N(g)^2 = 2|G|,$$

что, очевидно, переписывается в виде

$$(\chi_\Phi, \chi_\Phi)_G = 2. \quad (5)$$

Сравнивая (5) с соотношением (11) из § 4, мы приходим к заключению, что  $\Phi$  — прямая сумма двух неприводимых представлений ( $2 = 1 + 1$  — единственная запись 2 в виде суммы квадратов натуральных чисел). Но нам известно также, что  $\Phi = \Phi^{(1)} \dot{+} \Psi$ , где  $(\Phi^{(1)}, U)$  — единичное представление, а  $\Psi$  —  $(n-1)$ -мерное представление, действующее на пространстве  $W = \langle e_1 - e_n, e_2 - e_n, \dots, e_{n-1} - e_n \rangle$ . Если бы разложение  $V = U \oplus W$  можно было продолжить за счёт разложения  $W$ , то неприводимых слагаемых получилось бы больше двух. Таким образом, имеет место следующее нетривиальное утверждение.

*Естественное линейное представление  $(\Phi, V)$  2-транзитивной группы перестановок  $G$  над полем  $\mathbb{C}$  является суммой единичного представления и ещё одного неприводимого представления.*

В частности, каждая из групп  $S_n$ ,  $n > 2$ ;  $A_n$ ,  $n > 3$ , обладает неприводимым представлением  $\Psi$  над  $\mathbb{C}$  степени  $n-1$  с характером  $\chi_\Psi$ , вычисляемым по формуле

$$\chi_\Psi(g) = N(g) - 1. \quad \square \quad (6)$$

Как было показано на примере группы  $S_3$  (пример 1 из п. 1 § 2), матрицы  $\Psi_g$  находятся без особого труда. Для вычисления значений  $\chi_\Psi(g)$  по формуле (6) достаточно знать цикловую структуру перестановки  $g$ . Небольшая иллюстрация:

$A_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$\chi_\Psi$	3	-1	0	0

$S_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$
$\chi_\Psi$	3	-1	1	0	-1

$A_5$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4\ 5)$	$(1\ 2\ 3\ 5\ 4)$
$\chi_\Psi$	4	0	1	-1	-1

Б) *Неприводимые представления знакопеременной группы  $A_4$ .* Мы соберём уже известные нам факты. Группа  $A_4$  имеет четыре класса сопряжённых элементов. Представители классов и их мощности указаны в двух верхних строках таблицы

$12$	$1$	$3$	$4$	$4$
$A_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2\ 3)$	$(1\ 3\ 2)$
$\chi_1$	1	1	1	1
$\chi_2$	1	1	$\varepsilon$	$\varepsilon^{-1}$
$\chi_3$	1	1	$\varepsilon^{-1}$	$\varepsilon$
$\chi_4$	3	-1	0	0

Коммутант  $A'_4 = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  имеет индекс 3 в  $A_4$ , и поэтому  $A_4$  обладает тремя одномерными представлениями:  $\Phi^{(1)} = \chi_1$ ,  $\Phi^{(2)} = \chi_2$ ,  $\Phi^{(3)} = \chi_3$  (с ядром  $A'_4$  и с  $\varepsilon^3 = 1$ ,  $\varepsilon \neq 1$ ), и одним трёхмерным представлением  $\Phi^{(4)}$  ( $12 = 1^2 + 1^2 + 1^2 + 3^2$ ). Сравнив таблицы для  $A_4$  из примера 1 и из примера 2 из § 4, мы убедимся в том, что представление  $\Phi^{(4)}$  с характером  $\chi_4$  эквивалентно представлению  $\Phi$  группы  $A_4$  вращениями (группа тетраэдра) и представлению  $\Psi$ , связанному с 2-транзитивностью группы  $A_4$ .

В) *Неприводимые представления симметрической группы  $S_4$ .* Две верхние строки таблицы

$24$	$1$	$3$	$6$	$8$	$6$
$S_4$	$e$	$(1\ 2)(3\ 4)$	$(1\ 2)$	$(1\ 2\ 3)$	$(1\ 2\ 3\ 4)$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	-1	1	-1
$\chi_3$	2	2	0	-1	0
$\chi_4$	3	-1	-1	0	1
$\chi_5$	3	-1	1	0	-1

взяты из упр. 4 § 3 гл. 1. Представление  $\Phi^{(1)} = \chi_1$  единичное. Представление  $\Phi^{(2)}$  задаётся чётностью (знаком) перестановок из  $S_4$ . Так

как  $(S_4 : S'_4) = 2$  (пример из п. 2 § 4 гл. 1), то одномерных представлений больше нет. Двумерное представление  $\Phi^{(3)}$  с характером  $\chi_3$  и с ядром  $V_4 \triangleleft S_4$  получается из соображений, изложенных в доказательстве теоремы 5. Представление  $\Phi^{(4)}$  с характером  $\chi_4$  отвечает вращениям куба (см. таблицу для  $S_4$  из примера 2 § 4). Представление  $\Phi^{(5)} = \Psi$  с характером  $\chi_5$  (см. таблицу в примере 1) связано с 2-транзитивностью группы  $S_4$ . Оно эквивалентно также представлению, отвечающему всем преобразованиям симметрии тетраэдра  $\Delta_4$  (вращения плюс отражения; именно эти преобразования важны при описании колебаний молекулы фосфора (задача 2 из § 2 гл. 1 в [ВА I]).

Г) *Неприводимые представления группы кватернионов  $Q_8$ .* О группе  $Q_8$  всё сказано в примере 2 из п. 5 § 4 гл. 1. Там же приведено (но не названо своим именем) двумерное неприводимое представление  $\Phi^{(5)}$  с характером  $\chi_5$ ;

8 $Q_8$	1 $e$	1 $a^2$	2 $a$	2 $b$	2 $ab$
$\chi_1$	1	1	1	1	1
$\chi_2$	1	1	-1	-1	1
$\chi_3$	1	1	-1	1	-1
$\chi_4$	1	1	1	-1	-1
$\chi_5$	2	-2	0	0	0

Четыре одномерных представления имеют своим ядром коммутант  $\langle a^2 \rangle$  и определяются из таблицы в примере п. 3.

### УПРАЖНЕНИЯ

1. Получить соотношение (4), выписывая в явном виде выражение  $t_{ij} = (\Gamma_i, \chi_j)_G$  для коэффициентов разложения  $\Gamma_i = \sum_j t_{ij} \chi_j$  базисной центральной функции  $\Gamma_i$  (см. (7) из § 4) через неприводимые характеристы.

2. Проверить (и вспомнить об изоморфизме между векторным пространством  $V$  и сопряжённым к нему пространством  $V^*$  линейных функций), что отображение  $\tau : A \longrightarrow \hat{A}$ , определённое условием

$$a^\tau(\chi) = \chi(a),$$

задаёт изоморфизм абелевой группы  $A$  на  $\hat{A}$ .

Это упражнение вместе с теоремой 4 устанавливает часть так называемого *закона двойственности* для конечных абелевых групп. Аналогичный, но гораздо более глубокий закон двойственности для топологических абелевых групп, приводящий к важным следствиям, был установлен в 30-х годах Л.С. Понтрягиным.

3. Доказать, что если конечная абелева группа  $A$  допускает точное комплексное неприводимое представление, то  $A$  — циклическая группа.

4. Пусть  $A$  — конечная абелева группа,  $B$  — её подгруппа. Доказать, что любой характер группы  $B$  продолжается до характера группы  $A$  и число таких продолжений равно индексу  $(A : B)$ .

5. Обосновать фразу перед заключительными скобками в В) из п. 4.

6. Чему равна средняя величина  $\frac{1}{|G|} \sum_g \chi(g)$  значений комплексного характера  $\chi$  на элементах конечной группы  $G$ ?

7. Собрать из разных мест таблицы, относящиеся к группе  $A_5$ , в сводную таблицу характеров

$60$ $A_5$	$1$ $e$	$15$ $(1\ 2)(3\ 4)$	$20$ $(1\ 2\ 3)$	$12$ $(1\ 2\ 3\ 4\ 5)$	$12$ $(1\ 2\ 3\ 5\ 4)$
$\chi_1$	1	1	1	1	1
$\chi_2$	3	-1	0	$(1 + \sqrt{5})/2$	$(1 - \sqrt{5})/2$
$\chi_3$	3	-1	0	$(1 - \sqrt{5})/2$	$(1 + \sqrt{5})/2$
$\chi_4$	4	0	1	-1	-1
$\chi_5$	*	*	*	*	*

Дать описание неприводимых представлений с характерами  $\chi_1, \chi_2, \chi_3, \chi_4$ . Заполнить последнюю строку таблицы, используя второе соотношение ортогональности (4) для характеров.

8. Пусть  $P = \langle A^i B^j C^k; 0 \leq i, j, k \leq p-1 \rangle$  — группа порядка  $p^3$ , рассмотренная в упр. 3 из § 3 гл. 1;  $V = \langle e_0, e_1, \dots, e_{p-1} \rangle_C$  — комплексное векторное пространство размерности  $p$ ;  $\varepsilon$  — примитивный корень степени  $p$  из 1;  $\mathcal{A}, \mathcal{B}, \mathcal{C}$  — линейные операторы на  $V$ , определённые соотношениями

$$\mathcal{A}e_i = e_{i+1}, \quad \mathcal{B}^k e_i = \varepsilon^{-ki} e_i, \quad \mathcal{C}^k e_i = \varepsilon^k e_i, \quad 0 \leq i \leq p-1$$

(нижние индексы у базисных элементов берутся по модулю  $p$ ).

Показать, что отображение

$$\Phi^{(k)} : A \mapsto \mathcal{A}, \quad B \mapsto \mathcal{B}^k, \quad C \mapsto \mathcal{C}^k$$

задаёт линейное неприводимое представление группы  $P$ . Представления  $\Phi^{(1)}, \dots, \Phi^{(p-1)}$  попарно неэквивалентны и вместе с  $p^2$  одномерными представлениями ( $p^2$  — индекс коммутанта  $P' = \langle C \rangle$  в  $P$ ) исчерпывают все неприводимые комплексные представления группы  $P$ .

9. Дополнить вычислениями следующее рассуждение. Пусть

$$D_n = \langle a, b | a^n = e, b^2 = e, bab^{-1} = a^{n-1} \rangle$$

— группа диэдра порядка  $2n$ , свойства которой (включая описание классов сопряжённых элементов) даны в примере 1 из п. 5 § 4 гл. 1. Так как  $\langle a \rangle \triangleleft D_n$ , то отображениями  $a \mapsto 1, b \mapsto 1$  и  $a \mapsto 1, b \mapsto -1$  задаются два одномерных представления. Пусть  $\varepsilon$  — примитивный корень  $n$ -й степени из 1. Тогда отображение

$$\Phi^{(j)} : a \mapsto \begin{vmatrix} \varepsilon^j & 0 \\ 0 & \varepsilon^{-j} \end{vmatrix}$$

будет определять представление степени 2. Представление  $\Phi^{(j)}$  неприводимо при  $j = 1, 2, \dots, [(n-1)/2]$  ( $[\alpha]$  — целая часть вещественного числа  $\alpha$ ). При  $n = 2m$  представление  $\Phi^{(m)}$  распадается в прямую сумму двух одномерных представлений:  $a \mapsto -1, b \mapsto 1$  и  $a \mapsto -1, b \mapsto -1$ . Это согласуется с тем фактом, что коммутант  $D'_{2m}$  имеет индекс 4 в  $D_{2m}$  и  $D_{2m}/D'_{2m} \cong Z_2 \times Z_2$ . Все указанные представления неприводимы и составляют полное множество неприводимых комплексных представлений группы диэдра. Найти вещественную реализацию представлений  $\Phi^{(j)}$ . Указать в явном виде изоморфизм (эквивалентность)  $\Phi^{(j)} \approx \Phi^{(k)}$ ,  $k > m$ ,  $j \leq m$ .

**10. Кристаллографические группы** (к задаче 2 из § 2 гл. 1 в [ВА I]). Пусть  $E$  —  $n$ -мерное евклидово пространство и  $V$  — ассоциированное с ним векторное пространство с евклидовым скалярным произведением. Всякому движению  $d$  пространства  $E$  отвечает ортогональное линейное преобразование  $\bar{d} \in O(n)$ , причём так, что  $d_1 d_2 = \bar{d}_1 \bar{d}_2$ . Группа  $D$  движений пространства называется *кристаллографической группой*, если  $D$ -орбита произвольной точки дискретна (не имеет предельных точек) и существует компактное множество  $M \subset E$ , для которого  $D(M) = \bigcup_{d \in D} d(M) = E$ . Справедлива теорема Шёнфлиса–Бибербаха, согласно которой кристаллографическая группа  $D$  содержит  $n$  независимых аффинных переносов, порождающих в  $D$  нормальную подгруппу  $L$ , и  $\bar{D} \cong D/L$  — конечная группа (точечная кристаллографическая группа). Всего геометрически различных точечных кристаллографических групп при  $n = 3$  имеется 32. Среди них, очевидно, должны быть группы, содержащие отражения (несобственные движения). Из условий кристаллографичности следует, что всякое собственное вращение из  $\bar{D}$  изображается матрицей, подобной

$$A = \begin{vmatrix} \cos \theta & -\sin \theta & 0 \\ \sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

с  $\operatorname{tr} A = 1 + 2 \cos \theta \in \mathbb{Z}$ . Опираясь на теорему 2 из § 3 и на отмеченное соображение, показать, что при  $n = 3$  точечными кристаллографическими группами без отражений будут, лишь циклические  $C_1, C_2, C_3, C_4, C_6$ , диэдральные  $D_2, D_3, D_4, D_6$ , группа тетраэдра  $\mathbf{T}$  и группа куба (октаэдра)  $\mathbf{O}$ .

## § 6. Представления групп SU(2) и SO(3)

Частью “физического” мышления являются конкретные образы, связанные с представлениями группы SO(3). Действие SO(3), отражающее симметрию многих физических задач, с математической точки зрения интересно, в частности, тем, что оно индуцирует действие на пространстве решений уравнения  $\Delta f = 0$ , где

$$\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} + \frac{\partial^2}{\partial z^2}$$

— дифференциальный оператор Лапласа. Двумерный аналог этой задачи был рассмотрен в самом начале главы (задача 1).

Всякий элемент группы SO(3) является произведением нескольких операторов  $B_\varphi, C_\theta$  вида (1) из § 1 гл. 1. Но  $B_\varphi$  не действует на  $z$ , а  $C_\theta$  на  $x$ . Поэтому инвариантность уравнения  $\Delta f = 0$  относительно  $B_\varphi$  и  $C_\theta$  вытекает из тех выкладок, которые были проведены в двумерном случае. Мы приходим к заключению, что уравнение  $\Delta f = 0$  инвариантно относительно всей группы SO(3), или, что то же самое,

$$\Delta f = 0 \implies \Delta(\Phi_g f) = 0 \quad \forall g \in \text{SO}(3),$$

где  $\Phi_g f$  — функция, определённая соотношением

$$(\Phi_g f)(x, y, z) = f(g^{-1}(x), g^{-1}(y), g^{-1}(z)). \tag{1}$$

По условию для ортогонального преобразования  $g^{-1}$  с матрицей  $(a_{ij})_1^3$  столбец новых переменных имеет вид

$$\begin{vmatrix} g^{-1}(x) \\ g^{-1}(y) \\ g^{-1}(z) \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \begin{vmatrix} x \\ y \\ z \end{vmatrix}.$$

Согласно (1)

$$\begin{aligned} (\Phi_g(\Phi_h f))(x, y, z) &= (\Phi_h f)(g^{-1}(x), g^{-1}(y), g^{-1}(z)) = \\ &= f(h^{-1}(g^{-1}(x)), h^{-1}(g^{-1}(y)), h^{-1}(g^{-1}(z))) = \\ &= f((gh)^{-1}(x), (gh)^{-1}(y), (gh)^{-1}(z)) = (\Phi_{gh} f)(x, y, z). \end{aligned}$$

Стало быть,

$$\Phi_g \Phi_h = \Phi_{gh},$$

т.е. линейные операторы  $\Phi_g$ ,  $g \in \mathrm{SO}(3)$ , действуют на функциях так, что отображение  $\Phi : g \mapsto \Phi_g$  является представлением группы  $\mathrm{SO}(3)$ . Этот весьма естественный способ построения представлений (фактически применённый нами ранее при рассмотрении симметрических функций с действующей группой  $S_n$ ), годится в принципе для широкого класса групп и относится к типичным методам функционального анализа. Нужно лишь, исходя из конкретных условий, выбрать надлежащее пространство функций и затем разложить его на неприводимые инвариантные подпространства (задача гармонического анализа).

В случае группы  $\mathrm{SO}(3)$ , когда все неприводимые представления конечномерны (общий факт для компактных групп), за функции берутся однородные многочлены

$$f(x, y, z) = \sum_{s,t} a_{s,t} x^s y^t z^{m-s-t}$$

фиксированной степени  $m$  ( $m = 1, 2, 3, \dots$ ). Они образуют пространство  $P_m$  размерности  $\binom{m+2}{2}$  (см. [ВА I, гл. 5, § 2, упр. 4]). Так как  $\Delta f \in P_{m-2}$ , то условие  $\Delta f = 0$  эквивалентно  $\binom{m}{2}$  линейным условиям на коэффициенты  $a_{s,t}$ . Решения  $f \in P_m$  уравнения  $\Delta f = 0$  называются однородными гармоническими многочленами (гармоническими полиномами) степени  $m$ . Ввиду линейности оператора  $\Delta$  они образуют подпространство  $H_m$  размерности  $\binom{m+2}{2} - \binom{m}{2} = 2m + 1$  (у нас  $\leqslant 2m + 1$ , но на самом деле имеет место равенство). Согласно вышесказанному  $H_m$  инвариантно относительно действия  $\Phi = \Phi^{(m)}$  группы  $\mathrm{SO}(3)$ . Оказывается, справедлива теорема о том, что пространство  $H_m$  представления  $\Phi^{(m)}$  неприводимо над  $\mathbb{C}$  и любое неприводимое над  $\mathbb{C}$  представление группы  $\mathrm{SO}(3)$  эквивалентно одному из представлений  $(\Phi^{(m)}, H_m)$  нечётной размерности  $2m + 1$ . Вместо того чтобы доказывать эту теорему, мы, ограничившись

сказанным, обратимся к группе SU(2), где несколько легче получить семейство неприводимых представлений. Ввиду наличия естественного эпиморфизма  $SU(2) \rightarrow SO(3)$  с ядром из матриц  $\pm E$  (см. § 1 из гл. 1) всякое представление  $\Psi$  группы  $SO(3)$  можно считать также представлением  $SU(2)$  (см. доказательство теоремы 5 из § 5), удовлетворяющим так называемому *условию чётности*:  $\Psi_{-e} = \Psi_e$ . При этом, разумеется, будет также выполняться равенство  $\Psi_{-g} = \Psi_g$  для всех  $g \in SU(2)$ . Обратно: при выполнении условия чётности представление  $\Psi$  группы  $SU(2)$  является одновременно представлением группы  $SO(3)$ . Физический смысл имеют и “двузначные” представления  $SO(3)$ , т.е. представления группы  $SU(2)$ , не удовлетворяющие условию чётности. К их числу относится, например, обычное двумерное (спинорное) представление.

Отметим ещё, что любое неприводимое представление группы  $SO(3)$ , отличное от единичного, является точным, как это прямо вытекает из простоты  $SO(3)$  (теорема 3 из § 1 гл. 2).

**Теорема 1.** Пусть  $V_n = \langle x^k y^{n-k} \mid k = 0, 1, \dots, n \rangle_{\mathbb{C}}$  — пространство однородных многочленов степени  $n$  от двух комплексных переменных с действием  $\Psi^{(n)}$  на нём группы  $SU(2)$ , определённым по правилу

$$(\Psi_g^{(n)} f)(x, y) = f(\bar{\alpha}x - \beta y, \bar{\beta}x + \alpha y)$$

для каждого элемента

$$g = \begin{vmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{vmatrix}, \quad |\alpha|^2 + |\beta|^2 = 1.$$

Тогда  $(\Psi^{(n)}, V_n)$  — неприводимое представление группы  $SU(2)$  размерности  $n+1$ . При  $n$  чётном  $(\Psi^{(n)}, V_n)$  является также неприводимым представлением группы  $SO(3)$ .

**Доказательство.** Предположим, что многочлен

$$f(x, y) = \sum_{k=0}^n a_k x^k y^{n-k} \neq 0$$

содержится в некотором инвариантном подпространстве  $U \subset V_n$ . Тогда также

$$\sum_{k=0}^n (e^{-i\varphi})^k a_k x^k y^{n-k} = e^{-in\varphi/2} (\Psi_{b_\varphi}^{(n)} f)(x, y) \in U,$$

где  $b_\varphi$  — элемент из  $SU(2)$  вида (4) из § 1 гл. 1. Так как  $\varphi$  — произвольное вещественное число из интервала  $(0, 2\pi)$ , то можно составить линейную систему с определителем Вандермонда, из которой следует, что

$$f(x, y) \in U \implies x^k y^{n-k} \in U \tag{2}$$

для любого одночлена с коэффициентом  $a_k \neq 0$ . Но если  $x^k y^{n-k} \in U$  для какого-то  $k$ , то и

$$\bar{\alpha}^k \bar{\beta}^{n-k} x^n + \dots + (\bar{\alpha}x - \beta y)^k (\bar{\beta}x + \alpha y)^{n-k} = \Psi_g^{(n)}(x^k y^{n-k}) \in U.$$

Взяв  $g$  с  $\alpha\beta \neq 0$ , мы придём в силу (2) к включению  $x^n \in U$ , которое в свою очередь даёт нам

$$\sum_{s=0}^n \binom{n}{s} \bar{\alpha}^s (-\beta)^{n-s} x^s y^{n-s} \in U.$$

Так как  $\binom{n}{s} \bar{\alpha}^s (-\beta)^{n-s} \neq 0$ , то  $x^s y^{n-s} \in U$ ,  $s = 0, 1, \dots, n$ . Стало быть,  $U = V_n$ , и неприводимость  $(\Psi^{(n)}, V_n)$  доказана.

Далее

$$\Psi_{-e}^{(n)}(x^k y^{n-k}) = (-x)^k (-y^{(n-k)}) = (-1)^n x^k y^{n-k},$$

так что при  $n = 2m$  выполнено условие чётности (см. замечание выше) и  $(\Psi^{(2m)}, V_{2m})$  можно считать неприводимым представлением размерности  $2n+1$ .  $\square$

На самом деле  $\Psi^{(2m)}$  эквивалентно представлению  $\Phi^{(m)}$  группы  $\mathrm{SO}(3)$  на пространстве однородных гармонических многочленов степени  $m$ , но мы на этом не останавливаемся, как и не пытаемся (хотя это возможно) выбрать в  $V_n$  такой базис, чтобы представление  $\Psi^{(n)}$  стало унитарным. Отметим только, заимствуя терминологию из тензорного анализа, что представление  $\Psi^{(n)}$  группы  $\mathrm{SU}(2)$  реализуется также в классе ковариантных симметричных тензоров ранга  $n$ . Полную и достаточно прозрачную теорию представлений компактных групп, включая  $\mathrm{SU}(2)$  и  $\mathrm{SO}(3)$ , обычно развивают в рамках инфинитезимального метода, опирающегося на соответствие между группами и алгебрами Ли. Немного по этому поводу говорилось в гл. 2.

## УПРАЖНЕНИЯ

**1.** Построить  $2m+1$  линейно независимых однородных гармонических многочленов степени  $m$ .

**2.** Показать, что всякий однородный многочлен  $f \in P_m$  записывается в виде линейной комбинации с коэффициентами, зависящими от  $x^2 + y^2 + z^2$ , гармонических многочленов степеней  $m, m-2, m-4, \dots$

**3.** Вывести из упр. 2, что всякая полиномиальная функция  $\tilde{g} : (X, Y, Z) \mapsto g(x, y, z)$  на сфере  $S^2 : x^2 + y^2 + z^2 = 1$  разлагается по сферическим функциям — ограничениям гармонических многочленов на  $S^2$ .

**4.** Показать, не обращаясь к полному описанию неприводимых представлений группы  $\mathrm{SO}(3)$ , что гомоморфизм  $\tau : \mathrm{SO}(3) \rightarrow \mathrm{SU}(2)$  может быть только тривиальным.

## § 7. Тензорное произведение представлений

**1. Контрагredientное представление.** Пусть  $(\Phi, V)$  — представление группы  $G$  над полем  $\mathbb{C}$ . Введём в рассмотрение дуальное пространство  $V^*$  (пространство линейных функций на  $V$ ) и положим

$$(\Phi^*(g)\dot{f})(v) = f(\Phi(g^{-1})v), \quad f \in V^*, \quad v \in V. \quad (1)$$

Линейность оператора  $\Phi^*(g)$  проверяется немедленно. Выберем, далее, в  $V$  и  $V^*$  дуальные базисы:

$$V = \langle e_1, \dots, e_n \rangle, \quad V^* = \langle f_1, \dots, f_n \rangle, \quad f_i(e_j) = \delta_{ij}.$$

Матрица линейного оператора  $\Phi^*(g)$  в базисе  $(f_1, \dots, f_n)$  является транспонированной к матрице оператора  $\Phi(g^{-1})$  в базисе  $(e_1, \dots, e_n)$ :

$$\Phi_g^* = {}^t \Phi_{g^{-1}}. \quad (2)$$

Так как

$$\Phi_{gh}^* = {}^t \Phi_{(gh)^{-1}} = {}^t \Phi_{h^{-1}g^{-1}} = {}^t (\Phi_{h^{-1}} \Phi_{g^{-1}}) = {}^t \Phi_{g^{-1}} {}^t \Phi_{h^{-1}} = \Phi_g^* \Phi_h^*,$$

то соотношением (2) (или (1)) определяется, вообще говоря, новое линейное представление  $(\Phi^*, V^*)$  группы  $G$ ; оно называется представлением, *контрагredientным* (или *дуальным*) к  $(\Phi, V)$ . Необходимость рассмотрения таких представлений возникает каждый раз, когда группу, действующую на векторах (контравариантные тензоры), мы заставляем, как это фактически уже было в § 6, действовать на координатах векторов (ковариантные тензоры). Как нетрудно видеть хотя бы из (2),  $(\Phi^*)^* \approx \Phi$ . Представления, контрагredientные друг к другу, могут и не отличаться или быть эквивалентными. Если, например,  $(\Phi, G)$  — вещественное ортогональное представление, то  $\Phi_g^* = {}^t \Phi_g^{-1} = \Phi_g$ . Но в общем случае представления  $\Phi^*$  и  $\Phi$  не эквивалентны, как показывает простейший пример:

$$C_3 = \langle a \mid a^3 = e \rangle; \quad \Phi(a) = \varepsilon, \quad \Phi^*(a) = \varepsilon^{-1} \quad (\varepsilon^2 + \varepsilon + 1 = 0).$$

Для конечной группы  $G$  точный критерий эквивалентности контрагredientных представлений получается на языке теории характеров. Так как характеристические многочлены матриц  $A$  и  ${}^t A$  совпадают, то из элементарных свойств характеров (предложение из § 4) вытекает, что

$$\chi_{\Phi^*}(g) = \overline{\chi_\Phi(g)}.$$

В частности, представление  $\Phi$  с характером, принимающим только вещественные значения, эквивалентно  $\Phi^*$ . Разумеется, всегда

$$(\chi_{\Phi^*}, \chi_{\Phi^*})_G = (\chi_\Phi, \chi_\Phi)_G,$$

так что  $\Phi^*$ ,  $\Phi$  одновременно приводимы или неприводимы.

**2. Тензорное произведение представлений.** В [ВА II] определено и построено *тензорное произведение*  $T = V \otimes W$  произвольных векторных пространств  $V, W$  над полем  $P$ . Было определено также тензорное произведение

$$\mathcal{A} \otimes \mathcal{B} : V \otimes W \longrightarrow V \otimes W$$

линейных операторов  $\mathcal{A} : V \longrightarrow V$ ,  $\mathcal{B} : W \longrightarrow W$ . Имеется в виду, что

$$(\mathcal{A} \otimes \mathcal{B})(v \otimes w) = \mathcal{A}v \otimes \mathcal{B}w, \quad (3)$$

а далее по линейности

$$(\mathcal{A} \otimes \mathcal{B})\left(\sum_{i,j} v_i \otimes w_j\right) = \sum_{i,j} \mathcal{A}v_i \otimes \mathcal{B}w_j.$$

Отметим непосредственно вытекающие из определения (3) соотношения

$$(\mathcal{A} \otimes \mathcal{B})(\mathcal{C} \otimes \mathcal{D}) = \mathcal{A}\mathcal{C} \otimes \mathcal{B}\mathcal{D},$$

$$(\mathcal{A} + \mathcal{C}) \otimes \mathcal{B} = \mathcal{A} \otimes \mathcal{B} + \mathcal{C} \otimes \mathcal{B},$$

$$\mathcal{A} \otimes (\mathcal{B} + \mathcal{D}) = \mathcal{A} \otimes \mathcal{B} + \mathcal{A} \otimes \mathcal{D},$$

$$C\mathcal{A} \otimes \lambda\mathcal{B} = \lambda\mathcal{A} \otimes \mathcal{B} = \lambda(\mathcal{A} \otimes \mathcal{B}),$$

а также формулу для следа

$$\mathrm{tr} \mathcal{A} \otimes \mathcal{B} = \mathrm{tr} \mathcal{A} \cdot \mathrm{tr} \mathcal{B}. \quad (4)$$

Пусть теперь  $(\Phi, V)$ ,  $(\Psi, W)$  — два линейных представления группы  $G$  с характерами  $\chi_\Phi$  и  $\chi_\Psi$  соответственно. Определим естественным образом представление  $(\Phi \otimes \Psi, V \otimes W)$ , полагая

$$(\Phi \otimes \Psi)(g) = \Phi(g) \otimes \Psi(g) \quad \forall g \in G.$$

Из общих свойств тензорного произведения линейных операторов и из формулы (4) вытекает, что отображение  $\Phi \otimes \Psi$  будет действительно задавать представление группы  $G$  с пространством представления  $V \otimes W$  и с характером

$$\chi_{\Phi \otimes \Psi} = \chi_\Phi \chi_\Psi. \quad (5)$$

Будем говорить, что  $(\Phi \otimes \Psi, V \otimes W)$  — *тензорное произведение представлений*  $(\Phi, V)$  и  $(\Psi, W)$ . При  $\Psi = \Phi, W = V$  говорят также о *тензорном квадрате*. В правой части формулы (5) стоит обычное поточечное произведение центральных функций  $\chi_\Phi$  и  $\chi_\Psi$ .

Совершенно очевидно, что если  $U$  —  $G$ -инвариантное подпространство в  $V$ , то и  $U \otimes W$  будет  $G$ -инвариантным подпространством в  $V \otimes W$ . Аналогичное замечание относится к  $G$ -инвариантным подпространствам в  $W$ . Но из неприводимости  $V$  и  $W$  вовсе не следует неприводимость  $V \otimes W$ , как показывает пример тензорного квадрата  $\Phi^{(3)} \otimes \Phi^{(3)}$  двумерного представления группы  $S_3$  (см. таблицу в

п. 2 § 5). В самом деле,  $\dim_{\mathbb{C}} \Phi^{(3)} \otimes \Phi^{(3)} = 4$ , а максимальная степень неприводимого представления группы  $S_3$  равна 2.

Задача эффективного описания неприводимых представлений, содержащихся в  $\Phi \otimes \Psi$  и, более общо, в тензорном произведении

$$\Phi^{(1)} \otimes \Phi^{(2)} \otimes \dots \otimes \Phi^{(p)}$$

нескольких линейных представлений, имеет принципиальное значение, поскольку многие важные и весьма естественные представления групп возникают как тензорные произведения. Именно с этой точки зрения нужно смотреть на представления групп  $SU(2)$  и  $SO(3)$  (см. § 6), а также на примеры 3 и 4 из п. 2 § 1. Инвариантные подпространства симметричных и кососимметричных ковариантных (или контравариантных) тензоров постоянно встречаются в различных геометрических приложениях. Рассматриваемая задача привлекательна в особенности тогда, когда справедлива теорема о полной приводимости представлений.

**3. Кольцо характеров.** Для простоты ограничимся случаем конечной группы  $G$  и поля  $\mathbb{C}$ . Пусть  $\Phi^{(1)}, \Phi^{(2)}, \dots, \Phi^{(r)}$  — полное множество попарно неэквивалентных неприводимых представлений группы  $G$  над  $\mathbb{C}$  и  $\chi_1, \chi_2, \dots, \chi_r$  — соответствующие им характеристики ( $r$  — число классов сопряжённых элементов в  $G$ ). Нам известно, что

$$\Phi \otimes \Psi \approx m_1 \Phi^{(1)} + \dots + m_r \Phi^{(r)},$$

где кратности  $m_i$  зависят только от  $\Phi$  и  $\Psi$ . По формуле (5)

$$\chi_{\Phi} \chi_{\Psi} = m_1 \chi_1 + \dots + m_r \chi_r.$$

Пусть  $X_{\mathbb{Z}}(G)$  — множество всевозможных целочисленных линейных комбинаций характеристик  $\chi_1, \dots, \chi_r$ . Мы доказали ранее, что  $(\chi_1, \dots, \chi_r)$  — ортонормированный базис пространства  $X_{\mathbb{C}}(G)$ , поэтому  $X_{\mathbb{Z}}(G) \subset X_{\mathbb{C}}(G)$  является во всяком случае свободной абелевой группой  $\cong \mathbb{Z}^r$  с образующими  $\chi_1, \dots, \chi_r$ . Её элементы называются *обобщёнными характеристиками* группы  $G$ . Истинными характеристиками будут лишь комбинации  $\sum m_i \chi_i$  с  $m_i \geq 0$ .

Из предыдущих рассуждений видно, что тензорное произведение представлений индуцирует на  $X_{\mathbb{Z}}(G)$  бинарную алгебраическую операцию — коммутативную, ассоциативную, подчиняющуюся законам дистрибутивности. Короче говоря, справедлива

*Теорема 1. Обобщённые характеристики образуют коммутативное ассоциативное кольцо  $X_{\mathbb{Z}}(G)$  с единицей — единичным характером  $\chi_1$ .*

В свою очередь  $X_{\mathbb{C}}(G)$  — коммутативная ассоциативная алгебра размерности  $r$  над  $\mathbb{C}$ . Строение кольца  $X_{\mathbb{Z}}(G)$  (алгебры  $X_{\mathbb{C}}(G)$ ) полностью определяется *структурными константами* — целыми чис-

лами  $m_{ij}^k$  из соотношений

$$\chi_i \chi_j = \sum_k m_{ij}^k \chi_k. \quad (6)$$

В частности, равенства  $m_{ij}^k = m_{ji}^k$ ,  $m_{1j}^k = \delta_{kj}$  отражают свойства коммутативности  $X_{\mathbb{Z}}(G)$  и единичности  $\chi_1$ . Согласно (6)

$$\chi_i(g) \chi_j(g) = \sum_k m_{ij}^k \chi_k(g) \quad \forall g \in G.$$

Умножив обе части этого соотношения на  $\frac{1}{|G|} \overline{\chi_s(g)}$ , просуммировав по  $g \in G$  и воспользовавшись первым соотношением ортогональности для характеров, получим

$$m_{ij}^s = \frac{1}{|G|} \sum_{g \in G} \chi_i(g) \chi_j(g) \overline{\chi_s(g)}. \quad (7)$$

Таким образом, структурные константы выражаются в терминах самих характеров.

Из (7) можно извлечь одно несложное утверждение. Именно,

$$\begin{aligned} m_{ij}^1 &= \frac{1}{|G|} \sum_g \chi_i(g) \chi_j(g) \overline{\chi_1(g)} = \frac{1}{|G|} \sum_g \chi_i(g) \chi_j(g) = \\ &= \frac{1}{|G|} \sum_g \chi_i(g) \overline{\chi_j(g)} = (\chi_i, \chi_j^*)_G, \end{aligned}$$

где  $\chi_j^* = \chi_{\Psi}$ ,  $\Psi = \Phi^{(j)*}$  — характер представления, контрагредиентного к  $\Phi^{(j)}$  (см. п. 1). Таким образом, *единичное представление* *входит в качестве компоненты в разложение*  $\Phi^{(i)} \otimes \Phi^{(j)}$  *тогда и только тогда, когда*  $\Phi^{(i)}$  *эквивалентно представлению*  $\Phi^{(j')} = \Phi^{(j)*}$  (в противном случае  $m_{ij}^1 = (\chi_i, \chi_j^*)_G = 0$ ). Отметим ещё, что *тензорное произведение одномерного представления*  $\Phi^{(i)}$  *и произвольного неприводимого представления*  $\Phi^{(j)}$  *всегда является неприводимым представлением той же размерности, что и*  $\Phi^{(j)}$ . Это довольно понятно без всяких объяснений, а формально вытекает из критерия неприводимости характеров. Если

$$\chi = \chi_{\Phi^{(i)} \otimes \Phi^{(j)}} = \chi_i \chi_j,$$

то  $\chi_i(g)$  — комплексный корень некоторой степени из 1 и  $\chi_i(g) \overline{\chi_i(g)} = 1$ , а поэтому

$$\begin{aligned} (\chi, \chi)_G &= \frac{1}{|G|} \sum_g \chi_i(g) \chi_j(g) \overline{\chi_i(g) \chi_j(g)} = \\ &= \frac{1}{|G|} \sum_g \chi_j(g) \overline{\chi_j(g)} = (\chi_j, \chi_j)_G = 1. \end{aligned}$$

Пример 1.  $G = S_3$  (см. таблицы в п. 1 из § 2 и в п. 2 из § 5):

$$\Phi^{(1)} \otimes \Phi^{(3)} \approx \Phi^{(2)} \otimes \Phi^{(3)} \approx \Phi^{(3)}.$$

Пример 2.  $G = S_4$  (см. пример 3 из п. 4 § 5):

$$\Phi^{(2)} \otimes \Phi^{(4)} \approx \Phi^{(5)}, \quad \Phi^{(2)} \otimes \Phi^{(5)} \approx \Phi^{(4)}.$$

Наконец, докажем следующую любопытную теорему, служащую обобщением теоремы 2 из § 5 о разложении регулярного представления.

**Теорема 2.** *Пусть  $\chi = \chi_\Phi$  — характер точного представления  $(\Phi, V)$  конечной группы  $G$  над полем комплексных чисел  $\mathbb{C}$ , принимающий на  $G$  ровно  $m$  различных значений.*

*Тогда каждый неприводимый характер  $\chi_k$  входит с ненулевым коэффициентом в разложение хотя бы одного характера  $\chi^0 = \chi_1, \chi, \chi^2, \dots, \chi^{m-1}$ . Другими словами, всякое неприводимое представление содержится в разложении некоторой тензорной степени  $\Phi^{\otimes i} = \Phi \otimes \dots \otimes \Phi$ ,  $0 \leq i \leq m-1$ , любого точного представления  $\Phi$ .*

**Доказательство.** Пусть  $\omega_j = \chi(g_j)$ ,  $j = 0, 1, \dots, m-1$ , — различные значения, принимаемые характером  $\chi$  на  $G$ , причём  $\omega_0 = \deg \Phi$ . Пусть, далее,

$$G_j = \{g \in G \mid \chi(g) = \chi(g_j) = \omega_j\}.$$

Ввиду точности представления  $\Phi$  имеем

$$G_0 = \text{Ker } \Phi = \{e\}.$$

Пусть  $\chi_k$  — неприводимый характер группы  $G$ , не входящий в разложение ни одного из характеров  $\chi^i$ . Тогда

$$\begin{aligned} 0 &= |G|(\chi^i, \chi_k)_G = \\ &= \sum_{j=0}^{m-1} (\chi(g_j))^i \sum_{g \in G_j} \overline{\chi_k(g)} = \sum \omega_j^i T_j, \quad 0 \leq i \leq m-1, \end{aligned}$$

— однородная система линейных уравнений относительно

$$T_j = \sum_{g \in G_j} \overline{\chi_k(g)}$$

с определителем

$$\det(\omega_j^i) = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \omega_0 & \omega_1 & \dots & \omega_{m-1} \\ \dots & \dots & \dots & \dots \\ \omega_0^{m-1} & \omega_1^{m-1} & \dots & \omega_{m-1}^{m-1} \end{vmatrix},$$

отличным от нуля (определитель Вандермонда). Таким образом,  $T_j = 0$ ,  $j = 0, 1, \dots, m-1$ , т.е.

$$\sum_{g \in G_j} \chi_k(g^{-1}) = 0, \quad j = 0, 1, \dots, m-1.$$

В частности,

$$0 = \sum_{g \in G_0} \chi_k(g^{-1}) = \chi_k(e)$$

— противоречие, доказывающее теорему.  $\square$

В случае регулярного представления  $\rho$ , очевидно,  $m = 2$ .

**4. Инварианты линейных групп.** *Линейной группой степени  $n$  мы, как обычно, называем любую подгруппу в  $\mathrm{GL}(n, P)$ , где  $P$  — некоторое поле. В дальнейшем можно считать  $P = \mathbb{R}$  или  $P = \mathbb{C}$ . Если  $G$  — абстрактная группа и  $\Phi : G \rightarrow \mathrm{GL}(n, \mathbb{C})$  — её линейное представление, то пару  $(G, \Phi)$  мы тоже будем называть линейной группой. Линейные преобразования  $\Phi_g$  действуют на столбцы переменных  $x_1, \dots, x_n$ :*

$$\left\| \begin{array}{c} \Phi_g(x_1) \\ \vdots \\ \Phi_g(x_n) \end{array} \right\| = \Phi_g \left\| \begin{array}{c} x_1 \\ \vdots \\ x_n \end{array} \right\|.$$

Они переводят любую форму (однородный многочлен)  $f$  степени  $m$  снова в форму степени  $m$ :

$$(\tilde{\Phi}_g f)(x_1, \dots, x_n) = f(\Phi_g^{-1}(x_1), \dots, \Phi_g^{-1}(x_n)).$$

Различные частные случаи этого действия нам уже встречались (см. § 6). Отображение  $\tilde{\Phi}$  определяет представление группы  $G$  на пространстве  $P_m$  форм над  $\mathbb{C}$  степени  $m$  (или ковариантных симметричных тензоров ранга  $m$ ).

**Определение.** Форма  $f \in P_m$ , остающаяся неподвижной при действии  $\tilde{\Phi}_g$  (т.е.  $\tilde{\Phi}_g f = f \quad \forall g \in G$ ), называется (*целым*) *инвариантом* степени  $m$  линейной группы  $(G, \Phi)$ .

На самом деле нужно было бы брать остающийся на месте при действии  $\tilde{\Phi}(G)$  многочлен от коэффициентов “общей” формы степени  $m$ . Так поступают в общей теории инвариантов, но мы для простоты ограничимся данным определением. Если в качестве  $f$  взять рациональную функцию, то можно прийти к понятию *рационального инварианта*. Важным является также понятие *относительного инварианта*  $f$ , когда

$$\tilde{\Phi}_g f = \omega_g f,$$

где  $\omega_g \in \mathbb{C}$  — множитель, зависящий от элемента  $g \in G$ .

Ясно, что любое множество  $\{f_1, f_2, \dots\}$  инвариантов линейной группы  $(G, \Phi)$  порождает в  $\mathbb{C}[x_1, \dots, x_n]$  подкольцо  $\mathbb{C}[f_1, f_2, \dots]$  инвариантов.

Рассмотрим небольшое число примеров.

Пример 3. Квадратичная форма  $x_1^2 + x_2^2 + \dots + x_n^2$  и любые многочлены от неё являются целыми инвариантами ортогональной группы  $O(n)$ .

Пример 4. Элементарные симметрические многочлены  $s_1(x_1, \dots, x_n), \dots, s_n(x_1, \dots, x_n)$  являются целыми инвариантами симметрической группы  $S_n$ , рассматриваемой вместе с каноническим мономорфизмом  $\Phi: S_n \rightarrow \mathrm{GL}(n, \mathbb{R})$ . Основная теорема о симметрических многочленах утверждает, что инварианты  $s_1, \dots, s_n$  степеней  $1, 2, \dots, n$  алгебраически независимы, а полиномиальными (рациональными) функциями от них исчерпываются все целые (рациональные) инварианты группы  $(S_n, \Phi)$ .

Относительными инвариантами линейной группы  $(S_n, \Phi)$  служат кососимметрические многочлены:  $\Phi_\pi f = (\det \Phi_\pi)f = \epsilon_\pi f$ . Мы видели [ВА I, гл. 6, § 2, упр. 4], что любой кососимметрический многочлен  $f$  имеет вид  $f = \Delta_n \cdot g$ , где  $\Delta_n = \prod_{j < i} (x_i - x_j)$ , а  $g$  — произвольный симметрический многочлен, т. е. абсолютный инвариант.

Пример 5. Представлению  $\Phi_A: X \mapsto AXA^{-1}$  степени  $n^2$  полной линейной группы  $\mathrm{GL}(n, K)$  с пространством представления  $M_n(K)$  (см. пример 3 из § 1) отвечает система из  $n$  алгебраически независимых инвариантов — коэффициентов характеристического многочлена матрицы  $X = (x_{ij})$ . К ним относятся, в частности, хорошо известные нам инварианты  $\mathrm{tr} X = \sum_i x_{ii}$  и  $\det X$ .

Пример 6. На квадратичную форму

$$f(x_1, \dots, x_n) = \sum a_{ij} x_i x_j,$$

записанную в виде

$$f(x_1, \dots, x_n) = {}^t X A X, \quad ; A = (a_{ij}) = {}^t A, \quad X = [x_1, \dots, x_n],$$

действует ортогональная группа  $O(n)$ :

$$\begin{aligned} C \in O(n) \implies (C^{-1}f)(x_1, \dots, x_n) &= {}^t(CX) A (CX) = \\ &= {}^t X {}^t C A C X = {}^t X (C^{-1} A C) X. \end{aligned}$$

В этом случае принято говорить об инвариантах квадратичной формы  $f$  относительно  $O(n)$ :  $\mathrm{tr} A, \dots, \det A$ . Для бинарной квадратичной формы  $ax^2 + 2bxy + cy^2$  инварианты  $a + c$  и  $ac - b^2$ , характеризующие метрически различные классы кривых второго порядка, известны ещё из курса аналитической геометрии.

Пример 7. Симметрическую группу  $S_3$  рассмотрим как линейную группу степени 2, используя представление  $\Gamma$ , эквивалентное представлению  $\Phi^{(3)}$  из таблицы в конце п. 1 § 2:

$$\begin{aligned} \Gamma_{(1\ 2\ 3)} &= \begin{vmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{vmatrix}, \quad \Gamma_{(23)} = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}, \\ \varepsilon^2 + \varepsilon + 1 &= 0. \end{aligned}$$

Эквивалентность осуществляется посредством сопряжения

$$\begin{vmatrix} \varepsilon & 0 \\ 0 & 1 \end{vmatrix} \left\| \Phi_\sigma^{(3)} \right\| \begin{vmatrix} \varepsilon^{-1} & 0 \\ 0 & 1 \end{vmatrix} = \Gamma_\sigma.$$

Пусть  $u, v$  — независимые переменные, линейно преобразующиеся посредством  $\Gamma_\sigma$ :

$$\begin{aligned} \Gamma_{(1\ 2\ 3)}(u) &= \varepsilon u, \quad \Gamma_{(1\ 2\ 3)}(v) = \varepsilon^{-1} v; \\ \Gamma_{(2\ 3)}(u) &= v, \quad \Gamma_{(2\ 3)}(v) = u. \end{aligned}$$

Так как

$$\tilde{\Gamma}_{(1\ 2\ 3)}(uv) = \Gamma_{(1\ 2\ 3)}^{-1}(u)\Gamma_{(1\ 2\ 3)}^{-1}(v) = \varepsilon^{-1}u \cdot \varepsilon v = uv,$$

$$\tilde{\Gamma}_{(2\ 3)}(uv) = vu = uv,$$

$$\tilde{\Gamma}_{(1\ 2\ 3)}(u^3 + v^3) = (\varepsilon^{-1}u)^3 + (\varepsilon v)^3 = u^3 + v^3,$$

$$\tilde{\Gamma}_{(2\ 3)}(u^3 + v^3) = v^3 + u^3 = u^3 + v^3,$$

то группа  $(S_3, \Gamma)$  имеет формы

$$I_1 = uv, \quad I_2 = u^3 + v^3 \quad (7)$$

степеней 2 и 3 в качестве своих инвариантов.

Далее, группа  $S_3$  действует естественным образом на многочленах  $f(x_1, x_2, x_3)$  от трёх независимых переменных:

$$(\sigma f)(x_1, x_2, x_3) = f(x_{\sigma 1}, x_{\sigma 2}, x_{\sigma 3}).$$

Положив

$$\begin{aligned} u &= x_1 + \varepsilon^2 x_2 + \varepsilon x_3, \\ v &= x_1 + \varepsilon x_2 + \varepsilon^2 x_3, \end{aligned} \quad (8)$$

мы увидим, что

$$\Gamma_\sigma(u) = x_{\sigma 1} + \varepsilon^2 x_{\sigma 2} + \varepsilon x_{\sigma 3}.$$

В частности,

$$\Gamma_{(1\ 2\ 3)}(u) = x_2 + \varepsilon^2 x_3 + \varepsilon x_1 = \varepsilon u,$$

$$\Gamma_{(23)}(u) = x_1 + \varepsilon^2 x_3 + \varepsilon x_2 = v,$$

$$\Gamma_{(1\ 2\ 3)}(v) = x_2 + \varepsilon x_3 + \varepsilon^2 x_1 = \varepsilon^{-1} v,$$

$$\Gamma_{(23)}(v) = x_1 + \varepsilon x_3 + \varepsilon^2 x_2 = u,$$

т.е. действия  $\Gamma_\sigma$  на  $u, v$  и  $\sigma$  на  $x_1, x_2, x_3$  согласованы. При подстановке (8) в инварианты (7) последние перейдут в симметрические функции от  $x_1, x_2, x_3$ , которые по теореме 1 из [ВА I, гл. 6, § 2] можно выразить через элементарные симметрические функции  $s_i = s_i(x_1, x_2, x_3)$ . Небольшое упражнение показывает, что

$$I_1 = x_1^2 + x_2^2 + x_3^2 + (\varepsilon + \varepsilon^2)(x_1 x_2 + x_1 x_3 + x_2 x_3) = s_1^2 - 3s_2,$$

$$\begin{aligned} I_2 &= 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1^2 x_2 + x_1^2 x_3 + x_1 x_2^2 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2) + 12 x_1 x_2 x_3 = \\ &= 2s_1^3 - 9s_1 s_2 + 27s_3. \end{aligned}$$

Специализируем значения  $I_1, I_2$ , взяв за  $x_1, x_2, x_3$  три корня неполного кубического уравнения

$$x^3 + px + q = 0.$$

Тогда  $s_1 = 0, s_2 = p, s_3 = -q$ , и, следовательно,

$$I_1 = -3p, \quad I_2 = -27q. \quad (9)$$

Но из (7) следует, что

$$v = \frac{I_1}{u}, \quad I_2 = u^3 + \frac{I_1^3}{u^3}, \quad u = \sqrt[3]{\frac{I_2}{2} \pm \sqrt{\frac{I_2^2}{4} - I_1^3}}.$$

Все радикалы выбираются такими, что после подстановки значений (9) получатся формулы

$$\begin{aligned} u &= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}, \\ v &= \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}, \\ uv &= -3p, \end{aligned}$$

с величиной  $D = -4p^3 - 27q^2$  — дискриминантом нашего кубического уравнения (см. в [ВА I, гл. 6, § 2, формулу (16)]). Так как  $u$  и  $v$  теперь известны, то из линейной системы

$$\begin{aligned} x_1 + \varepsilon^2 x_2 + \varepsilon x_3 &= u, \\ x_1 + \varepsilon x_2 + \varepsilon^2 x_3 &= v, \\ x_1 + x_2 + x_3 &= 0 \end{aligned}$$

находятся сами корни. Мы пришли довольно естественным путём к формулам Кардано, о которых упоминалось в [ВА I, гл. 1, § 2, задача 1].

Последний пример не случайно устанавливает связь между инвариантами группы  $S_3$ , являющейся группой Галуа общего кубического уравнения, и формулами Кардано. Теория Галуа в значительной мере связана с изучением инвариантов полей (и соответствующих им групп), порождённых корнями алгебраических уравнений.

Отметим некоторые факты, относящиеся к системе образующих кольца инвариантов. Пусть  $w$  — произвольная форма от  $n$  независимых переменных  $x_1, \dots, x_n$ . Конечная группа  $G$  с линейным представлением  $\Phi$  степени  $n$  действует как группа перестановок на множестве

$$\Omega = \{\bar{\Phi}_g(w) \mid g \in G\}.$$

Ясно, что любая однородная симметрическая функция  $|G|$  элементов из  $\Omega$  (или, возможно, некоторого делителя числа  $|G|$ ) будет инвариантом линейной группы  $(G, \Phi)$ . Если теперь взять в качестве  $w$  переменную  $x_i$ , то  $x_i$  будет корнем алгебраического уравнения

$$\prod_{g \in G} (X - \Phi_g(x_i)) = 0,$$

коэффициенты которого являются инвариантами группы  $(G, \Phi)$ . Таким образом, каждая переменная  $x_i$  является (алгебраической) функцией инвариантов. Если бы алгебраически независимых инвариантов было меньше, чем  $n$ , то мы выразили бы  $x_1, \dots, x_n$  через меньшее число алгебраически независимых переменных, а это невозможно. Следовательно, мы доказали (если можно назвать доказательством столь смелое обращение с алгебраической зависимостью величин) одну из важных теорем теории инвариантов.

**Теорема 3.** *Конечная линейная группа степени  $n$  всегда обладает системой из  $n$  алгебраически независимых инвариантов.*

Для группы  $(S_3, \Gamma)$  такими инвариантами являются формы (7).

Можно было бы дополнить теорему 3 утверждением о том, что всё кольцо целых инвариантов конечной группы степени  $n$  порождается  $n$  алгебраически независимыми инвариантами  $f_1, f_2, \dots, f_n$  и, как правило, ещё одним инвариантом  $f_{n+1}$  (являющимся алгебраической функцией первых  $n$  инвариантов). Другими словами, все остальные инварианты являются многочленами от  $f_1, \dots, f_n, f_{n+1}$ . Этот факт справедлив для многих других линейных групп, как дискретных, так и непрерывных.

Общая теория инвариантов, развитая в середине XIX века трудами Кэли, Сильвестра, Якоби, Эрмита, Клебша, Гордана и других, а затем испытавшая второе рождение в нескольких фундаментальных работах Д. Гильберта, в наши дни стала частью алгебраической геометрии и теории алгебраических групп. Постоянный интерес к теории инвариантов обусловлен также широкими возможностями её применений во многих областях механики и физики.

### УПРАЖНЕНИЯ

1. При помощи формулы (6) и таблиц из п. 1 § 2, п. 2 § 5, п. 4 § 5 проверить, что справедливы разложения

$$\Phi^{(3)} \otimes \Phi^{(3)} \approx \Phi^{(1)} + \Phi^{(2)} + \Phi^{(3)}$$

для тензорного квадрата двумерного представления  $\Phi^{(3)}$  симметрической группы  $S_3$  и

$$\Phi^{(5)} \otimes \Phi^{(5)} \approx \Phi^{(1)} + \Phi^{(2)} + \Phi^{(3)} + \Phi^{(4)}$$

для тензорного квадрата двумерного представления  $\Phi^{(5)}$  группы кватернионов  $Q_8$ .

2. *Представления прямого произведения групп.* Пусть имеются две группы  $G, H$  с линейными представлениями  $(\Phi, V), (\Psi, W)$ . Тогда, полагая

$$(\Phi \otimes \Psi)(g \cdot h) = \Phi(g) \otimes \Psi(h),$$

где  $g \cdot h$  — элемент прямого произведения  $G \times H$  групп  $G, H$ , мы заставим  $G \times H$  действовать на тензорном произведении  $V \otimes_C W$ ; как обычно,

$$(\Phi(g) \otimes \Psi(h))(v \otimes w) = \Phi(g)v \otimes \Psi(h)w.$$

Проверить, что так определённое отображение

$$\Phi \otimes \Psi: G \times H \longrightarrow \mathrm{GL}(V \otimes W)$$

является представлением группы  $G \times H$  с характером  $\chi_{\Phi \otimes \Psi} = \chi_{\Phi} \chi_{\Psi}$ . Доказать следующее утверждение. Пусть  $\Phi^{(1)}, \dots, \Phi^{(r)}$  (соответственно  $\Psi^{(1)}, \dots, \Psi^{(s)}$ ) — все неприводимые представления группы  $G$  (соответственно  $H$ ). Тогда представления  $\Phi^{(i)} \otimes \Psi^{(j)}$  группы  $G \times H$  неприводимы, и все неприводимые представления группы  $G \times H$  исчерпываются представлениями

$$\Phi^{(i)} \otimes \Psi^{(j)}, \quad 1 \leq i \leq r, \quad 1 \leq j \leq s.$$

**3.** Формы  $xy, x^n + y^n$  являются инвариантами двумерной линейной группы диэдра

$$(D_n, \Phi) = \left\langle \begin{array}{cc} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{array} \right\rangle, \quad \left\langle \begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right\rangle,$$

$$\varepsilon^n = 1$$

(см. упр. 9 из § 5). Показать, что любой другой (целый) инвариант группы  $(D_n, \Phi)$  имеет вид многочлена от  $xy, x^n + y^n$ .

**4.** Проверить, что группа кватернионов, рассматриваемая в своём двумерном неприводимом представлении, не обладает квадратичными и кубическими инвариантами. Что можно сказать о формах  $x^2y^2, x^4 + y^4$ ?

## Глава 4

# КОЛЬЦА. АЛГЕБРЫ. МОДУЛИ

---

Повторное рассмотрение алгебраических структур, уже изучавшихся ранее, мотивируется следующими соображениями. Во-первых, хотелось бы в какой-то мере пополнить содержательными утверждениями наши сведения о полях и кольцах, опираясь, где это необходимо, на солидную теоретико-групповую базу. Во-вторых, результаты главы 3 о представлениях групп естественным образом включаются в общую теорию модулей над кольцами, и было бы жаль не упомянуть об этом хотя бы в краткой форме. Фундаментальное понятие модуля важно само по себе и достойно изучения гораздо более широком аспекте, но для этого читателю рекомендуется обратиться к другим источникам.

## § 1. Теоретико-кольцевые конструкции

**1. Идеалы колец и факторкольца.** Кольца классов вычетов и гомоморфизмы колец, рассмотренные в [ВА I, гл. 4, § 3], подготовили достаточно благоприятную почву для введения общих понятий. Напомним, что *ядром* гомоморфизма

$$f : (K, +, \cdot) \longrightarrow (K', \oplus, \odot)$$

называется подкольцо  $\text{Ker } f = \{a \in K \mid f(a) = 0'\} \subset K$ . Непосредственно видно, что это отнюдь не произвольное подкольцо. Действительно, если  $J = \text{Ker } f \subset K$ , то  $J \cdot x \subseteq J$  (поскольку  $f(zx) = f(z) \odot f(x) = 0' \odot f(x) = 0'$  для всех  $z \in J$ ) и  $x \cdot J \subseteq J$  для всех  $x \in K$ . Стало быть,  $JK \subset J$  и  $KJ \subset J$ . Подкольцо  $J$ , обладающее этими свойствами, называется (*двусторонним*) идеалом кольца  $K$ . Итак, ядра гомоморфизмов всегда являются идеалами.

Пример  $m\mathbb{Z} \subset \mathbb{Z}$  подсказывает способ построения идеалов (возможно, не всех) в произвольном коммутативном кольце  $K$ : если  $a$  — какой-то элемент из  $K$ , то множество  $aK$  всегда является идеалом в  $K$ . Действительно,

$$ax + ay = a(x + y), \quad (ax)y = a(xy).$$

Говорят, что  $aK$  — *главный идеал*, порождённый элементом  $a \in K$ .

Если брать кольца только с единицей, то идеалами будут подгруппы аддитивной группы кольца, выдерживающие умножение слева и справа на элементы кольца, а в определение гомоморфизма  $f : K \rightarrow K'$  целесообразно внести условие  $f(1) = 1'$ . При эпиморфизме это условие, конечно, автоматически выполняется.

Нормальные подгруппы групп, введённые в гл. 1, и идеалы колец имеют общее происхождение — они являются ядрами гомоморфизмов. Это обстоятельство находит своё выражение и в общности конструкции факторобразований, на чём мы собираемся вкратце остановиться.

При построении *факторкольца*  $K/J$  кольца  $K$  по идеалу  $J$  будем исходить из того, что “основу” кольца составляет аддитивная абелева группа. Поэтому за элементы из  $K/J$  следует брать смежные классы  $a + J$  (называемые *классами вычетов по модулю идеала*  $J$ ), сложение которых осуществляется по обычному правилу:

$$\begin{aligned} (a + J) \oplus (b + J) &= (a + b) + J, \\ \ominus (a + J) &= -a + J. \end{aligned} \tag{1}$$

В качестве произведения тех же классов берём

$$(a + J) \odot (b + J) = ab + J. \tag{2}$$

Необходима уверенность в том, что это умножение определено правильно, т.е. не зависит от выбора представителей соответствующих классов. Пусть  $a' = a + x$ ,  $b' = b + y$ , где  $x, y \in J$ . Тогда

$$a'b' = ab + ay + xb' = ab + z,$$

где  $z = ay + xb' \in J$ , поскольку  $J$  — двусторонний идеал. Поэтому  $a'b'$  лежит в одном смежном классе с элементом  $ab$ , а это и значит, что произведение (2) определено правильно. Для краткости положим  $\bar{a} = a + L$ , так что

$$\bar{a} \oplus \bar{b} = \overline{a + b}, \quad \bar{a} \odot \bar{b} = \overline{ab}.$$

В частности,  $\bar{0} = J$  и  $\bar{1} = 1 + J$  (если единица 1 имеется в  $K$ ). Нужно ещё убедиться, что для множества  $\bar{K} = K/J = \{\bar{a} \mid a \in K\}$ , рассматриваемого с операциями  $\oplus, \odot$ , выполнены все аксиомы кольца, но это довольно очевидно, поскольку операции над классами вычетов в  $\bar{K}$  сводятся к операциям над элементами из  $K$ . Скажем, дистрибутивность проверяется так:

$$(\bar{a} \oplus \bar{b}) \odot \bar{c} = \overline{(a + b)c} = \overline{(ac + bc)} = \overline{ac} \oplus \overline{bc} = \bar{a} \odot \bar{c} \oplus \bar{b} \odot \bar{c}.$$

Всё это показывает, что отображение

$$\pi : a \mapsto \bar{a}$$

является эпиморфизмом колец  $K \rightarrow \bar{K}$  с ядром  $\text{Кер } \pi = J$ . От частного примера факторкольца  $Z_m = \mathbb{Z}/m\mathbb{Z}$  и эпиморфизма  $\mathbb{Z} \rightarrow Z_m$  мы перешли к рассмотрению ситуации в произвольных кольцах.

Отметим теперь, что все гомоморфные образы кольца  $K$  исчерпываются по существу факторкольцами  $K$  по соответствующим идеалам. Действительно, если  $f : K \rightarrow K'$  — гомоморфизм и

$f(K)$  — образ кольца  $K$  относительно  $f$ , то, рассматривая  $f(K) \subset K'$  вместо  $K'$ , мы придём к эпиморфизму. Чтобы не усложнять обозначений, считаем с самого начала  $f$  эпиморфизмом, т.е. полагаем  $f(K) = K'$ . Согласно общему принципу, изложенному в [ВА I, гл. 1],  $f$  определяет отношение эквивалентности  $O_f$  на  $K$ ; в данном случае  $O_f$  задаётся разбиением  $K$  на смежные классы  $a + \text{Ker } f = C_a$ . Отображение  $f$  устанавливает биективное соответствие  $f'$  между элементами  $a' \in K'$  и классами  $C_a$ , а именно  $f'(C_a) = a'$ , если  $a' = f(a)$ . При этом

$$f'(C_a + C_b) = f'(C_{a+b}) = f(a+b) = f(a) + f(b) = f'(C_a) + f'(C_b),$$

$$f'(C_a \cdot C_b) = f'(C_{ab}) = f(ab) = f(a) \cdot f(b) = f'(C_a) \cdot f'(C_b),$$

так что биективное отображение  $f'$  — изоморфизм (для простоты операции сложения и умножения в  $K$ , в кольце классов вычетов  $K/\text{Ker } f$  и в  $K'$  обозначаются одинаково:  $+$  и  $\cdot$ ).

По сути дела нами доказана

**Теорема 1** (основная теорема о гомоморфизмах). *Любой идеал  $J$  кольца  $K$  определяет (при помощи формул (1), (2)) структуру кольца на фактормножестве  $K/J$ , причём  $K/J$  является гомоморфным образом кольца  $K$  с ядром  $J$ . Обратно: каждый гомоморфный образ  $K' = f(K)$  кольца  $K$  изоморчен факторкольцу  $K/\text{Ker } f$ .*

**Замечание.** Правая часть формулы (2), вообще говоря, не совпадает с произведением классов вычетов  $a + J$  и  $b + J$  в теоретико-множественном смысле. Например, при  $K = \mathbb{Z}$ ,  $J = 8\mathbb{Z}$  целое число  $24 \in 16 + 8\mathbb{Z}$  не содержится в  $(4 + 8\mathbb{Z})^2$ , поскольку  $(4+8s)(4+8t) = 16u$ .

Мы знаем, что  $Z_m = \mathbb{Z}/m\mathbb{Z}$  — поле тогда и только тогда, когда  $m = p$  — простое число. Евклидовость кольца  $\mathbb{Z}$  и кольца многочленов  $P[X]$  над полем  $P$  является причиной их большого сходства.

**2. Поле разложения многочлена.** Как часто бывает, взгляд со стороны на хорошо известный пример даёт возможность лучше понять его и перейти к разумным обобщениям.

**Теорема 2.** *Справедливы следующие утверждения:*

- i) *всякий идеал  $J$  кольца многочленов  $P[X]$  над полем  $P$  главный, т.е.  $J = (f(X)) := f(X)P[X]$  для некоторого многочлена  $f$ ;*
- ii) *факторкольцо  $P[X]/(f(X))$  является полем тогда и только тогда, когда  $f$  — неприводимый над  $P$  многочлен.*

**Доказательство.** i) Выберем в  $J$  многочлен  $f$  минимальной степени. Если  $g$  — любой многочлен из  $J$ , то деление с остатком на  $f$  ( $P$  — поле, поэтому нет нужды заботиться об обратимости старшего коэффициента у  $g(X)$ ) даст нам равенство  $g = qf + r$ ,  $\deg r < \deg f$ . Из него следует, что  $r \in J$ , поскольку  $g, f, qf$  — элементы идеала. В силу выбора  $f$  заключаем, что  $r = 0$ . Значит,  $g(X)$  делится на  $f(X)$ .

и  $J = (f(X)) = f(X)P[X]$ , т.е.  $J$  состоит из многочленов, делящихся на  $f(X)$ .

ii) Если  $f(X) = \frac{a(X)}{a(X)} \frac{b(X)}{b(X)} \in P[X]/(f(X))$  отличны от нуля  $\bar{0}$ , но

$$\overline{a(X)b(X)} = \overline{f(X)} = \bar{0}.$$

Значит,  $P[X]/(f(X))$  обладает нетривиальными делителями нуля и полем быть не может.

С другой стороны, представителем любого класса вычетов в  $P[X]/(f(X))$  может выступать многочлен  $a(X)$ ,  $\deg a(X) < \deg f(X)$ , и если  $a \neq 0$ , а  $f$  неприводим, то найдутся  $b, c \in P[X]$  такие, что  $ab + cf = 1$ . В таком случае  $\overline{ab} + \overline{cf} = \bar{1}$ , т.е.  $\overline{ab} = \bar{1}$ . Значит, любой класс вычетов  $\bar{a} \neq \bar{0}$  обратим, и кольцо  $P[X]/(f(X))$  является полем.  $\square$

Подчеркнём то обстоятельство, что элементы  $\bar{a} = a + (f)$ , где  $a \in P$ , образуют в  $P[X]/(f)$  подкольцо, изоморфное полю  $P$ . В случае неприводимого многочлена  $f(X)$  факторкольцо  $P[X]/(f)$  по теореме 2 является полем, содержащим подполе, изоморфное  $P$ .

**Следствие.** Для любого неприводимого многочлена  $f(X)$  над полем  $P$  существует расширение  $F \supset P$ , в котором  $f(X)$  имеет по крайней мере один корень. За  $F$  можно взять поле, изоморфное  $P[X]/(f)$ .

**Доказательство.** Обратим внимание на специальный элемент  $\bar{X} \in P[X]/(f)$ . Для любых  $a_0, a_1, \dots, a_m \in P$  имеем

$$\begin{aligned} \sum_{k=0}^m \overline{a_k X^k} &= \sum_k \{a_k + (f)\} \{X + (f)\}^k = \\ &= \sum_k \{a_k + (f)\} \{X^k + (f)\} = \left\{ \sum_k a_k X^k \right\} + (f) = \overline{\sum_k a_k X^k}. \end{aligned}$$

Короче, если  $g(Y) = \sum_k a_k Y^k \in P[Y]$ , то  $g(\bar{X}) = \overline{g(X)}$ . Запись  $g(\bar{X})$  имеет, конечно, смысл при отождествлении  $P$  с изоморфным ему полем, содержащимся в  $P[X]/(f)$ . В частности,

$$f(\bar{X}) = \overline{f(X)} = f + (f) = (f) = \bar{0},$$

т.е. элемент  $\bar{X} \in P[X]/(f)$  является корнем многочлена  $(f)$ .  $\square$

**Замечание.** По теореме 1 имеем изоморфизм  $\mathbb{C} = \mathbb{R}[i] \cong \mathbb{R}[X]/J$ , где  $J = \{f \in \mathbb{R}[X] \mid f(i) = 0\}$ . Так как  $a + ib \neq 0$  при  $(a, b) \neq (0, 0)$ , и так как  $i^2 + 1 = 0 \implies X^2 + 1 \in J$ , то из рассуждений, доказывающих теорему 2, вытекает, что  $J = (X^2 + 1)\mathbb{R}[X]$ . Элементами факторкольца  $\mathbb{R}[X]/J$  являются смежные классы  $(a + bX) + J$ ;  $a, b \in \mathbb{R}$ ; соответствие  $a + ib \mapsto (a + bX) + J$  устанавливает изоморфизм между  $\mathbb{C}$  и  $\mathbb{R}[X]/J$ .

В соответствии с установившейся терминологией принято говорить, что расширение  $F \subset P$  из следствия получено присоединением к  $P$  одного корня  $c$  многочлена  $f: F = P(c)$ . При этом  $f(X) = (X - c)g(X)$ , где  $g \in F[X]$ . Нам представилась реальная возможность построить расширение поля  $P$ , в котором многочлен  $f$  полностью распадается на линейные множители.

**Определение.** Пусть  $P$  — поле,  $f$  — нормализованный, не обязательно неприводимый многочлен степени  $n$  из  $P[X]$ . Тогда расширение  $F \subset P$  называется *полем разложения*  $f$  над  $P$ , если  $f(X) = (X - c_1) \dots (X - c_n)$  в  $F[X]$  и  $F = P(c_1, \dots, c_n)$ , т.е.  $F$  получается из  $P$  присоединением корней  $c_1, \dots, c_n$  многочлена  $f$ .

**Теорема 3.** Для всякого нормализованного многочлена  $f \in P[X]$  степени  $n > 0$  существует хотя бы одно поле разложения.

**Доказательство.** Условие нормализованности несущественно и используется только для удобства. Пусть

$$f(X) = f_1(X) \dots f_r(X)$$

— разложение  $f$  на неприводимые нормализованные множители в  $P[X]$ . Согласно следствию теоремы 2 существует расширение  $P_1 \supset \supset P$ , в котором имеется хотя бы один корень многочлена  $f_1$ . Этот корень  $c_1$  будет, разумеется, корнем и для  $f$ .

Пусть уже найдено расширение  $P_k \supset \dots \supset P_1 \supset P$ , над которым  $f$  имеет разложение

$$f(X) = (X - c_1) \dots (X - c_k) g_1(X) \dots g_s(X)$$

с  $k$  (не обязательно различными) линейными множителями,  $k < n$ . Применив опять следствие теоремы 2 к полю  $P_k$  и к неприводимому нормализованному многочлену  $g_1 \in P_k[X]$ , мы построим поле  $P_{k+1} \supset \supset P_k$ , позволяющее отцепить линейный множитель  $X - c_{k+1}$ , где  $c_{k+1} \in P_{k+1}$ , многочлена  $g_1(X)$ , а следовательно, и многочлена  $f(X)$ .

Продолжая действовать подобным образом, мы придём к полному разложению  $f$  на линейные множители над некоторым расширением  $P_n \supset P$ . Либо  $P_n$ , либо какое-то его подполе  $F$  и будет полем разложения для  $f$ . Не исключено, что  $F$  совпадает с  $P$ .  $\square$

Доказательство теоремы 3 содержит слишком много произвола, чтобы можно было говорить о единственности поля разложения многочлена  $f$ . Хотя на самом деле поле разложения с точностью до изоморфизма определено однозначно, мы докажем это лишь в следующей главе. Сейчас мы ограничимся рассмотрением примеров полей разложения.

1) Квадратичное поле  $\mathbb{Q}(\sqrt{d})$  — поле разложения многочлена  $X^2 - d$ .

2) Если присоединить к  $Z_2$  корень  $\theta$  неприводимого многочлена  $X^2 + X + 1$ , то получится поле  $Z_2(\theta) = \{0, 1, \theta, 1 + \theta\}$  из четырёх

элементов, изоморфное как полю  $Z_2[X]/(X^2 + X + 1)$ , так и полю  $GF(4)$  из [ВА I, гл. 4, § 3, п. 5]. Заметим, что

$$X^2 + X + 1 = (X - \theta)(X - \theta^2),$$

т.е.  $Z_2(\theta)$  — поле разложения многочлена  $X^2 + X + 1$ .

3) Многочлен  $X^2 + 1$  неприводим не только над  $\mathbb{R}$ , когда его полем разложения будет  $\mathbb{C}$ , но и над некоторыми другими полями, например над  $Z_3$ . Пусть  $\theta^2 = -1$  (если угодно,  $\theta = X + (X^2 + 1)Z_3[X]$  — элемент поля классов вычетов  $Z_3[X]/(X^2 + 1)$ ). Так как  $X^2 + 1 = (X - \theta)(X - -\theta^3)$ , то  $Z_3(\theta) = \{a + b\theta \mid a, b \in Z_3\}$  — поле разложения для  $X^2 + 1$  над  $Z_3$ .

Между прочим,  $Z_3(\theta)$  изоморфно полю матриц  $\begin{vmatrix} a & b \\ -b & a \end{vmatrix}$ ,  $a, b \in Z_3$ , из [ВА I, гл. 4, § 3, упр. 11]. Вот соответствующее отображение:

$$a + b\theta \mapsto a \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} + b \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}.$$

Обратим внимание на то, что

$$\begin{aligned} Z_3(\theta)^* &= \langle \lambda \rangle, \quad \lambda = 1 + \theta, \quad \lambda^2 = -\theta, \quad \lambda^3 = 1 - \theta, \quad \lambda^4 = -1, \\ \lambda^5 &= -1 - \theta, \quad \lambda^6 = \theta, \quad \lambda^7 = -1 + \theta, \quad \lambda^8 = 1, \end{aligned}$$

т.е. мультиплекативная группа поля  $Z_3(\theta)$  не только абелева, но и циклическая, как ей положено быть.

4) Согласно критерию Эйзенштейна многочлен  $X^3 - 2$  неприводим над  $\mathbb{Q}$ . Так как не все его корни вещественные, то  $\mathbb{Q}(\sqrt[3]{2})$  не может быть полем разложения. На самом деле полем разложения для  $X^3 - 2$  служит  $\mathbb{Q}(\sqrt[3]{2}, \varepsilon)$ , где  $\varepsilon$  — примитивный корень степени 3 из 1:

$$X^3 - 2 = (X - \sqrt[3]{2})(X - \varepsilon \sqrt[3]{2})(X - \varepsilon^2 \sqrt[3]{2}).$$

Что касается колец многочленов от нескольких независимых переменных, то уже в  $\mathbb{R}[X, Y]$  идеалы заведомо не исчерпываются главными.

Пример. Множество

$$J = \{Xf + Yg \mid f, g \in \mathbb{R}[X, Y]\},$$

состоящее из многочленов  $h(X, Y)$  таких, что  $h(0, 0) = 0$ , очевидно, является идеалом в  $\mathbb{R}[X, Y]$ . Так как  $1 \in \mathbb{R}[X, Y]$ , то из  $J = q(X, Y)\mathbb{R}[X, Y]$  следовало бы включение  $q(X, Y) \in J$ . Поэтому  $q(0, 0) = 0$  и, стало быть,  $\deg q \geq 1$ . У нас  $X, Y \in J$ , так что

$$X = qu, \quad Y = qv,$$

откуда с необходимостью вытекают равенства  $\deg u = \deg v = 0$ , т.е.  $u, v \in \mathbb{R}$  и  $Y = u^{-1}vX$  — противоречие, показывающее, что идеал  $J$  не является главным.

**3. Теоремы об изоморфизме колец.** Мы уже располагаем довольно значительным арсеналом типов колец и средств, позволяющих строить новые кольца из данного их набора. Примерами служат конструкции кольца матриц  $M_n(K)$ , поля отношений  $Q(K)$  и

кольца многочленов  $K[X_1, \dots, X_n]$ , где  $K$  — коммутативное кольцо (целостное в случае  $Q(K)$ ). Полезно обсудить ещё, хотя бы вкратце, теоретико-кольцевые аналоги тех общих фактов о гомоморфизмах, которые были установлены для групп в гл. 1. Доказательства, как правило, ничем не отличаются от случая групп, и оставляются читателю в качестве упражнений.

Основную теорему о гомоморфизмах для колец (теорема 1) мы дополним двумя теоремами об изоморфизме.

**Теорема 4.** Пусть  $K$  — кольцо,  $L$  — подкольцо,  $J$  — идеал в  $K$ . Тогда  $L + J = \{x + y \mid x \in L, y \in J\}$  — подкольцо в  $K$ , содержащее  $J$  в качестве идеала,  $L \cap J$  — идеал в  $L$ . Отображение

$$\varphi : x + J \mapsto x + (L \cap J), \quad x \in L,$$

осуществляет изоморфизм кольц:

$$(L + J)/J \cong L/(L \cap J).$$

**Доказательство.** Первые два утверждения совершенно очевидны. Что касается последнего, то нужно рассмотреть ограничение  $\pi_0 = \pi|_L$  естественного эпиморфизма  $\pi : K \rightarrow K/J$ . Его образ  $\text{Im } \pi_0$  состоит из смежных классов  $x + J$ ,  $x \in L$ , т.е.  $\text{Im } \pi_0 = (L + J)/J$ . Ядро  $\text{Ker } \pi_0$  эпиморфизма  $\pi_0 : L \rightarrow (L + J)/J$  состоит из элементов  $x \in L$ , для которых  $x + J = J$ . Значит,  $\text{Ker } \pi_0 = L \cap J$ . По теореме 1 соответствие  $\bar{\pi}_0 : x + (L \cap J) \mapsto \pi_0(x) = x + J$  устанавливает изоморфизм  $L/(L \cap J) \cong (L + J)/J$ . Остаётся заметить, что  $\varphi = \bar{\pi}_0^{-1}$ .  $\square$

Мы провели это рассуждение, скопированное с доказательства теоремы 3 из § 4 гл. 1, для того, чтобы подчеркнуть полный параллелизм с теорией групп.

**Теорема 5.** Пусть  $K$  — кольцо,  $J, L$  — его подкольца, причём  $J$  — идеал в  $K$  и  $J \subset L$ . Тогда  $\bar{L} = L/J$  — подкольцо в  $K/J$  и  $\pi^* : L \rightarrow \bar{L}$  является биективным отображением множества  $\Omega(K, J)$  подколец в  $K$ , содержащих  $J$ , на множество  $\Omega(\bar{K})$  всех подколец кольца  $\bar{K}$ . Если  $L \in \Omega(K, J)$ , то  $L$  — идеал в  $K$  тогда и только тогда, когда  $\bar{L}$  — идеал в  $\bar{K}$ , причём

$$K/L \cong \bar{K}/\bar{L} = (K/J)/(L/J).$$

Доказательство — лёгкое упражнение (см. доказательство теоремы 4 в § 4 гл. 1).

**Следствие.** Пусть  $K$  — коммутативное кольцо с единицей 1. Идеал  $J$  максимальен в  $K$  тогда и только тогда, когда факторкольцо  $K/J$  — поле.

На множестве идеалов кольца  $K$  определены следующие операции:

сумма  $J_1 + J_2 = \{x_1 + x_2 \mid x_k \in J_k\}$ ;

пересечение  $J_1 \cap J_2 = \{x \mid x \in J_1, x \in J_2\}$ ;

*произведение*  $J_1 J_2 = \left\{ \sum_i x_{1i} x_{2i} \mid x_{ki} \in J_k \right\} \subset J_1 \cap J_2$ .

Можно также говорить о сумме, пересечении, произведении любого конечного числа идеалов, причём справедливо следующее утверждение.

**Предложение.** *Если в кольце  $K$  с единицей имеют место равенства*

$$J + J_k = K, \quad k = 1, \dots, n,$$

*для идеалов  $J, J_1, \dots, J_n$ , то справедливы также равенства*

$$J + J_1 \cap J_2 \cap \dots \cap J_n = K = J + J_1 J_2 \dots J_n.$$

**Доказательство.** Так как  $J_1 J_2 \dots J_n \subset J_1 \cap J_2 \cap \dots \cap J_n$ , то достаточно установить равенство  $J + J_1 J_2 \dots J_n = K$ . При  $n = 1$  оно верно по условию. При  $n = 2$  имеем

$$1 = 1^2 = (x_1 + y_1)(x_2 + y_2) = x + y_1 y_2,$$

где  $x_1, x_2, x \in J$ ,  $y_i \in J_i$ . Значит,  $1 \in J + J_1 J_2$  и  $K = J + J_1 J_2$ . Далее — очевидная индукция по числу  $n$ .  $\square$

Пусть  $K_1, \dots, K_n$  — конечное семейство колец,  $K = K_1 \times \dots \times K_n$  — декартово произведение множеств. Введём на  $K$  структуру кольца, определив операции сложения и умножения покомпонентно:

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) = (x_1 + y_1, \dots, x_n + y_n);$$

$$(x_1, \dots, x_n) \cdot (y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n).$$

Мы приходим к *внешней прямой сумме*  $K = K_1 \oplus \dots \oplus K_n$  кольц  $K_i$ . Каждая из компонент  $K_i$  является образом при эпиморфизме  $\pi_i : (x_1, \dots, x_n) \mapsto x_i$ ,  $1 \leq i \leq n$ . Если, далее,

$$J_i = \{(0, \dots, x_i, \dots, 0) \mid x_i \in K_i\},$$

то  $J_i \cong K_i$ ,  $J_i$  — идеал в  $K$  и  $K = J_1 + \dots + J_n$ .

Пусть теперь  $K$  — кольцо с идеалами  $J_1, \dots, J_n$ , причём

$$K = J_1 + \dots + J_n, \quad J_k \cap \left( \sum_{j \neq k} J_j \right) = 0, \quad 1 \leq k \leq n.$$

Тогда  $K = J_1 \oplus \dots \oplus J_n$  — *внутренняя прямая сумма* своих идеалов  $J_k$ . Как и в теории групп, различие между внутренними и внешними прямыми суммами кольц чисто теоретико-множественное, и нет смысла отражать его в обозначениях.

### УПРАЖНЕНИЯ

1. Показать, что кольцо  $Q_M(\mathbb{Z})$  всех рациональных чисел  $a/b$  с  $b$ , не делящимся на фиксированное простое число  $p$ , содержит единственный максимальный идеал

$$J = \{a/b \in Q_M(\mathbb{Z}) \mid p \text{ делит } a\}.$$

Всякое кольцо, обладающее единственным максимальным идеалом, называется *локальным кольцом*.

2. Показать, что в любом локальном кольце  $K$  с максимальным идеалом  $\mathfrak{m}$  элементы, не лежащие в  $\mathfrak{m}$ , обратимы.

3. Идеал  $\mathfrak{p}$  кольца  $K$  с единицей называется *простым*, если факторкольцо  $K/\mathfrak{p}$  целостно. Всякий максимальный идеал прост. Дополнение  $M = K \setminus \mathfrak{p}$  в кольце  $K$  является *мультиликативным подмножеством* (моноидом, не содержащим 0). Кольцо  $Q_M(K)$  в этих условиях обозначается чаще символом  $M^{-1}K$  или просто  $K_{\mathfrak{p}}$ .

Показать, что кольцо  $K_{\mathfrak{p}}$  всегда локально и что его максимальный идеал  $\mathfrak{m}_{\mathfrak{p}}$  состоит из частных вида  $a/b$ , где  $a \in \mathfrak{p}$ ,  $b \in K \setminus \mathfrak{p}$ . Показать также, что  $\mathfrak{m}_{\mathfrak{p}} \cap K = \mathfrak{p}$ .

Операция перехода от  $K$  к локальному кольцу  $K_{\mathfrak{p}}$  называется *локализацией* кольца  $K$  относительно простого идеала  $\mathfrak{p}$ .

## § 2. Отдельные результаты о кольцах

Этот параграф можно рассматривать как небольшое, но полезное дополнение к главам 4 и 5 в [BA I].

**1. Целые гауссовые числа.** Ранее была доказана факториальность евклидовых колец, к числу которых относятся кольца  $\mathbb{Z}$  и  $P[X]$ . Ниже приводится ещё один пример евклидова кольца, а в следующем пункте — пример факториального кольца, не являющегося евклидовым.

**Теорема 1.** *Кольцо целых гауссовых чисел  $\mathbb{Z}[i]$  евклидово.*

**Доказательство.** Имеется в виду числовое кольцо

$$\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\},$$

содержащееся в квадратичном поле  $\mathbb{Q}(i) \in \mathbb{C}$ ,  $i^2 + 1 = 0$ , и геометрически отождествляемое со множеством узлов (точек) целочисленной решётки в комплексной плоскости  $\mathbb{C}$ . Понятно, что  $\mathbb{Z}[i]$  — целостное кольцо. Мы определим на  $\mathbb{Z}[i]^* = \mathbb{Z}[i] \setminus \{0\}$  отображение  $\delta : \mathbb{Z}[i]^* \rightarrow \mathbb{N} \cup \{0\}$ , полагая

$$\delta(m + in) = |m + in|^2 = m^2 + n^2$$

(т.е.  $\delta(a) = N(a)$  — норма числа  $a$  в  $\mathbb{Q}(i)$ ). Как известно,  $\delta(ab) = \delta(a)\delta(b)$  для всех  $a, b \in \mathbb{Z}[i]^*$ , так что свойство Е1) из определения евклидова кольца (см. п. 3, § 3 гл. 5 в [BA I]) автоматически выполнено. Чтобы убедиться в справедливости Е2), запишем дробь  $ab^{-1}$  с  $b \neq 0$  в виде  $ab^{-1} = \alpha + i\beta$  с  $\alpha, \beta \in \mathbb{Q}$  и возьмём ближайшие к  $\alpha, \beta$  целые числа  $k, l$  такие, что  $\alpha = k + \nu$ ,  $\beta = l + \mu$ ,  $|\nu| \leqslant 1/2$ ,  $|\mu| \leqslant 1/2$ . Тогда

$$a = b[(k + \nu) + i(l + \mu)] = bq + r,$$

где  $q = k + il \in \mathbb{Z}[i]$ , а  $r = b(\nu + i\mu)$ . Так как  $r = a - bq$ , то и  $r \in \mathbb{Z}[i]$ , причём

$$\delta(r) = |r|^2 = |b|^2(\nu^2 + \mu^2) \leqslant \delta(b) \left( \frac{1}{4} + \frac{1}{4} \right) = \frac{1}{2} \delta(b) < \delta(b).$$

Стало быть,  $\mathbb{Z}[i]$  — евклидово кольцо.  $\square$

Кольцо целых гауссовых чисел  $\mathbb{Z}[i]$  удобно для демонстрации в миниатюре методов теории алгебраических чисел. Поэтому мы остановимся на свойствах  $\mathbb{Z}[i]$  чуть подробнее. Сначала докажем нескольких простых утверждений.

**Определение.** Целостное кольцо  $K$ , все идеалы которого главные, т.е. имеют вид  $aK$ , называется *кольцом главных идеалов*.

**Предложение 1.** *Все евклидовы кольца являются кольцами главных идеалов.*

**Доказательство.** Для  $\mathbb{Z}$  и  $P[X]$  это было установлено ранее ([ВА I] и теорема 2 из § 1), а в общем случае рассуждения совершенно аналогичны: если  $J$  — идеал евклидова кольца  $K$ , то  $J = aK$ , как только  $a \in J$  и  $\delta(a) \leq \delta(x)$  для всех  $0 \neq x \in J$ .  $\square$

**Предложение 2.** *Пусть  $K$  — произвольное евклидово кольцо с функцией  $\delta$  и  $U(K)$  — группа его обратимых элементов. Тогда*

$$u \in U(K) \iff \delta(u) = \delta(1) \iff \delta(ux) = \delta(x) \quad \forall x \in K^*. \quad (1)$$

**Доказательство.** Действительно, согласно Е1),  $\delta(x) = \delta(1 \cdot x) \geq \delta(1)$  для всех  $x \in K^*$ , а если  $u \in U(K)$ , то  $\delta(1) = \delta(u \cdot u^{-1}) \geq \delta(u)$ , так что  $\delta(u) = \delta(1)$ . Обратно: в соответствии с предложением 1

$$\delta(ux) = \delta(x) \quad \forall x \in K^* \implies uxK = xK \implies$$

$$\implies x = uxv \implies uv = 1 \implies u \in U(K). \quad \square$$

В применении к кольцу  $\mathbb{Z}[i]$  критерий (1) означает, что  $m + in \in U(\mathbb{Z}[i]) \iff m^2 + n^2 = 1$ . Стало быть,  $U(\mathbb{Z}[i]) = \langle i \rangle$  — циклическая группа порядка 4.

**Определение.** Идеал  $J$  кольца  $K$  называется *максимальным*, если  $J \neq K$  и всякий идеал  $T$ , содержащий  $J$  собственным образом, совпадает с  $K$ .

**Предложение 3.** *В евклидовом кольце  $K$  свойство элемента  $p \in K$  быть простым эквивалентом условию максимальности идеала  $pK$ .*

**Доказательство.** В самом деле, пусть  $p$  — простой элемент и  $pK \subset T \subset K$ , где  $T$  — идеал в  $K$ . Согласно предложению 1  $T = aK$ , и так как  $p \in T$ , то  $p = ab$ , где один из элементов  $a, b$  обратим. Если  $b \in U(K)$ , то  $T = aK = abK = pK$ .

Обратно: пусть идеал  $pK$  максимальен и  $p = ab$  с  $a \notin U(K)$ . Тогда

$$aK \neq K \text{ и } pK \subset aK \implies pK = aK \implies$$

$$\implies a = pu = abu \implies bu = 1 \implies b \in U(K) \implies$$

$$\implies p \text{ — простой элемент.} \quad \square$$

**2. Каноническое разложение суммы двух квадратов.** Посмотрим теперь, что происходит с простым числом  $p \in \mathbb{Z}$  в кольце  $\mathbb{Z}[i]$ . Не исключено, что  $p$  остаётся простым элементом и в  $\mathbb{Z}[i]$ . В противном случае справедливо

*Предложение 4. Если простое число  $p \in \mathbb{Z}$  допускает нетривиальное разложение в  $\mathbb{Z}[i]$ , то*

$$p = (m + in)(m - in) = m^2 + n^2, \quad (2)$$

где  $m + in, m - in$  — простые элементы в  $\mathbb{Z}[i]$ .

**Доказательство.** Пусть  $p = \prod_{k=1}^r p_k$  — его единственное (по теореме 4 из [ВА I, § 3, гл. 5]) разложение на простые множители  $p_k$  в количестве  $r > 1$ . В силу предложения 2 имеем  $\delta(p_k) > 1$ , так что из  $p^2 = \delta(p) = \prod \delta(p_k)$ , и из факториальности  $\mathbb{Z}$  следуют с необходимостью равенства

$$r = 2, \quad p = p_1 p_2, \quad \delta(p_1) = \delta(p_2) = p$$

Если  $p_1 = m + in$ , то

$$p = \delta(p_1) = m^2 + n^2 = (m + in)(m - in) \implies p_2 = m - in. \quad \square$$

В частности,  $2 = (1 + i)(1 - i)$  не является простым элементом в  $\mathbb{Z}[i]$ .

Мы готовы теперь доказать следующий критерий.

**Теорема 2.** Простое число  $p \in \mathbb{Z}$  остаётся простым в  $\mathbb{Z}[i]$  тогда и только тогда, когда  $p = 4k - 1$ .

Всякое простое число  $p = 4k + 1$  представимо в виде  $p = m^2 + n^2$ , где  $m, n \in \mathbb{Z}$ .

**Доказательство.** Заметим сначала, что  $t^2 \equiv 0 \pmod{4}$  или  $t^2 \equiv 1 \pmod{4}$  для любого  $t \in \mathbb{Z}$ . Поэтому для нечётного простого числа  $p$ , не являющегося простым в  $\mathbb{Z}[i]$ , предложение 4 приводит к выводу:

$$p = m^2 + n^2 \equiv 0, 1, 2 \pmod{4} \implies p = 4k + 1.$$

В случае  $p = 4k + 1$  положим  $t = (2k)!$ . Так как, очевидно,

$$\begin{aligned} t = (-1)^{2k}(2k)! &= (-1)(-2) \dots (-2k) \equiv (p-1)(p-2) \dots (p-2k) \equiv \\ &\equiv ((p+1)/2) \dots (p-2)(p-1) \pmod{p}, \end{aligned}$$

то

$$t^2 \equiv (2k)!((p+1)/2) \dots (p-2)(p-1) \equiv (p-1)! \pmod{p},$$

или, с учётом теоремы Вильсона [ВА I, гл. 6, § 1],  $t^2 + 1 \equiv 0 \pmod{p}$ . Если теперь  $p$  — простой элемент в  $\mathbb{Z}[i]$ , то из равенства  $(t+i)(t-i) = t^2 + 1 = lp$ ,  $l \in \mathbb{Z}$ , по теореме 1 из [ВА I, гл. 5, § 3] следует делимость на  $p$  одного из элементов  $t+i, t-i$ . Но  $t \pm i = p(m + in) \implies \pm 1 = pn$ ,  $n \in \mathbb{Z}$ , что явно невозможно.  $\square$

Из установленных нами фактов несложно извлекается общая теоретико-числовая теорема.

**Теорема 3.** Число  $t \in \mathbb{Z}$  представимо в виде суммы квадратов двух чисел  $m, n \in \mathbb{Z}$  тогда и только тогда, когда в каноническое разложение  $t$  на простые множители каждый простой делитель  $p = 4k - 1$  входит с чётным показателем.

**Доказательство.** Действительно, достаточно показать, что если  $\text{НОД}(m, n) = 1$  и  $p \mid (m^2 + n^2)$ , то  $p = 4k + 1$ . Это довольно ясно, если заметить, что:

$$\begin{aligned} \text{НОД}(m, n) = 1, \quad m^2 + n^2 &\equiv 0 \pmod{p}, \quad mn \not\equiv 0 \pmod{p} \implies \\ &\implies m^{p-1} \equiv 1 \pmod{p}, \quad n^2 \equiv -m^2 \pmod{p} \implies \\ &\implies (m^{p-2}n)^2 = m^{2p-4}n^2 \equiv -m^{2p-2} \equiv -1 \pmod{p}. \end{aligned}$$

Таким образом, существует целое число  $s \in \mathbb{Z}$  такое, что  $s^2 \equiv -1 \pmod{p}$ ,  $s^4 \equiv 1 \pmod{p}$ . Стало быть, порядок  $p - 1$  мультипликативной группы  $\mathbb{Z}^*$  делится на 4 и  $p = 4k + 1$ .  $\square$

Согласно предложению 3 простота  $p = 4k - 1$  в  $\mathbb{Z}[i]$  эквивалентна максимальности идеала  $p\mathbb{Z}[i]$ , что в свою очередь выражается свойством факторкольца  $\mathbb{Z}[i]/p\mathbb{Z}[i]$  быть полем из  $p^2$  элементов (см. в этой связи упр. 11 в [ВА I], гл. 4 § 3 и теоремы об изоморфизме для колец в § 1). Это и не удивительно, если учесть, что при  $p = 4k - 1$  многочлен  $X^2 + 1$ , рассматриваемый над  $\mathbb{Z}_p$ , неприводим. Более подробно об этом будет говориться в следующей главе.

**3. Полиномиальные расширения факториальных колец.** Покажем, что кольца многочленов  $\mathbb{Z}[X_1, \dots, X_n]$  и  $P[X_1, \dots, X_n]$  ( $P$  — поле) факториальны при любом  $P$ . Это важное утверждение непосредственно вытекает из следующей теоремы.

**Теорема 4.** Если факториально кольцо  $K$ , то факториально и кольцо многочленов  $K[X]$ .

**Доказательство.** В основе доказательства лежат свойства многочленов, связанные с понятием примитивности и примыкающие к лемме Гаусса [ВА I, гл. 5, § 3]. Именно, нам понадобятся следующие два свойства.

а) *Примитивные многочлены  $f, g \in K[X]$ , ассоциированные в  $Q(K)[X]$  ( $Q(X)$  — поле отношений факториального кольца  $K$ ), ассоциированы в  $K[X]$  (лёгкое упражнение).*

б) *Многочлен  $f \in K[X]$  положительной степени, неприводимый над  $K$ , неприводим также над  $Q(K)$  (доказательство в [ВА I] для  $K = \mathbb{Z}$  годится и в общем случае).*

Приступая непосредственно к доказательству теоремы, запишем многочлен  $f \in K[X]$  положительной степени в виде  $f = d(f)f_0$ , где  $d(f)$  — содержание многочлена  $f$ , а  $f_0$  — его примитивная составляющая. Индукцией по степени примитивных многочленов мы полу-

чим разложение  $f_0$  в произведение  $f_0 = f_1 \dots f_s$  неприводимых над  $K$  примитивных многочленов  $f_1, \dots, f_s$ .

Пусть  $f_0 = g_1 \dots g_t$  — ещё одно такое же разложение. Тогда согласно б)  $f_i$  и  $g_j$  неприводимы над  $Q(K)$ , а поскольку кольцо  $Q(K)[X]$  факториально (см. [ВА I, следствие теоремы 4 из § 3, гл. 5]),  $s = t$  и при надлежащем упорядочении многочлен  $f_i$  ассоциирован с  $g_i$  в  $Q(K)[X]$ , а следовательно (по а)), и в  $K[X]$ .

Что касается многочлена  $f$  с необратимым в  $K$  содержанием  $d(f)$ , то, взяв ещё разложение  $d(f) = p_1 \dots p_r$  на простые множители  $p_i \in K$ , мы придём к разложению  $f$ . Единственность такого разложения (в обычном понимании) следует из только что установленной единственности разложения  $f_0$  и из факториальности  $K$ , отвечающей за единственность разложения  $d(f) = p_1 \dots p_r$ .  $\square$

**Теорема 5.** *Имеют место строгие включения:*

$$\{\text{евклидовы кольца}\} \subset \{\text{кольца главных идеалов}\} \subset$$

$$\subset \{\text{факториальные кольца}\} \quad (3)$$

**Доказательство.** Первое включение установлено предложением 1. Существуют примеры (мы их не приводим), показывающие, что оно строгое.

Для доказательства второго включения рассмотрим в кольце главных идеалов  $K$  возрастающую последовательность идеалов  $(d_1) \subset (d_2) \subset \dots$  Непосредственно проверяется, что  $D = \cup_i (d_i)$  — идеал в  $K$ . Следовательно,  $D = (d)$ . По определению  $d \in (d_m) \subset D$  для некоторого  $m$ , откуда  $(d_m) = (d_{m+1}) = \dots$  Стабилизация на конечном шаге возрастающей цепочки идеалов влечёт обрыв цепочки необратимых делителей  $d_1, d_2, d_3, \dots$  с  $d_i \mid d_{i-1}$  и, стало быть, существование разложения в  $K$  на неразложимые элементы.

Единственность разложения в  $K$  является следствием тех же причин:

$$(a, b) = aK + bK = dK = (d) \implies d = \text{НОД}(a, b) = ax + by.$$

Дальнейшие рассуждения повторяют доказательство следствия ii) из теоремы 3 в [ВА I, гл. 5 § 3].

Идеалы  $(2, X)$  в  $\mathbb{Z}[X]$  и  $(X, Y)$  в  $\mathbb{R}[X, Y]$  не являются главными (см. пример из § 1). В то же время по теореме 4 кольца  $\mathbb{Z}[i]$  и  $\mathbb{R}[X, Y]$  факториальны. Тем самым истинность цепочки (3) установлена.  $\square$

Кольца главных идеалов интересны с чисто алгебраической точки зрения, поскольку они характеризуются свойствами таких естественных объектов, как ядра гомоморфизмов. С другой стороны, евклидовы кольца более удобны для исследования в силу наличия в них алгоритма деления с остатком.

**4. Строение мультиликативной группы  $U(Z_n)$ .** Универсальное свойство прямых сумм заключается в следующем довольно очевидном утверждении.

Если  $S = K_1 \oplus \dots \oplus K_n$  и  $K$  — произвольное кольцо с заданными гомоморфизмами  $\varphi_i : K \rightarrow K_i$ , то существует единственный гомоморфизм  $\varphi = (\varphi_1, \dots, \varphi_n : K \rightarrow S)$  с ядром  $\text{Ker } \varphi = \cap \text{Ker } \varphi_i$ , делающий треугольные диаграммы

$$\begin{array}{ccc} K & \xrightarrow{\varphi_i} & K_i \\ & \searrow \varphi & \swarrow \pi_i \\ & S & \end{array}$$

при  $i = 1, \dots, n$  коммутативными ( $\pi_i$  — канонические отображения).

Применим это утверждение к кольцу  $K$  с 1 и с идеалами  $J_1, \dots, J_n$  и к прямой сумме

$$S = K/J_1 \oplus \dots \oplus K/J_n.$$

Положив  $\varphi_i : K \rightarrow K/J_i = K_i$ , мы получим гомоморфизм

$$\varphi : x \mapsto (x + J_1, \dots, x + J_n) \quad (4)$$

кольца  $K$  в  $S$  с ядром  $\text{Ker } \varphi = J_1 \cap \dots \cap J_n$ .

**Теорема 6** (китайская теорема об остатках). *Если в указанных выше условиях  $K$  — кольцо с единицей и  $J_i + J_j = K$  для  $1 \leq i \neq j \leq n$ , то отображение  $\varphi$  (см. (4)) является эпиморфизмом.*

**Доказательство.** Нам нужно убедиться, что при любых заданных элементах  $x_1, \dots, x_n \in K$  найдётся  $x \in K$ , для которого  $x + J_i = x + J_i$ , т.е.  $x - x_i \in J_i$ ,  $i = 1, 2, \dots, n$ . При  $n = 1$  это очевидно, а при  $n = 2$  возьмём элементы  $a_1 \in J_1$ ,  $a_2 \in J_2$ , для которых  $a_1 + a_2 = 1$ , и положим  $x = x_1 a_2 + x_2 a_1$ . Тогда

$$x - x_1 = (x_1 a_2 + x_2 a_1) - x_1 (a_1 + a_2) = (x_2 - x_1) a_1 \in J_1,$$

$$x - x_2 = (x_1 a_2 + x_2 a_1) - x_2 (a_1 + a_2) = (x_1 - x_2) a_2 \in J_2.$$

Далее рассуждаем индукцией по  $n$ . Пусть мы уже нашли элемент  $y$ , для которого  $y - x_i \in J_i$ ,  $i = 1, 2, \dots, n-1$ . Так как по условию  $J_i + J_n = K$ ,  $1 \leq i \leq n-1$ , то согласно предложению из § 1  $J_1 \cap \dots \cap J_{n-1} + J_n = K$ . Применим разобранный нами случай  $n=2$  к идеалам  $J_1 \cap \dots \cap J_{n-1}$ ,  $J_n$  и к элементам  $x - x_n \in J_n$ . Но

$$x - y \in J_1 \cap \dots \cap J_{n-1} \implies x - y \in J_i, \quad 1 \leq i \leq n-1.$$

С учётом выбора  $y$  получаем

$$x - x_i = (x - y) + (y - x_i) \in J_i, \quad 1 \leq i \leq n-1.$$

Стало быть, элемент  $x$  удовлетворяет всем поставленным требованиям.  $\square$

В теореме 6 и в предшествующих ей рассуждениях кольцо  $K$  не предполагалось коммутативным. Пусть, далее,  $K$  — целостное кольцо и  $a_1, \dots, a_n$  — его  $n$  попарно взаимно простых элементов, т.е.  $a_i K + a_j K = K$  при  $i \neq j$  (в факториальном кольце  $K$  это определение согласуется с определением взаимной простоты, получающимся из разложения  $a_i$  на простые множители). Записывая включение  $x - x_i \in a_i K$  в виде сравнения по модулю главного идеала  $a_i K$ , мы, как обычно, пользуемся обозначением  $x \equiv x_i \pmod{a_i}$ .

**Следствие 1.** *Пусть  $K$  — целостное кольцо и  $a_1, \dots, a_n$  — его попарно взаимно простые элементы. Тогда для любых  $x_1, \dots, x_n \in K$  найдётся элемент  $x \in K$  такой, что*

$$x \equiv x_i \pmod{a_i}, \quad i = 1, \dots, n.$$

**Следствие 2.** *Пусть  $n$  — натуральное число с каноническим разложением  $n = p_1^{m_1} \dots p_r^{m_r}$ ,  $Z_n = \mathbb{Z}/n\mathbb{Z}$  — кольцо классов вычетов по модулю  $n$  и  $U(Z_n)$  — мультиликативная группа его обратимых элементов. Тогда:*

- i)  $Z_n \cong Z_{p_1^{m_1}} \oplus \dots \oplus Z_{p_r^{m_r}}$  (прямая сумма колец);
- ii)  $U(Z_n) \cong U(Z_{p_1^{m_1}}) \times \dots \times U(Z_{p_r^{m_r}})$  (прямое произведение групп).

**Доказательство.** i) Заменив в (4)  $n$  на  $r$ , положив

$$K = \mathbb{Z}, \quad J_i = p_i^{m_i} \mathbb{Z}, \quad S = Z_{p_1^{m_1}} \oplus \dots \oplus Z_{p_r^{m_r}},$$

мы придём к гомоморфизму  $\varphi: \mathbb{Z} \rightarrow S$  с ядром  $\text{Кер } \varphi = \bigcap_i J_i = n\mathbb{Z}$ . Эпиморфность  $\varphi$  вытекает из теоремы 6, поскольку  $\text{НОД}(p_i, p_j) = 1$  при  $i \neq j$ .

ii) Так как в произвольной прямой сумме  $K = K_1 \oplus \dots \oplus K_r$  компоненты  $K_i$  аннулируют друг друга:  $K_i K_j = 0$ ,  $i \neq j$ , то непосредственно из определения обратимых элементов следует, что  $U(K) = U(K_1) \times \dots \times U(K_r)$ . Остается применить это к разложению i).  $\square$

**Замечание.** Из утверждения ii) непосредственно видно, что  $\varphi(n) = \prod_{i=1}^r \varphi(p_i^{m_i})$ , а так как  $\varphi(p^m) = p^{m-1}(p-1)$ , то вновь получается формула для значений функции Эйлера (см. [ВА I, гл. 1, § 9, упр. 3]). Порядок элемента конечной группы является делителем порядка группы, поэтому

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

для любого целого числа  $a$ , взаимно простого с  $n$  (обобщение малой теоремы Ферма, известное под названием *теорема Эйлера*).

Для полного понимания строения группы  $U(Z_n)$  нам в силу следствия 2 из теоремы 6 достаточно разобрать случай  $n = p^m$ .

**Теорема 7.** *Пусть  $m$  — целое положительное число.*

i) *Если  $p$  — нечётное простое число, то  $U(Z_{p^m})$  — циклическая группа.*

ii) Группы  $U(Z_2)$  и  $U(Z_4)$  — циклические порядков 1 и 2 соответственно, в то время как  $U(Z_{2^m})$ ,  $m \geq 3$ , — прямое произведение циклической группы порядка  $2^{m-2}$  и циклической группы порядка 2.

Доказательство. i) По определению взаимно простое с  $n$  целое число  $t$  имеет порядок  $r$  по модулю  $n$ , если  $|\langle t + n\mathbb{Z} \rangle| = r$ , т.е.  $t^r \equiv 1 \pmod{n}$ , но  $t^k \not\equiv 1 \pmod{n}$  для  $k < r$ . При  $r = \varphi(n)$  говорят о примитивном (или первообразном) корне  $t$  по модулю  $n$ . Обычно  $t$  берут из приведённой системы вычетов  $0, 1, \dots, n-1$  по модулю  $n$ , но мы никакой системы вычетов не фиксируем.

Согласно теореме 11 из § 3, гл. 2 группа  $Z_p^* = U(Z_p)$  циклическая, т.е. существует примитивный корень  $a_0$  по модулю  $p$ . Так как  $a_0^{p^{m-1}} \equiv a_0 \pmod{p}$ , то и целое число  $a = a_0^{p^{m-1}}$  будет примитивным корнем по модулю  $p$ . С другой стороны,

$$a^{p-1} = a_0^{p^{m-1}(p-1)} = a_0^{\varphi(p^m)} \equiv 1 \pmod{p^m}.$$

Значит, смежный класс  $\bar{a} = a + p^m\mathbb{Z}$  порождает в  $U(Z_{p^m})$  циклическую подгруппу порядка  $p-1$ .

Далее,

$$(1+p)^p = \sum_{i=0}^p \binom{p}{i} p^i = 1 + p^2 + \frac{1}{2}(p-1)p^3 + \sum_{i \geq 3} \binom{p}{i} p^i.$$

Так как  $p > 2$ , то  $(1+p)^p \equiv 1 + p^2 \pmod{p^3}$ . Предположив по индукции, что  $(1+p)^{p^j} \equiv 1 + p^{j+1} \pmod{p^{j+2}}$ , мы находим

$$\begin{aligned} (1+p)^{p^{j+1}} &= [1 + (1+sp)p^{j+1}]^p = \sum_{i=0}^p \binom{p}{i} (1+sp)^i p^{(j+1)i} = \\ &= 1 + (1+sp)p^{j+2} + \frac{1}{2}(p-1)(1+sp)^2 p^{2(j+1)+1} + \dots, \end{aligned}$$

откуда

$$(1+p)^{j+1} \equiv 1 + p^{j+2} \pmod{p^{j+3}}.$$

В частности,

$$(1+p)^{p^{m-1}} \equiv 1 \pmod{p^m},$$

но

$$(1+p)^{p^{m-2}} \equiv 1 + p^{m-1} \not\equiv 1 \pmod{p^m},$$

и, стало быть, смежный класс  $\bar{b} = 1 + p + p^m\mathbb{Z}$  с представителем  $b = 1 + p$  порождает в  $U(Z_{p^m})$  циклическую группу порядка  $p^{m-1}$ . Согласно предложению 2 из § 3 гл. 2 элементы  $\bar{a}, \bar{b}$  взаимно простых порядков  $p-1, p^{m-1}$  порождают циклическую группу  $\langle \bar{a}\bar{b} \rangle$  порядка

$$p^{m-1}(p-1) = \varphi(p^m) = |U(Z_{p^m})|.$$

С группами  $U(Z_2)$  и  $U(Z_4)$  всё ясно. При  $m > 2$ , исходя из триадиального сравнения  $5 \equiv 1 + 2^2 \pmod{2^3}$ , индукцией по  $j$  легко проверяется, что

$$5^{2^j} \equiv 1 + 2^{j+2} \pmod{2^{j+3}}.$$

В частности,

$$5^{2^{m-3}} \equiv 1 + 2^{m-1} \not\equiv 1 \pmod{2^m}, \quad 5^{2^{m-2}} \equiv 1 \pmod{2^m},$$

так что 5 имеет порядок  $2^{m-2}$  по модулю  $2^m$  и смежный класс  $5 + 2^m\mathbb{Z}$  порождает в  $U(Z_{2^m})$  циклическую подгруппу индекса 2. Заметим, что  $-1 + 2^m\mathbb{Z} \notin \langle 5 + 2^m\mathbb{Z} \rangle$ , поскольку

$$5^j \equiv -1 \pmod{2^m} \implies 5^j \equiv -1 \pmod{4} \implies 1 \equiv -1 \pmod{4}$$

— противоречие. Так как  $|(-1 + 2^m\mathbb{Z})| = 2$ , то

$$U(\mathbb{Z}/2^m\mathbb{Z}) = \langle 5 + 2^m\mathbb{Z} \rangle \times \langle -1 + 2^m\mathbb{Z} \rangle$$

— абелева 2-группа типа  $(2^{m-2}, 2)$  (см. § 3 из гл. 2).  $\square$

**Следствие.** Группа  $U(Z_n)$  является циклической (или, что равносильно, примитивный корень по модулю  $n$  существует) тогда и только тогда, когда целое число  $n > 1$  имеет вид  $2, 4, p^m$  или  $2p^m$ , где  $p$  — нечётное простое число.

### УПРАЖНЕНИЯ

1. Доказать, что ненулевой элемент  $p$  факториального кольца  $K$  является простым тогда и только тогда, когда  $K/pK$  — целостное кольцо.

2. Доказать, что если целостное кольцо  $K$  не является полем, то  $K[X]$  не является кольцом главных идеалов.

3. Показать, что элементы  $x + y\sqrt{-3}$ , где  $x, y \in \mathbb{Z}$  или же  $x = (2k+1)/2$ ,  $y = (2l+1)/2$ ,  $k, l \in \mathbb{Z}$ , составляют целостнее кольцо  $K$ . Проверить, что оно евклидово с функцией  $\delta = N$  (норма в  $\mathbb{Q}(\sqrt{-3})$ ). Показать, что подкольцо  $\mathbb{Z}[\sqrt{-3}] \subset K$  не является даже факториальным.

4. Найти все простые элементы кольца целых гауссовых чисел.

5. Усовершенствовать следствие теоремы 6 в случае факториального кольца  $K$ , для чего, наряду с попарно взаимно простыми элементами  $a_1, \dots, a_n$ , ввести элементы  $\tilde{a}_i = \prod_{j \neq i} a_j$ . Найти  $b_i \in K$ , для которых

$$b_i \equiv 1 \pmod{a_i}, \quad b_i \equiv 0 \pmod{\tilde{a}_i}, \quad 1 \leq i \leq n.$$

Пусть  $x_1, \dots, x_n \in K$ . Ввести элемент  $x = \sum b_i x_i$  и проверить, что  $x \equiv x_i \pmod{a_i}$ ,  $1 \leq i \leq n$  (удобство, ощущимое в тех случаях, когда имеют дело с большим числом наборов  $x_1, \dots, x_n$ ).

6. Применить предыдущее упражнение к модулям  $a_1 = 5, a_2 = 9$  и к парам  $(x_1, x_2) = (2, 5), (3, 2), (3, 5)$ . Что можно сказать о порядке  $x$  по модулю 45?

7. Пусть  $p$  — нечётное простое число. Если сравнение  $x^2 \equiv a \pmod{p}$  имеет решение, то целое число  $a$  называется *квадратичным вычетом по модулю  $p$* , в противном случае — *квадратичным невычетом*. Символ Лежандра  $\left(\frac{a}{p}\right)$  определяется соотношением

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{если } a \equiv 0 \pmod{p}, \\ 1, & \text{если } a \not\equiv 0 \pmod{p} \text{ — квадратичный вычет,} \\ -1, & \text{если } a \not\equiv 0 \pmod{p} \text{ — квадратичный невычет.} \end{cases}$$

Показать, что  $(\frac{a}{p}) = 1 \iff a + p\mathbb{Z} \in (Z_p^*)^2$  и  $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$ . Далее,  $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$  и число квадратичных вычетов в приведённой системе  $1, 2, \dots, p - 1$  совпадает с числом невычетов. Проверить для небольших нечётных простых чисел  $p$  и  $q$  выполнение **квадратичного закона взаимности**

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

доказанного в общем случае (многими способами) Гауссом. Извлечь из теоремы 1 соотношение  $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{8}}$ .

**8.** Доказать (в обозначениях предыдущего упражнения), что  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ , т.е. 2 является квадратом по  $\pmod{p}$  в точности тогда, когда  $p \equiv \pm 1 \pmod{8}$ .

**9.** (Дополнение к [ВА I, гл. 3, § 4]). Пусть  $f(X) = f(\dots, x_{ij}, \dots)$  — ненулевой многочлен от  $n^2$  независимых переменных  $x_{ij} \in K$ ,  $1 \leq i, j \leq n$ , с коэффициентами в  $\mathbb{Z}$  или в некотором поле, рассматриваемый как функция матрицы  $X = (x_{ij})$ . Доказать, что если  $f(XY) = f(X)f(Y)$  для всех  $X, Y \in M_n(K)$ , то  $f(X) = (\det X)^m$ , где  $m$  — некоторое неотрицательное целое число. В частности,  $f(X) = \det X$ , коль скоро  $f(\text{diag}(x, 1, \dots, 1)) = x$ .

### § 3. Модули

Понятие модуля служит носителем фундаментального принципа, выработанного в алгебре почти сто лет назад. Он заключается в том, что предметом изучения любой алгебраической системы должны быть не только внутренние свойства этой системы, но и все её представления (в самом широком смысле этого слова).

**1. Первоначальные сведения о модулях.** Начнём с классического определения. Пусть  $K$  — ассоциативное кольцо с единицей и  $V$  — аддитивно записываемая абелева группа. Пусть, далее, задано отображение  $(x, v) \mapsto xv$  из  $K \times V$  в  $V$ , удовлетворяющее условиям:

- M1)  $x(u+v) = xu+xv$ ,
- M2)  $(x+y)v = xv+yv$ ,
- M3)  $(xy)v = x(yv)$ ,
- M4)  $1 \cdot v = v$

для всех  $x, y \in K$ ,  $u, v \in V$ . Тогда  $V$  называется *левым  $K$ -модулем* (или *левым модулем над кольцом  $K$* ). Аналогично определяется правый  $K$ -модуль. В дальнейшем мы говорим просто о  $K$ -модуле, хотя в некоторых ситуациях оба вида модулей появляются вместе.

Аксиома M4) (условие *унитарности* модуля), естественно, является лишней, если кольцо  $K$  не обладает единицей. Более существенно, что возможны модификации аксиомы M3), приспособленные к некоторым неассоциативным кольцам. Пример модуля над неассоциативным кольцом приведён в конце главы. Пока мы будем исходить из данного выше определения.

Пусть  $V$  —  $K$ -модуль. Подгруппа  $U \subset V$  называется *подмодулем* в  $V$ , если  $xu \in U$  для всех  $x \in K$ ,  $u \in U$ .

Пусть, далее,  $U$  и  $V$  — произвольные  $K$ -модули. Гомоморфизмом  $K$ -модулей (или просто  $K$ -гомоморфизмом) из  $U$  в  $V$  называется отображение  $\sigma : U \rightarrow V$  такое, что

$$\sigma(u_1 + u_2) = \sigma(u_1) + \sigma(u_2),$$

$$\sigma(xu) = x\sigma(u)$$

для всех  $u_1, u_2, u \in U$ ,  $x \in K$ . Легко проверяется, что  $\text{Ker } \sigma = \{u \in U \mid \sigma(u) = 0\}$  является  $K$ -подмодулем в  $U$ , а образ  $\text{Im } \sigma$  —  $K$ -подмодулем в  $V$ .

Со всяким подмодулем  $U \subset V$  над  $K$  ассоциируется фактормодуль  $V/U = \{v + U \mid v \in V\}$  (факторгруппа аддитивной абелевой группы) с действием  $K$ , определённым по правилу

$$x(v + U) = xv + U.$$

Основная теорема о гомоморфизмах и две теоремы об изоморфизме, доказанные нами для групп, а затем для колец, дословно переносятся, с незначительным изменением доказательств, на модули.

После гл. 1, где рассматривались аксиомы типа M3), M4), и после основательной гл. 3 о представлениях групп (аксиомы M1), M3), M4)) примеры  $K$ -модулей, которые мы приведём, вряд ли вызовут ощущение новизны. Тем не менее стоит их обсудить и сопоставить друг с другом.

1) Всякая абелева группа  $A$  является  $\mathbb{Z}$ -модулем. Именно, отображение  $(n, a) \mapsto na$  из  $\mathbb{Z} \times A$  в  $A$  удовлетворяет всем аксиомам M1)–M4). Точка зрения на абелевы группы как на модули над  $\mathbb{Z}$  оказывается весьма полезной. В этом мы убедились в гл. 2 при описании конечно порождённых абелевых групп, где по сути дела была использована вся модульная терминология.

2) Всякая абелева группа  $A$  является модулем над своим кольцом эндоморфизмов  $\text{End } A$ . По определению  $\text{End } A$  состоит из всех отображений  $\varphi : A \rightarrow A$ , удовлетворяющих условию  $\varphi(a + a') = \varphi(a) + \varphi(a')$ . Операции сложения и умножения в  $\text{End } A$  вводятся естественным образом:

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

$$1(x) = x, \quad 0(x) = 0.$$

Отображение  $(\varphi, a) \mapsto \varphi(a)$  из  $\text{End } A \times A$  в  $A$  наделяет, очевидно,  $A$  структурой  $\text{End } A$ -модуля.

3) Векторное пространство  $V$  над полем  $P$  является, несомненно,  $P$ -модулем. Если нам дан ещё линейный оператор  $\mathcal{A} : V \rightarrow V$ , то мы наделим  $V$  структурой модуля  $V_{\mathcal{A}}$  над кольцом многочленов  $P[X]$ , полагая

$$f(X)v = f(\mathcal{A})v = \alpha_0 v + \alpha_1 \mathcal{A}v + \dots + \alpha_k \mathcal{A}^k v$$

для любого  $v \in V$  и любого многочлена  $f \in P[X]$ . Аксиомы M1–M4) выполнены, поскольку вместе с  $\mathcal{A}$  оператор  $f(\mathcal{A})$  будет также линейным и

$$(f + g)(\mathcal{A}) = f(\mathcal{A}) + g(\mathcal{A}), \quad (fg)(\mathcal{A}) = f(\mathcal{A})g(\mathcal{A})$$

(универсальное свойство колец многочленов). Подмодулями в  $V_{\mathcal{A}}$  будут служить  $\mathcal{A}$ -инвариантные подпространства. Различным линейным операторам одного и того же пространства  $V$  соответствуют, вообще говоря, различные (неизоморфные)  $P[X]$ -модули.

4) Произвольный левый идеал  $J$  кольца  $K$  наделён естественной структурой  $K$ -модуля с действием  $(x, y) \mapsto xy$ ,  $x \in K$ ,  $y \in J$ , индуцированным операцией умножения в  $K$ . В случае  $J = K$  кольцо  $K$  рассматривается как модуль  $_K K$  над собой. Этот взгляд на  $K$  приводит к плодотворным результатам.

5) Возвращаясь к предыдущему примеру, построим faktormodуль  $K/J = \{y + J \mid y \in K\}$ . Согласно общему определению  $(x, y + J) \mapsto xy + J$  — действие  $K$  на  $K/J$ . Заметим, что канонический эпиморфизм  $\pi : K \rightarrow K/J$ , являясь гомоморфизмом  $K$ -модулей, удовлетворяет соотношению  $\pi(xy) = xy + J = x(y + J) = x\pi(y)$ . Если же  $J$  — двусторонний идеал, то  $K/J$  — кольцо и  $\pi$  — гомоморфизм колец:  $\pi(xy) = \pi(x)\pi(y)$ .

Пересечение  $\cap_i V_i$ , любого семейства подмодулей  $V_i \subset V$  над  $K$  является подмодулем в  $V$ . В частности, пересечение всех подмодулей, содержащих заданное множество  $T \subset V$ , приводит к подмодулю  $\langle T \rangle$ , порождённому множеством  $T$  и состоящему из всевозможных элементов вида  $x_1 t_1 + \dots + x_s t_s$ , где  $x_i \in K$ ,  $t_i \in T$ . Заметим, кстати, что ненулевые элементы  $t_1, \dots, t_s \in V$  называются линейно зависимыми над  $K$ , если  $x_1 t_1 + \dots + x_s t_s = 0$ , где не все  $x_i$  равны нулю. Подмодуль, порожденный семейством  $\{V_1, \dots, V_m\}$  подмодулей  $V_i$ , называется их суммой и обозначается обычным образом:  $\sum_i V_i = V_1 + \dots + V_m$ .

Модуль  $V$  над  $K$ , порождённый единственным элементом  $v$ , называется циклическим. Он имеет вид  $V = Kv = \{xv \mid x \in K\}$ , где  $v \in V$ , и является аналогом циклической группы. В частности, циклический модуль  $_K K = K \cdot 1$  (см. пример 4) — аналог группы  $(\mathbb{Z}, +)$ .

Если  $V = Kv_1 + \dots + Kv_n$  — сумма конечного числа циклических модулей, то модуль  $V$  называется конечно порождённым или  $K$ -модулем конечного типа.

Легко проверяется, что отображение  $x \mapsto xv$  является гомоморфизмом модулей  $_K K \rightarrow Kv$ . Его ядро  $\text{Ann}(v) = \text{Ann}_K(v) = \{x \in K \mid xv = 0\}$  — левый идеал в  $K$ , называемый аннулятором (или кручением) элемента  $v$ . Таким образом,  $Kv \cong K/\text{Ann}(v)$ . Элемент  $v \in V$  с  $\text{Ann}(v) \neq 0$  называется периодическим. Модуль, все элементы которого периодические, тоже называется периодическим. Если  $V$  не содержит ненулевых периодических элементов, то говорят, что

$V$  — модуль без кручения.

Аннулятором (или кручением)  $K$ -модуля  $V$  называется множество

$$\text{Ann}(V) = \{a \in K \mid aV = 0\} = \bigcap_{v \in V} \text{Ann}(v)$$

Модуль называется точным, если  $\text{Ann}(V) = 0$ .

К тем же понятиям можно подойти с другой стороны. Пусть  $V(x)$  — множество элементов  $v \in V$ , аннулируемых элементом  $x \in K$ . Если  $K$  — целостное кольцо, то  $V(x) + V(y) \subset V(xy)$  и имеет смысл понятие подмодуля кручения

$$\text{Tor}(V) = \sum_{x \in K} V(x)$$

(кручение — от *torsion* (англ.)). В случае равенства  $\text{Tor}(V) = V$  говорят, что  $V$  — модуль кручения. Если же  $\text{Tor}(V) = 0$ , то мы снова приходим к понятию модуля без кручения.

Характерные примеры периодических модулей: а) всякая конечная абелева группа (периодический модуль конечного типа над  $\mathbb{Z}$ ; кручение —  $m\mathbb{Z}$  или просто показатель  $m$  группы); б) модуль  $V_A$  над  $P[X]$ , ассоциированный с линейным оператором  $\mathcal{A}$  (см. пример 3; кручение — главный идеал, порождённый минимальным многочленом оператора  $\mathcal{A}$ ).

Предложение 1.  $\text{Ann}(V)$  всегда является двусторонним идеалом кольца  $K$ . Полагая  $(x + \text{Ann}(V))v = xv$ , мы наделяем  $V$  структурой точного  $K/\text{Ann}(V)$ -модуля.

Доказательство. Положим  $A = \text{Ann}(V)$ . Ясно, что  $A$  — аддитивная подгруппа в  $K$ . Далее,  $(xax')v = xa(x'v) = (xa)v' = x(av') = x \cdot 0 = 0$  для любых  $x, x' \in K$ ,  $a \in A$ ,  $v \in V$ , откуда и следует, что  $KAK \subseteq A$ , т.е.  $A$  — двусторонний идеал в  $K$ . Если теперь  $x + A = x' + A$ , то  $x - x' \in A$ , откуда  $(x - x')v = 0$ , или  $xv = x'v$ . Стало быть,  $(x + A)v = (x' + A)v$ , т.е. действие факторкольца  $K/A$  на  $V$  определено корректно. Нетрудно проверить, что относительно этого действия  $V$  является  $(K/A)$ -модулем. Наконец,

$$(x + A)V = 0 \implies x + A \in \text{Ann}_{K/A}(V) \implies xV = 0 \implies x \in A.$$

Следовательно, лишь нулевой элемент в  $K/A$  аннулирует  $V$ .  $\square$

Из предложения 1 вытекает, что факторкольцо  $K/\text{Ann}(V)$  изоморфно подкольцу кольца  $\text{End}(V)$  (см. пример 2).

Если  $V, W$  — два  $K$ -модуля, то множество  $\text{Hom}_K(V, W)$  всех  $K$ -линейных гомоморфизмов  $\sigma : V \rightarrow W$  является абелевой группой относительно операции поточечного сложения гомоморфизмов:

$$\begin{aligned} (\sigma + \tau)(xv) &= \sigma(xv) + \tau(xv) = x\sigma(v) + x\tau(v) = \\ &= x(\sigma(v) + \tau(v)) = x((\sigma + \tau)(v)). \end{aligned}$$

Для модулей  $V, W$  над коммутативным кольцом  $K$  множество  $\text{Hom}_K(V, W)$  само является  $K$ -модулем, если под  $x\sigma$ ,  $x \in K$ ,  $\sigma \in \text{Hom}_K(V, W)$ , понимать отображение  $v \mapsto x(\sigma(v))$ :

$$(x\sigma)(yv) = x \cdot \sigma(yv) = x(y\sigma(v)) = (xy)\sigma(v) = \\ = (yx)\sigma(v) = y(x\sigma(v)) = y((x\sigma)(v)).$$

В случае  $W = V$  множество  $\text{End}_K(V) = \text{Hom}_K(V, V)$  является кольцом; умножением служит естественная композиция  $K$ -гомоморфизмов  $\varphi \circ \psi$ :

$$(\varphi \circ \psi)(xv) = \varphi(\psi(xv)) = \varphi(x\psi(v)) = x\varphi(\psi(v)) = x((\varphi \circ \psi)(v)).$$

Следует иметь в виду, что, рассматривая  $V$  как аддитивную абелеву группу, мы пишем  $\text{End}_{\mathbb{Z}}(V)$  и, вообще говоря,  $\text{End}_K(V)$  — собственное подкольцо в  $\text{End}_{\mathbb{Z}}(V)$ . В случае векторного пространства  $V$  над полем  $K$  обычно пишут  $\mathcal{L}(V) = \text{End}_K(V)$ , называя  $\mathcal{L}(V)$  *кольцом (или алгеброй) линейных операторов*.

Кольцо  $\text{End}_K(V)$   *$K$ -эндоморфизмы модуля  $V$  называют ещё централизатором кольца  $K$  на  $V$* . Его роль особенно заметна в случае неприводимых модулей. Модуль  $V$  над кольцом  $K$  называется *неприводимым (или простым)*, если: а)  $V \neq 0$ ; б)  $0, V$  — единственные подмодули в  $V$ ; в)  $KV \neq 0$  (это условие автоматически выполняется, если  $K$  содержит единицу). Ясно, что  *$K$ -модуль  $V \neq 0$  неприводим тогда и только тогда, когда  $V = Kv$  — циклический модуль при любом  $v \neq 0$  из  $V$* .

**Предложение 2** (лемма Шура). *Если  $V, W$  — два неприводимых  $K$ -модуля и  $\sigma$  — ненулевой  $K$ -гомоморфизм из  $V$  в  $W$ , то  $\sigma$  — изоморфизм. Далее,  $\text{End}_K(V)$  — кольцо с делением (тело) для любого неприводимого  $K$ -модуля  $V$ .*

Доказательство см. в § 4 гл. 3, где та же лемма Шура (теорема 1) доказана для неприводимых  $G$ -пространств.

**2. Свободные модули.** Мы называем  $K$ -модуль  $V$  (*внутренней*) прямой суммой своих подмодулей  $V_1, \dots, V_n$ , если

$$V = V_1 + \dots + V_n \quad \text{и} \quad V_i \cap \sum_{j \neq i} V_j = 0 \quad \text{для } i = 1, \dots, n.$$

Другими словами,  $V = V_1 \oplus \dots \oplus V_n$  (обозначение прямой суммы подмодулей), если любой элемент  $v \in V$  единственным образом записывается в виде линейной комбинации  $v = v_1 + \dots + v_n$ ,  $v_i \in V_i$ . *Внешняя прямая сумма  $K$ -модулей  $V_1, \dots, V_n$  определяется очевидным образом (как в случае колец), с действием  $x(v_1, \dots, v_n) = (xv_1, \dots, xv_n)$  элемента  $x \in K$  на строку  $(v_1, \dots, v_n)$ ,  $v_i \in V_i$ .*

Пусть, далее,  $V$  —  $K$ -модуль и  $\{v_1, \dots, v_n\}$  — конечное подмножество в  $V$ . Говорят, что  $\{v_1, \dots, v_n\}$  *порождает  $V$  свободно*, если  $V = Kv_1 + \dots + Kv_n$  и каждое отображение  $\varphi$  множества  $\{v_1, \dots, v_n\}$  в

какой-либо  $K$ -модуль  $W$  продолжается до  $K$ -гомоморфизма  $\tilde{\varphi} : V \rightarrow W$ , так что  $\tilde{\varphi}(v_i) = \varphi(v_i)$ ,  $1 \leq i \leq n$ .

Модуль  $V$  над  $K$ , свободно порождённый некоторым подмножеством  $\{v_1, \dots, v_n\}$ , называется *свободным модулем ранга  $n$* , а  $\{v_1, \dots, v_n\}$  — его (*свободным*) *базисом* над  $K$ .

**Предложение 3.** Эквивалентны утверждения:

- i) множество  $\{v_1, \dots, v_n\}$  порождает  $V$  свободно;
- ii) множество  $\{v_1, \dots, v_n\}$  линейно независимо и  $\langle v_1, \dots, v_n \rangle = V$ ;
- iii) каждый элемент  $v \in V$  однозначно записывается в виде  $v = \sum_i x_i v_i$ ,  $x_i \in K$ ;
- iv)  $V = Kv_1 \oplus \dots \oplus Kv_n$  — прямая сумма и  $\text{Ann}(v_i) = 0$ ;
- v)  $V \cong_K K \oplus \dots \oplus_K K$  — прямая сумма  $n$  экземпляров  $_K K$  (таким образом, свободный  $K$ -модуль ранга  $n$  относительно базиса  $\{v_1, \dots, v_n\}$  изоморчен модулю  $K^n$  строк  $(x_1, \dots, x_n)$  длины  $n$  с компонентами  $x_i \in K$ ).

**Доказательство** близко к рассуждениям, проведённым в [ВА II] для линейных пространств над полем, но нужно соблюдать некоторую осторожность, связанную либо с некоммутативностью кольца  $K$ , либо с существованием необратимых элементов в  $K$ .  $\square$

Имеются довольно сложные примеры некоммутативных колец с  $K^m \cong K^n$  при  $m \neq n$ , но коммутативные кольца в этом отношении ведут себя хорошо.

**Предложение 4.** Ранг конечно порождённого модуля над целостным кольцом  $K$  определён однозначно.

**Доказательство.** Пусть  $\{v_1, \dots, v_n\}$ ,  $\{u_1, \dots, u_m\}$  — два базиса свободного модуля  $V$  над  $K$ . Тогда

$$v_j = \sum_{i=1}^m a_{ij} u_i, \quad u_i = \sum_{k=1}^n b_{ki} v_k.$$

Ввиду коммутативности  $K$  для матриц  $A = (a_{ij})$  и  $B = (b_{kl})$  размеров  $m \times n$  и  $n \times m$  соответственно получаются соотношения

$$AB = E_m, \quad BA = E_n.$$

Вложив  $K$  в поле отношений  $Q(K)$ , мы получим посредством теоремы 3 из [ВА I, гл. 2, § 3] (верной для любого поля, а не только для  $\mathbb{R}$ ), что  $\min(n, m) \geq m$ ,  $\min(n, m) \geq n$ , откуда  $m = n$ . Добавим, что случай  $m < \infty$ ,  $n = \infty$  невозможен, поскольку в выражения для  $u_i$  входит лишь конечное число базисных элементов  $v_k$ , свободно порождающих весь модуль  $V$ .  $\square$

**Замечание.** В случае произвольного коммутативного кольца  $K$  с единицей будет достигнут тот же эффект, как в предложении 4, если выбрать в  $K$  некоторый максимальный идеал  $J$  и перейти к полю  $K/J$ . Детали мы опускаем.

Заметим, что, в отличие от ситуации в векторных пространствах, произвольно взятое порождающее множество свободного  $K$ -модуля не обязано содержать базис модуля. Например, два различных простых числа  $p, q$  всегда порождают  $\mathbb{Z}\mathbb{Z}$ , поскольку  $up + vq = 1$  для некоторых  $u, v \in \mathbb{Z}$ . Но  $\{p, q\}$  не является базисом, ибо  $p \cdot q - q \cdot p = 0$ , а  $\mathbb{Z}p, \mathbb{Z}q$  — собственные подмодули в  $\mathbb{Z}\mathbb{Z}$ .

Роль свободных модулей запрограммирована в их определении.

**Теорема 1.** *Каждый  $K$ -модуль конечного типа является гомоморфным образом свободного  $K$ -модуля конечного типа.*

**Доказательство.** Пусть  $U = \sum_{i=1}^n Ku_i$  —  $K$ -модуль, порождённый  $n$  элементами  $u_1, \dots, u_n$ . Возьмём свободный  $K$ -модуль  $V$  с базисом  $\{v_1, \dots, v_n\}$ . Его существование обеспечено предложением 3, v). Отображение  $\varphi : v_i \mapsto u_i$  продолжаемо в соответствии с определением свободного модуля до  $K$ -гомоморфизма  $\tilde{\varphi} : V \rightarrow U$ . Образ  $\text{Im } \tilde{\varphi}$  содержит порождающее множество модуля  $U$  и, стало быть, весь модуль  $U$ .  $\square$

Не всегда подмодуль свободного модуля свободен, даже если он является его прямым слагаемым. Вот простейший пример. Пусть  $K = \mathbb{Z}_6$ ,  $U = K(2 + 6\mathbb{Z})$ ,  $W = K(3 + 6\mathbb{Z})$ . Тогда  $K = U \oplus W$  — прямая сумма  $K$ -модулей  $U, W$ , ни один из которых не является свободным:  $|K| = 6$ , в то время как  $|U| = 3$ ,  $|W| = 2$ .

**Теорема 2.** *Пусть  $V = Kv_1 \oplus \dots \oplus Kv_n$  — свободный модуль ранга  $n$  над кольцом  $K$  главных идеалов. Тогда каждый его подмодуль  $U$  — свободный ранга  $t \leq n$ .*

**Доказательство.** Пусть сначала  $n = 1$ , т.е.  $V \cong K$ . Любой подмодуль  $U \subset V$  изоморден идеалу в  $K$  и, стало быть,  $U \cong (u) = Ku$ . Если  $u = 0$ , то  $U = 0$  (нулевой подмодуль можно считать свободным модулем нулевого ранга). Если же  $u \neq 0$ , то  $au \neq 0$  для всех  $0 \neq a \in K$ , поскольку  $K$  — целостное кольцо. Значит,  $U$  — свободный (циклический) модуль ранга 1. При  $n > 1$  рассуждаем по индукции.

Рассмотрим в  $V$  свободный подмодуль  $V' = Kv_2 \oplus \dots \oplus Kv_n$  ранга  $n - 1$ . Фактормодуль  $\bar{V} = V/V'$  свободный, с циклической образующей  $\bar{v}_1 = v_1 + V'$ . Он содержит подмодуль  $\bar{U} = (U + V')/V'$ . Если  $\bar{U} = 0$ , то  $U \subset V'$ , и тогда утверждение теоремы верно по предположению индукции.

Если же  $\bar{U} \neq 0$ , то рассуждение, проведённое выше для случая  $n = 1$ , показывает, что  $\bar{U}$  обладает циклической образующей  $\bar{u}_1 = u_1 + V'$ , где  $u_1 \in U$ .

Если ещё  $U \cap V' = 0$ , то

$$\begin{aligned} u \in U \implies \bar{u} = u + V' \in \bar{U} \implies \bar{u} = a_1 \bar{u}_1, \quad a_1 \in K \implies u - a_1 u_1 \in V' \implies \\ \implies u = a_1 u_1 \implies U = Ku_1 \text{ — свободный модуль ранга 1.} \end{aligned}$$

Пусть, наконец,  $U \cap V' \neq 0$ . По индукции подмодуль  $U \cap V'$  свободного модуля  $V'$  ранга  $n - 1$  обладает свободным базисом  $\{u_2, \dots, u_m\}$ , где  $0 < m - 1 \leq n - 1$ . Почти дословно повторяя проведённое выше

рассуждение, убеждаемся в том, что  $\{u_1, u_2, \dots, u_m\}$  — свободный  $K$ -базис для  $U$ . Действительно,

$$\begin{aligned} u \in U \implies \bar{u} = u + V' \in \bar{U} \implies \bar{u} = a_1 \bar{u}_1, a_1 \in K \implies \\ \implies u - a_1 u_1 \in U \cap V' \implies u - a_1 u_1 = a_2 u_2 + \dots + a_m u_m \implies \\ \implies u = a_1 u_1 + a_2 u_2 + \dots + a_m u_m, m \leq n. \end{aligned}$$

Согласно предложению 3, ii) нам нужно убедиться в линейной независимости образующих  $u_1, \dots, u_m$ . Но  $\sum_i x_i u_i = 0 \implies x_1 \bar{u}_1 = - \sum_{i>0} x_i \bar{u}_i = 0$  в  $\bar{V}$ . Значит,  $x_1 = 0$ , поскольку  $\bar{u}_1$  — базис в  $\bar{V}$ , а так как  $\{u_2, \dots, u_m\}$  — свободный базис в  $U \cap V'$ , то

$$x_2 u_2 + \dots + x_m u_m = 0 \implies x_2 = \dots = x_m = 0. \quad \square$$

**Следствие.** *Каждый подмодуль модуля конечного типа над кольцом главных идеалов сам является модулем конечного типа.*

Доказательство вытекает из теорем 1, 2 и из второй теоремы об изоморфизме (теоремы о соответствии между подмодулями).

Достаточно несложно получить полное описание модулей конечного типа над кольцом  $K$  главных идеалов. Но самые интересные случаи нами рассмотрены (периодические модули над  $\mathbb{Z}$  и над  $P[X]$  в гл. 2 и в [ВА II, гл. 2, § 3]). Демонстрацию же единого модульного подхода к другого рода задачам можно найти в списке дополнительной литературы.

**3. Целые элементы кольца.** Пусть  $K$  — целостное кольцо. Элемент  $t \in K$  называется *целым* (*целым над  $\mathbb{Z}$* ), если  $t$  — корень нормализованного многочлена  $X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{Z}[X]$ . В том случае, когда  $K$  — конечное алгебраическое расширение поля  $\mathbb{Q}$  или же  $K$  — поле, порождённое всеми комплексными алгебраическими числами, говорят о *целых алгебраических числах*, относя к ним, естественно, все элементы из  $\mathbb{Z}$ . Легко видеть (см. также гл. 5), что рациональное число  $t$  является целым алгебраическим тогда и только тогда, когда  $t \in \mathbb{Z}$ . Если, далее,  $a_0 u^n + a_1 u^{n-1} + \dots + a_n = 0$ , то  $(a_0 u)^n + a_0 a_1 (a_0 u)^{n-1} + \dots + a_0^n a_n = 0$ , а это значит, что *любое алгебраическое число, умноженное на подходящий элемент  $a_0 \in \mathbb{Z}$ , становится целым алгебраическим числом*.

Обращаясь к общему случаю, заметим, что  $K$  удобно трактовать как  $\mathbb{Z}$ -модуль. Любые элементы  $t_1, t_2, \dots, t_n \in K$  порождают в  $K$  подмодуль  $Kt_1 + Kt_2 + \dots + Kt_n$  конечного типа. Если, в частности,  $t$  — целый элемент и  $t^n + a_1 t^{n-1} + \dots + a_n = 0$ ,  $a_i \in \mathbb{Z}$ , то подкольцо  $\mathbb{Z}[t] \subset K$  является  $\mathbb{Z}$ -модулем конечного типа, поскольку  $\mathbb{Z}[t] = \mathbb{Z}1 + \mathbb{Z}t + \dots + \mathbb{Z}t^{n-1}$ . Обратно: пусть  $\mathbb{Z}[t]$  —  $\mathbb{Z}$ -модуль конечного типа с образующими  $v_1, \dots, v_n \in K$ . Тогда соотношения

$$tv_i = a_{i1}v_1 + a_{i2}v_2 + \dots + a_{in}v_n, \quad 1 \leq i \leq n,$$

с матрицей  $A = (a_{ij}) \in M_n(\mathbb{Z})$  приводят к выводу, что линейная однородная система

$$(t - a_{11})x_1 - a_{12}x_2 - \dots - a_{1n}x_n = 0,$$

$$-a_{n1}x_1 - a_{n2}x_2 - \dots + (t - a_{nn})x_n = 0,$$

рассматриваемая над полем отношений  $Q(K)$ , имеет ненулевое решение  $(x_1, \dots, x_n) = (v_1, \dots, v_n)$  (не все  $v_i$  равны нулю, поскольку  $1 \in \mathbb{Z}[t]$ ). Значит определитель системы равен нулю (см. [ВА I, гл. 3]) и  $t$  — корень нормализованного многочлена  $f(T) = \det(TE - A)$ . Мы доказали, что элемент  $t \in K$  является целым тогда и только тогда, когда подкольцо  $\mathbb{Z}[t] \subset K$  является  $\mathbb{Z}$ -модулем конечного типа.

**Теорема 3.** Целые элементы кольца  $K$  образуют в  $K$  подкольцо.

**Доказательство.** Пусть  $u, v \in K$  — целые элементы. Тогда

$$\mathbb{Z}[u, v] = \sum_{i \leq n, j \leq m} \mathbb{Z} u^i v^j$$

—  $\mathbb{Z}$ -модуль конечного типа. Так как  $\mathbb{Z}$  — кольцо главных идеалов, то следствие теоремы 2 (или непосредственная проверка) показывает, что подмодули  $\mathbb{Z}[u - v], \mathbb{Z}[uv]$  тоже являются  $\mathbb{Z}$ -модулями конечного типа. Согласно приведённому выше критерию элементы  $u - v, uv$  должны быть целыми.  $\square$

**Пример.** Корень  $\varepsilon$  любой степени из 1 является, очевидно, целым алгебраическим числом. По теореме 3 целочисленные линейные комбинации корней из 1 также будут целыми алгебраическими числами. В частности (см. доказательство предложения из § 4 гл. 3), значения  $\chi_\Phi(g)$ ,  $g \in G$ , характера  $\chi_\Phi$  любого линейного представления  $\Phi$  над  $\mathbb{C}$  конечной группы  $G$  являются целыми алгебраическими числами.

### УПРАЖНЕНИЯ

**1.** Используя общие результаты о модулях над  $\mathbb{C}[X]$ , наметить схему доказательства теоремы о ЖНФ (см. [ВА II]).

**2.** Используя общие результаты о модулях над  $\mathbb{Z}$ , наметить схему доказательства теоремы о конечно порождённых абелевых группах.

**3.** Пусть  $A = P[X_1, \dots, X_n]$  — кольцо многочленов от  $n$  переменных над полем  $P$ . Последовательность  $(f_1, \dots, f_r)$  из  $r$  многочленов  $f_i \in A$  называется *унимодулярной*, если  $Af_1 + Af_2 + \dots + Af_r = A$ , т.е.

$$u_1 f_1 + u_2 f_2 + \dots + u_r f_r = 1 \tag{*}$$

для некоторых  $u_i \in A$ ,  $1 \leq i \leq r$ .

Пусть, далее,  $V$  — модуль конечного типа над  $A$ . В связи с некоторыми тонкими вопросами из алгебраической геометрии французский математик Ж.-П. Серр (1955 г.) выдвинул гипотезу

$$\{V \oplus A^s \cong A^{s+t} \implies V \cong A^t\},$$

которой была придана следующая изящная форма: всякое соотношение (\*) можно записать в виде равенства

$$\left| \begin{array}{cccc} f_1 & f_2 & \dots & f_r \\ u_{21} & u_{22} & \dots & u_{2r} \\ \cdots & \cdots & \cdots & \cdots \\ u_{r1} & u_{r2} & \dots & u_{rr} \end{array} \right| = 1$$

при подходящих  $u_{ij} \in A$ . Это утверждение, несмотря на свою кажущуюся простоту, было доказано лишь в 1976 г. независимо А.А. Суслиным (Россия) и Д. Квилленом (США). Попробуйте это реализовать при небольших  $n$  и  $r$ .

Основная идея — изучить действие группы  $\mathrm{GL}(r, A[X_1, \dots, X_{n-1}])$  на множестве унимодулярных последовательностей и использовать индукцию по  $n$ . С доказательством можно познакомиться по оригинальной статье: Суслин А.А.// ДАН СССР. — 1976. — Т. 229, № 5. — С. 1063–1066; или по докладу на семинаре Н. Бурбаки: Ferrand D.// Sémin. N. Bourbaki, 28 ème année, 1975/76, Juin 1976. Изложение вполне элементарное. Какой ценой оно достигнуто, можно судить по более раннему докладу на семинаре Н. Бурбаки: Bass H.// Sémin. N. Bourbaki, 26ème année, 1973/74, Juin 1974. В указанной литературе содержатся постановки нерешённых задач. Весь круг вопросов очень хорош для обсуждения на спецсеминаре.

## § 4. Алгебры над полем

**1. Определения и примеры алгебр.** Мы уже пользовались понятием алгебры в самых разных ситуациях (см. гл. 1 § 1, а также [ВА I, II]), поэтому определение ниже приводится фактически лишь для полноты изложения.

**Определение. Алгеброй** (или *линейной алгеброй*) над полем  $P$  называется пара, состоящая из кольца  $(A, +, \cdot)$  и векторного пространства  $A$  над  $P$  (базисное множество  $A$  у кольца и векторного пространства одно и то же; одинаковы также операция сложения  $+$  и нулевой элемент  $0$ ). При этом

$$\lambda(xy) = (\lambda x)y = x(\lambda y)$$

для всех  $\lambda \in P$ ,  $x, y \in A$ . Алгебра называется *ассоциативной*, если ассоциативно кольцо  $(A, +, \cdot)$ . Размерность над  $P$  векторного пространства  $A$  называется также *размерностью алгебры*  $A$ .

На алгебры переносятся, с незначительными уточнениями, основные понятия теории колец. Так, *подалгеброй* алгебры  $A$  считается всякое подкольцо  $B$ , являющееся одновременно подпространством векторного пространства  $A$ . Если  $T$  — подмножество в  $A$ , то порождённая им подалгебра  $P[T]$  является пересечением всех подалгебр в  $A$ , содержащих  $T$ . Аналогичным образом определяются идеалы и факторалгебры по ним. Гомоморфизмами алгебр служат гомоморфизмы колец, являющиеся вместе с тем  $P$ -линейными отображениями.

*Центр*  $Z(A)$  *ассоциативной алгебры*  $A$  определяется как множество всех элементов  $a \in A$ , перестановочных с каждым элементом из  $A$ :  $a \in Z(A) \iff ax = xa \quad \forall x \in A$ . Очевидно, что центр  $Z(A)$  — подалгебра в  $A$ . Равенство  $Z(A) = A$  имеет место тогда и только тогда, когда  $A$  — коммутативная алгебра.

Если  $A$  — ассоциативная алгебра с единицей 1, то непосредственно проверяется, что  $\lambda \cdot 1 \in Z(A)$ , причём соответствие  $\lambda \mapsto \lambda \cdot 1$   $\forall \lambda \in P$ , определяет мономорфное отображение  $P$  в  $A$ . В этом смысле под алгеброй  $A$  можно понимать кольцо  $A$  вместе с выделенным подполем, содержащимся в центре  $Z(A)$ .

Приведём некоторые примеры ассоциативных алгебр.

1) Расширение  $F \supset P$  конечной степени  $[F : P]$  поля  $P$  является, очевидно, коммутативной ассоциативной алгеброй (с единицей) конечной размерности  $\dim_P F = [F : P]$ .

2) Кольцо многочленов  $K = P[X_1, \dots, X_n]$  с коэффициентами в поле  $P$  несёт естественную структуру бесконечномерной коммутативной ассоциативной алгебры над полем  $P$ . Заметим, что

$$K = K_0 \oplus K_1 \oplus K_2 \oplus \dots$$

— прямая сумма конечномерных векторных подпространств  $K_m$  однородных многочленов степени  $m$  ( $K_0 = P$ ), причём  $K_i K_j \subset K_{i+j}$ . Алгебры подобного типа называются *градуированными*.

3) Коммутативная алгебра  $X_{\mathbb{C}}(G)$  с единицей  $\chi_1$ , порождённая над  $\mathbb{C}$  всеми характерами конечной группы  $G$ , имеет размерность  $r$ , равную числу классов сопряжённых элементов в  $G$ .

4) Кольцо  $M_n(P)$  квадратных матриц порядка  $n$  с коэффициентами в поле  $P$  является алгеброй размерности  $n^2$  над  $P$ . Базисные элементы  $\{E_{ij} \mid i, j = 1, 2, \dots, n\}$  алгебры  $M_n(P)$  перемножаются по правилу  $E_{ik} E_{lj} = \delta_{kl} E_{ij}$ . Согласно теореме 4 из [ВА I, § 3, гл. 2] центр  $Z(M_n(P)) = \{\lambda E\} \cong P$ .

Назовём ассоциативную алгебру  $A$  с единицей *центральной простой над полем*  $P$ , если  $Z(A) \cong P$  и в  $A$  нет двусторонних идеалов, отличных от 0 и  $A$ .

**Предложение 1.**  $M_n(P)$  — *центральная простая алгебра*.

**Доказательство.** Пусть  $J$  — идеал в  $M_n(P)$ , отличный от нулевого, и пусть

$$0 \neq a = \sum_{ij} \alpha_{ij} E_{ij} \in J.$$

Если  $\alpha_{kl} \neq 0$ , то  $E_{st} = \alpha_{kl}^{-1} E_{sk} \cdot a \cdot E_{lt} \in J$  при любых  $s, t = 1, \dots, n$ , и, стало быть,  $J = M_n(P)$ .  $\square$

Аналогичное утверждение справедливо для полной матричной алгебры  $M_n(D)$  над произвольным телом  $D$ . Исключительно важная

теорема Веддербарна, а в более общем контексте — теорема Веддербарна–Артина гласит, что *всякая конечномерная ассоциативная простая алгебра над полем  $P$  изоморфна  $M_n(D)$ , где натуральное число  $n$  определено однозначно, а тело  $D$  (являющееся алгеброй конечной размерности над  $P$ ) — с точностью до изоморфизма.*

Матричная алгебра  $M_n(P)$  обладает ещё следующим универсальным свойством.

**Предложение 2.** *Всякая  $n$ -мерная ассоциативная алгебра  $A$  над полем  $P$  изоморфна некоторой подалгебре в  $M_k(P)$ , где  $k \leq n+1$ .*

**Доказательство.** Будем сначала считать  $A$  алгеброй с 1 и вложим её в  $M_n(P)$ . С этой целью каждому элементу  $a \in A$  поставим в соответствие линейный оператор  $L_a : x \mapsto ax$  на векторном пространстве  $A$ . Линейность  $L_a$  является следствием билинейности операции умножения в  $A$ . Так как, очевидно,  $L_{\lambda a} = \lambda L_a$ ,  $L_{a+b} = L_a + L_b$ ,  $L_{ab} = L_a L_b$  (ассоциативность) и  $L_1 = \mathcal{E}$ , то отображение  $a \mapsto L_a$  является гомоморфизмом. Его инъективность обеспечена существованием единичного элемента:  $a \neq 0 \implies L_a \cdot 1 = a \cdot 1 = a$ ,  $L_a \neq 0$ .

Пусть теперь  $A$  — алгебра без единицы. Введём в рассмотрение векторное пространство  $\tilde{A} = P \oplus A$  и определим на нём умножение, полагая

$$(\lambda, a)(\lambda', a') = (\lambda\lambda', aa' + \lambda a' + \lambda' a).$$

Легко проверяется, что с этим законом умножения  $\tilde{A}$  является алгеброй над  $P$  с единичным элементом  $(1, 0)$ .

Так как  $\dim_P \tilde{A} = \dim_P A + 1 = n + 1$ , то предыдущее рассуждение позволяет вложить  $\tilde{A}$ , а вместе с тем и  $A$  в  $M_{n+1}(P)$ .  $\square$

Нетрудно усмотреть полное сходство в доказательствах предложения 2 и теоремы Кэли [ВА I] для конечных групп. В обоих случаях используется регулярное представление. Более общо: под *представлением алгебры  $A$  над  $P$*  понимается любой гомоморфизм

$$A \longrightarrow \mathcal{L}(V) = \text{End}_F(V),$$

где  $F \supset P$  — некоторое расширение поля  $P$ . Другими словами, векторное пространство  $V$  над  $F$  снабжается структурой левого  $A$ -модуля в смысле определений § 3, причём

$$(\lambda x) \cdot v = x \cdot (\lambda v) \quad \forall \lambda \in P, x \in A, v \in V.$$

Выбрав в  $V$  какой-нибудь базис, мы придём, как и в случае групп, к матричному представлению  $A \longrightarrow M_r(F)$ , где  $r = \dim_F(V)$ .

**2. Алгебры с делением (тела).** Как показывает сформулированная выше теорема Веддербарна, изучение алгебр с делением — важная составная часть общей структурной теории ассоциативных

алгебр. Лемма Шура (предложение 2 из § 3) также подтверждает это соображение. Прежде чем приводить какие-либо результаты об алгебрах с делением, остановимся на одном вспомогательном утверждении.

**Предложение 3.** В ассоциативной алгебре  $A$  (с единичным элементом 1) размерности  $n$  над полем  $P$  каждый элемент  $a \in A$  является корнем многочлена  $\mu_a \in P[X]$  степени  $\leq n$ . Элемент  $a \in A$  обратим в точности тогда, когда  $\mu_a(0) \neq 0$ . Если в  $A$  нет делителей нуля, то  $A$  — алгебра с делением. Если поле  $P$  алгебраически замкнуто, то  $n = 1$  и  $A = P$ .

**Доказательство.** В силу конечномерности  $A$  элементы  $1, a, a^2, \dots$  не могут быть все линейно независимыми над  $P$ . Стало быть, найдётся нормализованный многочлен  $\mu_a(X) = X^m + \alpha_1 X^{m-1} + \dots + \alpha_m$  наименьшей степени  $m \leq n$  с коэффициентами  $\alpha_i \in P$  такой, что  $\mu_a(a) = 0$ . Если  $\alpha_m \neq 0$ , то соотношение  $\mu_a(a) = 0$ , переписанное в виде

$$[-\alpha_m^{-1}(a^{m-1} + \alpha_1 a^{m-2} + \dots + \alpha_{m-1})]a = 1,$$

показывает, что  $a$  — обратимый элемент.

Обратно: предположим, что  $a \in A$  не является делителем нуля, но  $\alpha_m = 0$ . Тогда

$$(a^{m-1} + \alpha_1 a^{m-2} + \dots + \alpha_{m-1})a = 0 \implies$$

$$\implies a^{m-1} + \alpha_1 a^{m-2} + \dots + \alpha_{m-1} = 0,$$

что противоречит минимальности  $\mu_a(X)$ . Значит,  $\alpha_m \neq 0$ . В частности, все элементы в  $A$ , не являющиеся делителями нуля, обратимы.

Если поле  $P$  алгебраически замкнуто, то

$$\mu_a(X) = (X - c_1) \dots (X - c_m), \quad c_i \in P,$$

откуда

$$(a - c_1)b = 0, \quad b = (a - c_2) \dots (a - c_m) \neq 0.$$

Отсутствие делителей нуля в  $A$  оставляет единственную возможность:  $m = 1$  и  $a - c_1 = 0$ ,  $a = c_1 \in P$ . Так как это верно для любого элемента  $a \in A$ , то  $A = P$ .  $\square$

Мы видим, что свойства алгебры с делением существенно зависят от основного поля  $P$ . Естественно, что исторически алгебры с делением над полем вещественных чисел  $\mathbb{R}$  вызывали особый интерес. Существование поля  $\mathbb{C} = \mathbb{R} + i\mathbb{R}$  давало повод к поискам других “гиперкомплексных” систем. В гл. 1, § 1, п. 5 была рассмотрена алгебра кватернионов  $\mathbb{H}$ , являющаяся ассоциативной, но некоммутативной алгеброй с делением. Место, занимаемое кватернионами, хорошо выявляется следующей замечательной теоремой с красивым доказательством.

**Теорема 1** (Г. Фробениус). *Над полем  $\mathbb{R}$  существуют лишь три конечномерные ассоциативные алгебры с делением:  $\mathbb{R}$ ,  $\mathbb{C}$  и  $\mathbb{H}$ .*

Прежде чем приступить к доказательству, остановимся на аддитивной структуре алгебры с делением  $A$ . В рассуждениях ниже существенно то известное нам из [ВА I, ВА II] обстоятельство, что минимальный многочлен  $\mu_a(t)$  (см. предложение 3) любого элемента  $0 \neq a \notin \mathbb{R}$  должен быть неприводимым и, стало быть, квадратичным. Заметим ещё, что  $\mu_a(t)$  — есть не что иное, как минимальный многочлен линейного оператора  $L_a : x \mapsto ax$  на  $A$ . Более конкретно:  $\mu_x(t) = t - \alpha$  или  $t^2 - 2\alpha t + \beta$ ,  $\alpha^2 < \beta$ . Если  $x \notin \mathbb{R}$ , то, положив  $y = x - \alpha$ , будем иметь  $\mu_y(t) = t^2 + (\beta - \alpha^2)$ . Итак, каждый элемент из  $A$  имеет вид  $\alpha + y$ , где  $\alpha \in \mathbb{R}$ ,  $y = 0$  или  $y^2 = \gamma < 0$ ,  $\gamma \in \mathbb{R}$ .

**Лемма 1.** *Подмножество*

$$A' = \{u \in A \mid u^2 \in \mathbb{R}, u^2 \leq 0\}$$

*является векторным подпространством в  $A$ .*

**Доказательство.** Ясно, что  $u \in A'$ ,  $\alpha \in \mathbb{R} \implies \alpha u \in A'$ , поэтому достаточно убедиться в справедливости импликации  $u, v \in A' \implies u + v \in A'$  для непропорциональных векторов  $u, v$ .

Сначала проверим, что линейная зависимость  $u = \alpha v + \beta$  с  $\alpha, \beta \in \mathbb{R}$  невозможна. В самом деле, по условию  $uv \neq 0$  и

$$u^2 = \gamma < 0, \quad v^2 = \delta < 0.$$

Поэтому

$$u = \alpha v + \beta \implies \gamma = u^2 = (\alpha v + \beta)^2 = \alpha^2 \delta + 2\alpha \beta v + \beta^2.$$

Так как  $v \notin \mathbb{R}$ , то  $\alpha \beta = 0$ , т.е.  $\alpha = 0$  или  $\beta = 0$ . Если  $\alpha = 0$ , то  $u \in \mathbb{R}$ , а если  $\beta = 0$ , то  $u$  пропорционально  $v$ . Обе возможности заранее исключались.

Итак, линейная независимость  $u, v \in A'$  приводит к линейной независимости  $1, u, v$ . Оба элемента  $u + v, u - v$  — корни квадратных уравнений, т.е.

$$(u + v)^2 = p(u + v) + q, \quad (u - v)^2 = r(u - v) + s, \quad p, q, r, s \in \mathbb{R}.$$

Используя соотношения

$$(u \pm v)^2 = u^2 \pm (uv + vu) + v^2, \quad u^2 = \gamma, \quad v^2 = \delta,$$

будем иметь

$$\gamma + \delta + (uv + vu) = p(u + v) + q,$$

$$\gamma + \delta - (uv + vu) = r(u - v) + s.$$

Складывая, находим

$$(p + r)u + (p - r)v + (q + s - 2\gamma - 2\delta) = 0.$$

Но, как мы видели,  $u, v, 1$  линейно независимы, поэтому  $p = r = 0$ . Стало быть,  $(u + v)^2 = q \in \mathbb{R}$ , а так как  $u + v \notin \mathbb{R}$ , то  $q < 0$ . Это и значит, что  $u + v \in A'$ , т.е.  $A'$  — подпространство в  $A$ .  $\square$

**Доказательство теоремы 1.** Для  $u \in A'$  пишем  $u^2 = -q(u)$ , где  $q(u) \in \mathbb{R}$  и  $q(u) \geq 0$ . Кроме того,  $q(u) = 0 \iff u = 0$ . Очевидно,  $q(\alpha u) = \alpha^2 q(u)$  и

$$f(u, v) := q(u + v) - q(u) - q(v) = -(uv + vu)$$

— симметричная билинейная форма на  $A$ , отвечающая положительно определённой квадратичной форме  $q$ .

Если  $A = \mathbb{R}$ , то рассуждения заканчиваются. Пусть  $A \neq \mathbb{R}$ . Тогда  $A' \neq 0$ , и мы можем выбрать вектор  $\mathbf{i} \in A$  с  $q(\mathbf{i}) = 1$ , т.е.  $\mathbf{i}^2 = -1$ . С точностью до изоморфизма получаем равенство  $\mathbb{R}[\mathbf{i}] = \mathbb{C} = \mathbb{R} + \mathbb{R}\mathbf{i}$ . Если  $A = \mathbb{C}$ , то наши рассуждения снова заканчиваются.

Считаем  $A \not\cong \mathbb{C}$ . Тогда  $A' \not\cong \mathbb{R}\mathbf{i}$ , и можно выбрать элемент  $\mathbf{j} \perp \mathbb{R}\mathbf{i}$ ,  $q(\mathbf{j}) = 1$ . В этом случае  $\mathbf{j}^2 = -1$  и  $\mathbf{ij} + \mathbf{ji} = -f(\mathbf{i}, \mathbf{j}) = 0$ , так что  $\mathbf{ij} = -\mathbf{ji}$ . Полагая  $\mathbf{k} = \mathbf{ij}$ , получим  $\mathbf{k}^2 = -1$ ,  $\mathbf{ik} + \mathbf{ki} = 0 = \mathbf{jk} + \mathbf{kj}$ . Следовательно,  $\mathbf{k} \in A'$  и  $\mathbf{k} \perp \mathbf{i}, \mathbf{j}$ . Стало быть,  $1, \mathbf{i}, \mathbf{j}, \mathbf{k}$  линейно независимы и

$$\mathbb{R} + \mathbb{R}\mathbf{i} + \mathbb{R}\mathbf{j} + \mathbb{R}\mathbf{k} = \mathbb{H}$$

— алгебра кватернионов.

Если  $A \not\cong \mathbb{H}$ , то существует  $\mathbf{l} \in A'$  с  $q(\mathbf{l}) = 1$  и  $\mathbf{l} \perp \mathbf{i}, \mathbf{j}, \mathbf{k}$ . Другими словами,

$$\mathbf{li} = -\mathbf{il}, \quad \mathbf{lj} = -\mathbf{jl}, \quad \mathbf{lk} = -\mathbf{kl}.$$

Однако в силу ассоциативности умножения в  $A$  первые два соотношения дают

$$\mathbf{lk} = \mathbf{l}(\mathbf{ij}) = (\mathbf{li})\mathbf{j} = -(\mathbf{il})\mathbf{j} = -\mathbf{i}(\mathbf{lj}) = \mathbf{i}(\mathbf{jl}) = (\mathbf{ij})\mathbf{l} = \mathbf{kl}.$$

Получается противоречие с третьим соотношением. Значит,  $A = \mathbb{H}$ .  $\square$

**Замечание.** Сравнительно недавно на основе глубоких топологических соображений было доказано, что *над  $\mathbb{R}$  всякая конечно-мерная алгебра с делением (не обязательно ассоциативная) имеет размерность 1, 2, 4 или 8. Все возможности реализуются*.

В начале XX века Веддербарном был получен результат о конечных телах, имеющий важное значение для геометрии. Эту теорему мы сейчас докажем, опираясь, правда, на некоторые элементарные свойства круговых многочленов  $\Phi_n(X)$ , устанавливаемые в следующей главе. Порочного круга при этом не возникнет.

**Теорема 2** (Веддербарн). *Каждое конечное ассоциативное кольцо с делением коммутативно, т.е. является полем.*

**Доказательство.** Пусть  $D$  — конечное кольцо с делением,  $Z = Z(D)$  — его центр. Очевидно, что  $Z$  — поле и  $D$  — конечномерное

векторное пространство над  $Z$ :

$$D = Ze_1 + Ze_2 + \dots + Ze_n.$$

Согласно результатам, устанавливаемым в гл. 5, § 2,  $Z = \mathbb{F}_q$  для некоторого  $q = p^m$ , так что  $|D| = q^n$ . Пусть, далее,  $x \in D \setminus Z$ . Перестановочные с  $x$  элементы образуют множество  $C(x) = \{y \in D \mid yx = xy\}$ , замкнутое относительно операций сложения и умножения. Другими словами,  $C(x)$  — подалгебра с делением в  $D$ , содержащая  $Z$ . Если  $q^d$  — число элементов в  $C(x)$ , то  $d = d(x)$  — делитель  $n$ ,  $d < n$ , поскольку, интерпретируя  $D$  как левое векторное пространство

$$D = C(x)f_1 + \dots + C(x)f_r$$

над  $C(x)$ , мы имеем  $q^n = |C(x)|^r = q^{dr}$ . Заметим теперь, что  $Z^*$  — центр мультиликативной группы  $D^*$ , а  $(q^n - 1)/(q^d - 1) = (D^* : C(x)^*)$  — число элементов, сопряжённых с  $x$  в  $D^*$ . Поэтому формула (2') из § 3 гл. 1 принимает вид

$$q^n - 1 = |D^*| = (q - 1) + \sum_d \frac{q^n - 1}{q^d - 1}, \quad (*)$$

где  $d$  пробегает некоторое множество делителей  $n$ , меньших  $n$ .

Свойства кругового многочлена  $\Phi_n(X)$  (см. упр. 6 из § 2 гл. 5) показывают, что целое число  $\Phi_n(q)$  делит как  $q^n - 1$ , так и  $(q^n - 1)/(q^d - 1)$  при  $d \mid n$ ,  $d < n$ . В таком случае согласно (\*)  $\Phi_n(q) \mid (q - 1)$ , а это влечёт (см. упр. 7 из § 1) равенство  $n = 1$  и, стало быть, коммутативность  $D = Z$ .  $\square$

**3. Групповые алгебры и модули над ними.** В связи с регулярным представлением конечной группы  $G$  в § 1 из гл. 3 вводилось векторное пространство  $\langle e_g \mid g \in G \rangle$  над полем  $K$ . Мы превратим его теперь в  $K$ -алгебру, полагая  $e_g e_h = e_{gh}$  и распространяя это правило по линейности на произвольные “векторы”  $\sum \alpha_g e_g$ ,  $\alpha_g \in K$ . Для упрощения записи  $e_g$  обычно заменяют на  $g$  и рассматривают множество  $K[G]$  всевозможных формальных сумм  $\sum \alpha_g g$ ,  $\alpha_g \in K$ . По определению

$$\sum_g \alpha_g g = \sum_g \beta_g g \iff \alpha_g = \beta_g \quad \forall g \in G.$$

Операции над формальными суммами

$$\begin{aligned} \sum_g \alpha_g g + \sum_g \beta_g g &= \sum_g (\alpha_g + \beta_g) g, \\ \lambda \left( \sum_g \alpha_g g \right) &= \sum_g (\lambda \alpha_g) g, \end{aligned} \quad (1)$$

$$\left( \sum_g \alpha_g g \right) \left( \sum_h \beta_h h \right) = \sum_{g,h} \alpha_g \beta_h g h = \sum_u \gamma_u u, \quad \gamma_u = \sum_g \alpha_g \beta_{g^{-1}} u$$

задают на  $K[G]$  структуру ассоциативной алгебры. Принято называть  $K[G]$  групповой алгеброй конечной группы  $G$  над полем  $K$ . Базисными элементами пространства  $K[G]$  служат формальные произведения  $1 \cdot g$ ,  $g \in G$ , отождествляемые с элементами  $g \in G$ ;  $\dim_K K[G] = |G|$ . Таким образом, группа  $G$  считается вложенной в алгебру  $K[G]$ . Единичный элемент  $e \in G$  является единицей в  $K[G]$ . В том случае, когда  $K$  — коммутативное ассоциативное кольцо с единицей, получается групповое кольцо  $K[G]$  группы  $G$  над  $K$ .

Кроме того, аналогичная конструкция применима к произвольной, не обязательно конечной группе  $G$ , если условиться рассматривать лишь суммы  $\sum \alpha_g g$  с конечным числом отличных от нуля коэффициентов. Удобно также интерпретировать  $S = \sum \alpha_g g$  как функцию на группе  $G$  (со значениями  $S(g) = \alpha_g$  в  $K$ ), равную почти всюду нулю (т.е. с конечным числом отличных от нуля значений). При этом формулам (1) отвечают операции поточечного сложения

$$(S_1 + S_2)(g) = S_1(g) + S_2(g)$$

и свёртка функций

$$S_3 = S_1 * S_2, \quad S_3(u) = \sum_g S_1(g)S_2(g^{-1}u).$$

Теория групповых колец — обширный раздел алгебры, имеющий собственную проблематику, но для нас  $K[G]$  — лишь иллюстрация общих понятий, введённых в последних двух главах.

**Теорема 3.** *Существует взаимно однозначное соответствие между  $K[G]$ -модулями, являющимися конечномерными векторными пространствами над полем  $K$ , и линейными представлениями группы  $G$ .*

**Доказательство.** Пусть  $(\Phi, V)$  — представление группы  $G$ . Продолжим  $\Phi$  по линейности на элементы из  $K[G]$ , определяя

$$\tilde{\Phi}\left(\sum \alpha_g g\right) = \sum \alpha_g \Phi(g),$$

и положим

$$\left(\sum \alpha_g g\right) \circ v = \sum \alpha_g \Phi(g)v \quad \forall v \in V.$$

Операция  $\circ$  вводит на  $V$  структуру  $K[G]$ -модуля в обычном понимании этого слова. Заметим, что

$$\begin{aligned} \left(\sum \alpha_g g\right) \circ (\lambda v) &= \sum \alpha_g \Phi(g)(\lambda v) = \sum \alpha_g \lambda \Phi(g)v = \\ &= \lambda \left(\sum \alpha_g \Phi(g)v\right) = \lambda \left(\left(\sum \alpha_g g\right) \circ v\right), \end{aligned}$$

т.е. умножения на скаляры в  $V$  и в  $K[G]$  согласованы. Пару  $(\tilde{\Phi}, V)$  естественно называть линейным представлением алгебры  $K[G]$ .

Обратно: если  $V$  — векторное пространство над  $K$ , являющееся модулем над  $K[G]$  с действием

$$\left( \sum \alpha_g g, v \right) \mapsto \left( \sum \alpha_g g \right) \circ v,$$

то, полагая

$$\tilde{\Phi} \left( \sum \alpha_g g \right) v = \left( \sum \alpha_g g \right) \circ v,$$

мы определим гомоморфизм  $\tilde{\Phi} : K[G] \rightarrow \text{End}_K(V)$  (т. е. представление алгебры  $K[G]$ ), ограничение которого  $\Phi = \tilde{\Phi}|_G$  на  $G$  даст нам представление группы  $G$ .  $\square$

В соответствии с теоремой 3 пространство представления  $V$  группы  $G$  часто называют *модулем представления* группы  $G$  или, коротко, —  *$G$ -модулем*. Соответствующие терминологические изменения касаются других понятий теории представлений.

Пусть, далее,  $G$  — конечная группа,  $K = \mathbb{C}$  — поле комплексных чисел. Согласно результатам гл. 3 каждый неприводимый (или, говорят ещё, *простой*)  $G$ -модуль над  $\mathbb{C}$  (т.е.  $\mathbb{C}[G]$ -модуль) с характером  $\chi_i$  изоморден некоторому левому идеалу  $J_i$  алгебры  $\mathbb{C}[G]$  (см. в этой связи пример 4 из § 3). Если  $\dim_{\mathbb{C}}[G] = n_i$ , то  $\mathbb{C}[G]$  содержит прямую сумму

$$A_i = J_{i,1} \oplus \dots \oplus J_{i,n_i}$$

левых идеалов,  $\mathbb{C}[G]$ -изоморфных  $J = J_{i,1}$ . Выбирая в каждом классе изоморфных левых идеалов по одному представителю  $J_i$ , мы можем написать разложение

$$\mathbb{C}[G] = A_1 \oplus A_2 \oplus \dots \oplus A_r, \quad (2)$$

соответствующее разложению регулярного представления группы  $G$ . Заметим, что каждая из компонент  $A_i$  определена однозначно.

Если теперь  $J$  — минимальный левый идеал алгебры  $\mathbb{C}[G]$  и  $t \in \mathbb{C}[G]$ , то  $Jt$  — тоже минимальный левый идеал (возможно, нулевой). Стало быть, отображение  $\varphi : J \rightarrow Jt$ , определённое соотвествием  $v \mapsto vt$  ( $v \in J$ ), является либо нулевым отображением, либо  $\mathbb{C}[G]$ -изоморфизмом, поскольку  $xv \in J$  для любого  $x \in \mathbb{C}[G]$  и  $\varphi(xv) = (xv)t = x(vt) = x\varphi(v)$ . По этой причине  $J \subset A_i \implies Jt \subset A_i \forall t \in \mathbb{C}[G]$  и, следовательно,  $A_i$  — двусторонний идеал в  $\mathbb{C}[G]$ . Разложение (2) прямое, так что

$$i \neq j \implies A_i A_j \subset A_i \cap A_j = 0.$$

Мы собираемся получить более точную информацию о разложении (2), опираясь на развитую в гл. 3 теорию характеров. Вначале найдём центр  $Z(\mathbb{C}[G])$  групповой алгебры  $\mathbb{C}[G]$ . По определению

$$z \in Z(\mathbb{C}[G]) \iff zg = gz \quad \forall g \in G.$$

Если  $z = \sum_{h \in G} \gamma_h h$ , то

$$\sum_{t \in G} \gamma_{g^{-1}t} t = g \left( \sum_h \gamma_h h \right) = \left( \sum_h \gamma_h h \right) g = \sum_{t \in G} \gamma_{tg^{-1}} t,$$

откуда  $\gamma_{g^{-1}t} = \gamma_{tg^{-1}}$   $\forall t \in G$ . Положив  $t = gh$ , получим  $\gamma_h = \gamma_{ghg^{-1}}$ . Это значит, что

$$Z(\mathbb{C}[G]) = \langle K_1, K_2, \dots, K_r \rangle_{\mathbb{C}},$$

где

$$K_i = \sum_{g \in \mathcal{K}_i} g, \quad \mathcal{K}_i = g_i^G, \quad i = 1, 2, \dots, r \quad (3)$$

( $g_1, g_2, \dots, g_r$  — представители классов сопряжённых элементов группы  $G$ ). Понятно, что  $K_1, K_2, \dots, K_r$  — линейно независимые элементы, и, стало быть,  $\dim_{\mathbb{C}} Z(\mathbb{C}[G]) = r$ .

Каждому элементу  $a \in A_i$  поставим в соответствие линейный оператор  $L_a^{(i)}$ , действующий на минимальном левом идеале  $J_i = J_{i,1}$  по правилу  $L_a^{(i)}(v) = av$ ,  $v \in J_i$ . Так как, очевидно,

$$L_{\lambda a}^{(i)} = \lambda L_a^{(i)}, \quad L_{a+b}^{(i)} = L_a^{(i)} + L_b^{(i)}, \quad L_{ab}^{(i)} = L_a^{(i)} L_b^{(i)},$$

то  $\varphi : a \mapsto L_a^{(i)}$  — гомоморфизм алгебры  $A_i$  в алгебру эндоморфизмов  $\text{End}_{\mathbb{C}} J_i \cong M_{n_i}(\mathbb{C})$ . Предположим, что  $0 \neq a \in \text{Ker } \varphi$ , т.е.  $aJ_i = 0$ . Все левые идеалы  $J_{i,j}$   $\mathbb{C}[G]$ -изоморфны, и если  $\varphi_j : J_i \rightarrow J_{i,j}$  — изоморфизм, то

$$aJ_{i,j} = a\varphi_j(J_i) = a\varphi_j(eJ_i) = \varphi_j(a \cdot eJ_i) = \varphi_j(0) = 0.$$

Значит,  $aA_i = aJ_{i,1} + \dots + aJ_{i,n_i} = 0$ , а в таком случае и  $a\mathbb{C}[G] = 0$ , поскольку  $a \in A_i \implies aA_j = 0$  для всех  $j \neq i$ . Однако  $ae = a \neq 0$ . Полученное противоречие показывает, что  $\text{Ker } \varphi = 0$ . Стало быть,  $\varphi$  — мономорфизм, а так как  $\dim A_i = n_i^2 = \dim M_{n_i}(\mathbb{C})$ , то  $A_i \xrightarrow{\varphi} M_{n_i}(\mathbb{C})$ . С учётом предложения 2 мы приходим к следующей теореме о строении групповой алгебры  $\mathbb{C}[G]$ .

**Теорема 4.** Групповая алгебра  $\mathbb{C}[G]$  конечной группы  $G$  над полем комплексных чисел  $\mathbb{C}$  разлагается в прямую сумму (2) простых двусторонних идеалов, изоморфных полным матричным алгебрам:

$$\mathbb{C}[G] \cong M_{n_1}(\mathbb{C}) \oplus M_{n_2}(\mathbb{C}) \oplus \dots \oplus M_{n_r}(\mathbb{C}).$$

В частности, групповая алгебра абелевой группы порядка  $n$  над  $\mathbb{C}$  изоморфна прямой сумме  $n$  экземпляров поля  $\mathbb{C}$ .

Следствие (теорема Бернсайда). Пусть  $\Phi$  — неприводимое матричное представление степени  $n$  над  $\mathbb{C}$  конечной группы  $G$ . Тогда среди матриц  $\Phi_g$  имеется  $n^2$  линейно независимых, т.е.  $\langle \Phi_g \mid g \in G \rangle_{\mathbb{C}} = M_n(\mathbb{C})$ .  $\square$

Строение центра  $Z(\mathbb{C}[G])$  как коммутативной подалгебры в  $\mathbb{C}[G]$  полностью определяется *структурными константами* — целыми числами  $n_{ij}^k$  из соотношений

$$K_i K_j = \sum_{s=1}^r n_{ij}^s K_s. \quad (4)$$

Имея в виду выражение (3) для  $K_i$ , легко понять, что  $n_{ij}^s$  — число пар  $(g, h)$ ,  $g \in \mathcal{K}_i$ ,  $h \in \mathcal{K}_j$ , для которых  $gh = g_s \in \mathcal{K}_s$ . Выберем в  $Z(\mathbb{C}[G])$  другой базис

$$I_i = \frac{n_i}{|G|} \sum_{s=1}^r \overline{\chi_i(g_s)} K_s = \frac{n_i}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g, \quad 1 \leq i \leq r. \quad (5)$$

Здесь, как и в § 5 из гл. 3,  $\chi_1, \dots, \chi_r$  — характеристы неприводимых представлений,  $n_1, \dots, n_r$  — их степени. Обратный переход совершается по формуле

$$K_s = |\mathcal{K}_s| \sum_{i=1}^r \frac{\chi_i(g_s)}{n_i} I_i.$$

Чтобы убедиться в этом, нужно воспользоваться соотношением (4) из § 5 гл. 3. Оно же показывает, что

$$\begin{aligned} \sum_{i=1}^r I_i &= \frac{1}{|G|} \sum_{g \in G} g \sum_i n_i \overline{\chi_i(g)} = \frac{1}{|G|} \sum_{g \in G} g \sum_i \chi_i(e) \overline{\chi_i(g)} = \\ &= \frac{1}{|G|} e |C_G(e)| = e. \end{aligned}$$

Далее, применяя обобщённое соотношение ортогональности из упр. 1 § 4 гл. 3, мы находим

$$\begin{aligned} I_i I_j &= \frac{n_i n_j}{|G|^2} \sum_{g, t \in G} \overline{\chi_i(g)} \overline{\chi_j(t)} g t = \frac{n_i n_j}{|G|} \sum_{h \in G} \left\{ \frac{1}{|G|} \sum_{g \in G} \overline{\chi_i(g)} \chi_j(hg) \right\} h^{-1} = \\ &= \frac{n_i n_j}{|G|} \frac{\delta_{ij}}{n_i} \sum_{h \in G} \chi_j(h) h^{-1} = \delta_{ij} I_j. \end{aligned}$$

Таким образом, центральные элементы  $I_i$ , вычисляемые по формуле (5), удовлетворяют соотношениям

$$\begin{aligned} e &= I_1 + I_2 + \dots + I_r, \\ I_i^2 &= I_i, \quad I_i I_j = 0, \quad i \neq j, \end{aligned} \quad (6)$$

и называются по этой причине *центральными ортогональными идеалами* групповой алгебры  $\mathbb{C}[G]$ . Соотношение  $e = I_1 + \dots + I_r$  — условие полноты этой системы. Положив  $B_i = I_i \mathbb{C}[G]$ , мы немедленно обнаруживаем, что  $B_i$  — двусторонний идеал в  $\mathbb{C}[G]$  с единичным

элементом  $I_i$  и что имеет место разложение в прямую сумму

$$\mathbb{C}[G] = B_1 \oplus B_2 \oplus \dots \oplus B_r. \quad (7)$$

Непосредственно из (5) следует, что

$$\chi_j(I_i) = n_i \frac{1}{|G|} \sum_g \overline{\chi_i(g)} \chi_j(g) = n_i \delta_{ij}.$$

Поэтому  $B_i$  содержит минимальный левый идеал  $J \subset A_i$ , отвечающий характеру  $\chi_i$ . Так как  $A_i$ , и  $B_i$  — двусторонние идеалы, то  $A_i \subset \subset B_i$ . Сравнивая разложения (2) и (7), мы заключаем, что  $A_i = B_i$ . Итак, доказан усовершенствованный вариант теоремы 3.

**Теорема 5.** Элементы  $I_i$ ,  $1 \leq i \leq r$ , вычисляемые по формуле (5), образуют полную систему центральных ортогональных идеалов потенций групповой алгебры  $\mathbb{C}[G]$  конечной группы  $G$ . Простая компонента  $I_i \mathbb{C}[G]$  прямого разложения

$$\mathbb{C}[G] = I_1 \mathbb{C}[G] \oplus I_2 \mathbb{C}[G] \oplus \dots \oplus I_r \mathbb{C}[G],$$

изоморфная полной матричной алгебре  $M_{n_i}(\mathbb{C})$ , содержит все минимальные левые идеалы, отвечающие характеру  $\chi_i$ .

Всю теорию представлений групп можно развить, исходя из теоремы Веддербарна–Артина (см. п. 1) и из общей структурной теории групповых алгебр (её заключительный вывод для конечных групп сформулирован в теореме 3). Мы шли в обратном направлении, опираясь по существу лишь на лемму Шура.

В заключение докажем два полезных утверждения о степенях и значениях характеров неприводимых представлений.

**Теорема 6.** Степень  $n$  неприводимого представления  $(\Phi, V)$  над  $\mathbb{C}$  конечной группы  $G$  делит порядок  $|G|$ .

**Доказательство.** Пусть  $\tilde{\Phi}$  — соответствующее представление групповой алгебры  $\mathbb{C}[G]$ . По лемме Шура (предложение 3 из § 3) линейный оператор  $\tilde{\Phi}(K_i)$ , перестановочный со всеми  $\Phi(g)$ ,  $g \in G$ , и потому принадлежащий  $\text{End}_{\mathbb{C}[G]}(V)$ , должен быть кратен единичному оператору:  $\tilde{\Phi}(K_i) = \omega_i \mathcal{E}$ . Имеем

$$n\omega_i = \text{tr } \omega_i \mathcal{E} = \text{tr } \tilde{\Phi}(K_i) = \sum_h \text{tr } \Phi(h g_i h^{-1}) = |\mathcal{K}_i| \chi_\Phi(g_i),$$

откуда

$$\omega_i = \frac{|\mathcal{K}_i| \chi_\Phi(g_i)}{n}.$$

Применяя  $\tilde{\Phi}$  к соотношениям (4), получим

$$\omega_i \omega_j = \sum_{k=1}^r n_{ij}^k \omega_k.$$

Стало быть,  $\mathbb{Z}[\omega_i]$  — подмодуль  $\mathbb{Z}$ -модуля  $\mathbb{Z}[\omega_1, \dots, \omega_r]$  конечного типа и согласно результатам п. 3 из § 3  $\omega_i$  — целое алгебраическое число. По тем же причинам

$$\begin{aligned}\frac{|G|}{n} &= \frac{|G|}{n}(\chi_\Phi | \chi_\Phi)_G = \frac{1}{n} \sum_g \chi_\Phi(g) \overline{\chi_\Phi(g)} = \\ &= \frac{1}{n} \sum_{i=1}^r |\mathcal{K}_i| \cdot \chi_\Phi(g_i) \overline{\chi_\Phi(g_i)} = \sum \omega_i \overline{\chi_\Phi(g_i)}\end{aligned}$$

— целое алгебраическое число. Значит,  $|G|/n \in \mathbb{Z}$ .  $\square$

**Лемма 2.** Пусть  $A$  — циклическая группа и  $\chi$  — её характер, возможно, приводимый. Положим  $S = \{a \in A \mid A = \langle a \rangle\}$ . Допустим, что  $\chi(s) \neq 0 \forall s \in S$ . Тогда

$$\sum_{s \in S} |\chi(s)|^2 \geq |S|.$$

**Доказательство.** Пусть  $n = |A|$  и  $F$  — поле разложения многочлена  $X^n - 1$  над  $\mathbb{Q}$ . В следующей главе изучается группа Галуа  $G = \text{Gal } F/\mathbb{Q}$  и действие  $G$  на характеристиках. Для наглядности будем изображать это действие экспоненциально. Если  $\sigma \in G$  и  $\zeta$  — корень степени  $n$  из 1, то  $\zeta^\sigma = \zeta^m$ ,  $\text{НОД}(m, n) = 1$ . Далее,  $\chi(s) = \zeta_1 + \dots + \zeta_k$ ,  $\zeta_i^n = 1$ , и по определению

$$\chi^\sigma(s) = \zeta_1^m + \dots + \zeta_k^m = \chi(s^m).$$

Группа  $G$  абелева и  $\alpha \mapsto \bar{\alpha}$ ,  $\alpha \in F$ , — тоже элемент из  $G$ , так что  $\alpha^\sigma = (\bar{\alpha})^\sigma$ ,  $\alpha \in F, \sigma \in G$ . Таким образом,

$$\begin{aligned}|\alpha^\sigma|^2 &= \alpha^\sigma \overline{\alpha^\sigma} = \alpha^\sigma (\bar{\alpha})^\sigma = (\alpha \bar{\alpha})^\sigma = (|\alpha|^2)^\sigma, \\ (|\chi(s)|^2)^\sigma &= |\chi(s^m)|^2, \quad \text{НОД}(m, n) = 1\end{aligned}$$

( $m$  зависит только от  $\sigma$ ).

Заметим, что  $s \in S \implies s^m \in S$ , если  $\text{НОД}(m, n) = 1$ . Кроме того,  $x \mapsto x^m$  — биекция на  $A$ , являющаяся перестановкой. Значит,  $\prod_{s \in S} |\chi(s)|^2$  — инвариант относительно  $G$ , а потому является рациональным числом. Вместе с тем это целое алгебраическое число. Таким образом, это число должно лежать в  $\mathbb{Z}$ . По условию  $\chi(s) \neq 0$ , поэтому  $\prod_{s \in S} |\chi(s)|^2 \geq 1$ . Но

$$\frac{1}{k} \sum_{i=1}^k r_i \geq (\prod_i r_i)^{1/k}$$

для любых положительных вещественных чисел  $r_1, \dots, r_k$ . В нашем случае

$$\frac{1}{|S|} \sum_{s \in S} |\chi(s)|^2 \geq 1. \quad \square$$

**Теорема 7** (У. Бернсайд). *Пусть  $G$  — конечная группа,  $\chi \in \text{Irr}(G)$ . Если  $\chi(e) > 1$ , то  $\chi(g) = 0$  хотя бы для одного  $g \in G$ .*

**Доказательство.** Расщепим  $G$  на классы, назвав два элемента из  $G$  эквивалентными, если они порождают одну и ту же циклическую подгруппу в  $G$ . Предположим, что  $\chi(g) \neq 0$  для любого  $g \in G$ . Тогда по лемме 2

$$\sum_{s \in S} |\chi(s)|^2 \geq |S|$$

для каждого класса эквивалентности  $S$ . Суммируя по всем классам эквивалентности неединичных элементов, получим неравенство

$$\sum_{g \neq e} |\chi(g)|^2 \geq |G| - 1.$$

Таким образом,

$$|G| = \sum_{g \in G} |\chi(g)|^2 \geq |G| - 1 + \chi(e)^2,$$

откуда  $\chi(e) \leq 1$  — противоречие.  $\square$

**Следствие.** *Если группа  $G$  совпадает со своим коммутантом  $G'$ , то*

$$|G| \cdot \prod_{i=1}^r K_i = \left( \prod_{i=1}^r |\mathcal{K}_i| \right) \sum_{l=1}^r K_l \quad (8)$$

(т.е. центральные элементы  $\prod_i K_i$  и  $\sum_i K_i$  из  $\mathbb{Q}[G]$  пропорциональны).

**Доказательство.** Пусть  $g_1, \dots, g_r$  — представители классов сопряжённости  $\mathcal{K}_1, \dots, \mathcal{K}_r$  и  $K_1, \dots, K_r$  — суммы элементов из  $\mathcal{K}_1, \dots, \mathcal{K}_r$ . Мы знаем (см. (4)), что

$$K_i K_j = \sum_{l=1}^r n_{ij}^l K_l,$$

$$\omega(K_i) \omega(K_j) = \sum_l n_{ij}^l \omega(K_l),$$

где  $\omega(K_i) = \chi(g_i)|\mathcal{K}_i|/\chi(e)$  — целое алгебраическое число. Умножая обе части соотношения

$$\frac{\chi(g_i)\chi(g_j)}{\chi(e)} |\mathcal{K}_i| |\mathcal{K}_j| = \sum_l n_{ij}^l \chi(g_l) |\mathcal{K}_l|$$

на  $\overline{\chi(g_s)}$  и суммируя по  $\chi$ , получаем формулу для структурных констант

$$n_{ij}^s = \frac{|\mathcal{K}_i| |\mathcal{K}_j|}{|G|} \sum_{\chi} \frac{\chi(g_i)\chi(g_j)\overline{\chi(g_s)}}{\chi(e)}. \quad (9)$$

По аналогии с (9), положив

$$\prod_{i=1}^r K_i = \sum_{l=1}^r N_l K_l,$$

будем иметь

$$\frac{\chi(g_1) \dots \chi(g_r) \prod_{i=1}^r |\mathcal{K}_i|}{\chi(e)^{r-1}} = \sum_{l=1}^r N_l \chi(g_l) |\mathcal{K}_l|,$$

так что

$$N_s = \frac{\prod_i |\mathcal{K}_i|}{|G|} \sum_{\chi} \frac{\chi(g_1) \dots \chi(g_r) \overline{\chi(g_s)}}{\chi(e)^{r-1}}. \quad (*)$$

Если теперь  $G = G'$ , то все характеристы, кроме  $1_G$ , имеют степень больше 1 (теорема 5 из § 5 гл. 3) и  $\chi(g_1)\chi(g_2) \dots \chi(g_r) = 0$  для  $\chi \neq 1_G$  по теореме 6. Непосредственно из формулы (\*) имеем  $N_s = \frac{\prod_i |\mathcal{K}_i|}{|G|} \cdot 1 \forall s$ , т.е. то, что нужно.  $\square$

**Замечание.** Пусть  $A$  — любая (т.е. не обязательно ассоциативная) алгебра произвольной размерности над полем  $P$ . Каждым трём элементам  $x, y, z \in A$  поставим в соответствие выражение  $(x, y, z) = (xy)z - x(yz)$ , называемое их *ассоциатором*. В зависимости от тождественных соотношений, связывающих ассоциаторы или иные выражения, получаются различные типы (как ещё говорят, *примитивные классы, многообразия*) алгебр. Примерами служат:

- 1) *ассоциативные алгебры*  $(x, y, z) = 0$ ;
- 2) *альтернативные алгебры*  $(x, x, y) = 0 = (y, x, x)$ ;
- 3) *йордановы алгебры*  $(x, y, x^2) = 0$ ,  $xy - yx = 0$ .

По этому аксиоматическому пути можно, очевидно, двигаться неограниченно. Замечательно, однако, что многие классы неассоциативных алгебр возникли естественным путём в областях, далёких от алгебры как науки. В качестве наиболее ярких примеров следует назвать йордановы алгебры, пришедшие в математику, как упоминалось в [ВА II], из квантовой механики (от физика Йордана), и алгебры Ли, предназначенные первоначально исключительно для описания (при определённых условиях) локальной структуры топологических групп (Софус Ли — один из крупнейших математиков XIX века). Об алгебрах Ли речь уже шла на страницах книги, и они будут фигурировать снова в следующем параграфе.

## УПРАЖНЕНИЯ

**1. Алгебра обобщённых кватернионов.** Показать, что таблицей умножения

.	1	$e_1$	$e_2$	$e_3$
1	1	$e_1$	$e_2$	$e_3$
$e_1$	$e_1$	$n$	$e_3$	$ne_2$
$e_2$	$e_2$	$-e_3$	$m$	$-me_1$
$e_3$	$e_3$	$-ne_2$	$me_1$	$-nm$

с  $n, m \in \mathbb{Z}$ ,  $nm \neq 0$ , на четырёхмерном векторном пространстве  $\mathbb{H}(n, m) = \langle 1, e_1, e_2, e_3 \rangle_{\mathbb{Q}}$  над  $\mathbb{Q}$  вводится структура ассоциативной алгебры с единицей. Использовать для этой цели представление

$$x = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3 \mapsto A_x = \begin{vmatrix} x_0 + x_1 \sqrt{n} & x_2 \sqrt{m} + x_3 \sqrt{nm} \\ x_2 \sqrt{m} - x_3 \sqrt{nm} & x_0 - x_1 \sqrt{n} \end{vmatrix}.$$

Определитель  $\det A_x = x_0^2 - x_1^2 n - x_2^2 m + x_3^2 nm$  называется *нормой элемента*  $x$ . Проверить, что при выполнении условия  $x \in \mathbb{H}(n, m)$ ,  $x \neq 0 \implies N(x) \neq 0$  пространство  $\mathbb{H}(n, m)$  является алгеброй с делением (*обобщённой алгеброй кватернионов*). Используя понятия и результаты упр. 7 из § 2, показать, что при простом  $p \equiv \pm 3 \pmod{8}$  алгебра  $\mathbb{H}(2, p)$  будет алгеброй с делением.

**2.** Пусть  $A$  — алгебра с единицей 1 над  $\mathbb{R}$ . Пусть на  $A$  задана операция сопряжения  $x \mapsto \bar{x}$ , обладающая свойствами  $\bar{\bar{x}} = x$ ,  $\bar{xy} = \bar{y}\bar{x}$ . Снабдим пространство  $A \oplus A = \{(x, y) \mid x, y \in A\}$  билинейной операцией умножения

$$(x, y)(u, v) = (xu - \bar{v}y, y\bar{u} + vx).$$

Получается алгебра, называемая *удвоением алгебры*  $A$ .

Проверить, что  $\mathbb{C}$  — удвоение алгебры  $\mathbb{R}$ , а  $\mathbb{H}$  — удвоение алгебры  $\mathbb{C}$ . Удвоение алгебры  $\mathbb{H}$  называется *алгеброй Кэли*  $\mathbb{Ca}$ .

Проверить, что  $\mathbb{Ca}$  — некоммутативная и неассоциативная алгебра. Выразить в явном виде операцию сопряжения на  $\mathbb{Ca}$ .

**3.** Рассмотреть  $\mathbb{F}_{2^n}$  как векторное пространство  $V$  размерности  $n$  над  $\mathbb{F}_2$ . Наряду с операцией сложения, наследуемой из  $\mathbb{F}_{2^n}$ , ввести на  $V$  операцию умножения  $(x, y) \mapsto x \circ y = \sqrt{xy}$ . Здесь  $x \mapsto \sqrt{x}$  — автоморфизм на  $\mathbb{F}_{2^n}$ , обратный к  $x \mapsto x^2$ , так что  $\sqrt{x+y} = \sqrt{x} + \sqrt{y}$ . Показать, что  $(V, +, \circ)$  — коммутативная (неассоциативная) алгебра над  $\mathbb{F}_2$ , обладающая свойствами: а) в  $V$  нет делителей нуля и нет единицы; б) уравнение  $a \circ x = b$  с  $a \neq 0$  однозначно разрешимо; в) группа автоморфизмов  $\text{Aut}(V)$  действует на  $V \setminus \{0\}$  транзитивно.

**4.** В любой алгебре выполняется тождество для ассоциаторов

$$t(x, y, z) + (t, x, y)z = (tx, y, z) - (t, xy, z) + (t, x, yz).$$

Убедиться в этом прямой проверкой и показать, что если в алгебре  $A$  с единицей 1 над полем  $P$  для всех ассоциаторов имеет место включение  $(x, y, z) \in P \cdot 1$ , то  $A$  — ассоциативная алгебра.

**5.** Пусть  $G$  и  $H$  — конечные группы и  $\mathbb{C}[G] \cong \mathbb{C}[H]$  — изоморфизм  $\mathbb{C}$ -алгебр. Можно ли утверждать, что  $G \cong H$ ?

**6.** Пусть  $\Phi$  — комплексное матричное неприводимое представление степени  $n$  конечной группы  $G$ . Доказать, что если

$$\text{tr}\{C\Phi_x\} = 0 \quad \forall x \in G,$$

где  $C$  — постоянная  $(n \times n)$ -матрица, то  $C = 0$ .

## § 5. Неприводимые модули над алгеброй Ли $\mathfrak{sl}(2)$

**1. Исходный материал.** Напомним, что в алгебре Ли  $L$  над полем  $P$  произведение элементов  $x, y \in L$  принято обозначать  $[x, y]$  или ещё проще  $[xy]$ . По определению алгебры Ли билинейная операция  $(x, y) \mapsto [xy]$  удовлетворяет двум требованиям:

- i)  $[xx] = 0$  ( $[xy] = -[yx]$  — антикоммутативность);
- ii)  $[[xy]z] + [[yz]x] + [[zx]y] = 0$  (тождество Якоби).

Мы знаем также из [ВА II], что если  $A$  — ассоциативная алгебра над полем  $P$ , то на векторном пространстве  $A$  можно задать структуру алгебры Ли  $L(A)$ , полагая  $[xy] = xy - yx$  (коммутатор двух элементов).

Пусть, в частности,  $A = \text{End}_P(V) = \mathcal{L}(V)$  — алгебра всех линейных операторов конечномерного векторного пространства  $V$  над  $P$ . Любой гомоморфизм

$$\varphi: L \longrightarrow L(\mathcal{L}(V))$$

называется *представлением алгебры Ли*  $L$ . В соответствии с терминологией предыдущих параграфов пространство представления  $V$  называется также  *$L$ -модулем* (или *модулем над алгеброй Ли*  $L$ ). Формально  $L$ -модуль задаётся тремя аксиомами:

- L1)  $x(\alpha u + \beta v) = \alpha xu + \beta xv$ ;
- L2)  $(\alpha x + \beta y)v = \alpha xv + \beta yv$ ;
- L3)  $[xy]v = x(yv) - y(xv)$ .

На самом деле каждый  $L$ -модуль является модулем над универсальной обёртывающей алгеброй  $U(L)$  — ассоциативной алгеброй, порожденной  $L$  (теорему Биркгофа–Витта на этот счёт мы не формулируем).

Пример 1. *Дифференцированием* произвольной алгебры  $A$  (не обязательно ассоциативной) над полем  $P$  называется дифференцирование  $\mathcal{D}$  кольца  $(A, \cdot)$ :

$$\mathcal{D}(u + v) = \mathcal{D}(u) + \mathcal{D}(v), \quad \mathcal{D}(u \cdot v) = \mathcal{D}(u) \cdot v + u \cdot \mathcal{D}(v), \quad u, v \in A,$$

перестановочное с действием констант из  $P$ :  $\mathcal{D}(\lambda a) = \lambda \mathcal{D}(a)$ ,  $\lambda \in P$ ,  $a \in A$ . Умножение

$$[\mathcal{D}_1 \mathcal{D}_2] = \mathcal{D}_1 \mathcal{D}_2 - \mathcal{D}_2 \mathcal{D}_1$$

наделяет множество всех дифференцирований  $\text{Der}(A)$ , являющееся векторным пространством над  $P$ , структурой алгебры Ли.

Если, в частности,  $A = P[X]$  — алгебра многочленов, то  $\text{Der}(A)$  состоит из дифференцирований  $\mathcal{D}_u$ ,  $u \in A$ , действующих по правилу

$$\mathcal{D}_u(f) = u \frac{df}{dX} = uf'.$$

По определению

$$\begin{aligned} [\mathcal{D}_u \mathcal{D}_v](f) &= \mathcal{D}_u(\mathcal{D}_v f) - \mathcal{D}_v(\mathcal{D}_u f) = \mathcal{D}_u(vf') - \mathcal{D}_v(uf') = \\ &= u(vf')' - v(uf')' = u(v'f' + vf'') - v(u'f' + uf'') = (uv' - u'v)f'. \end{aligned}$$

Следовательно,

$$[\mathcal{D}_u \mathcal{D}_v] = \mathcal{D}_{uv' - u'v},$$

и мы видим, что алгебра  $\text{Der}(A)$  изоморфна бесконечномерной алгебре Ли  $(A, [\cdot, \cdot])$  с базисным пространством  $A$  и умножением  $[uv] = uv' - u'v$ . Положив  $A_{(i)} = \langle X^{i+1} \rangle_P$ , мы получим разложение  $A$  в прямую сумму

$$A = A_{(-1)} \oplus A_{(0)} \oplus A_{(1)} \oplus A_{(2)} \oplus \dots,$$

обладающее свойством *градуированной алгебры Ли*

$$[A_{(i)}, A_{(j)}] \subset A_{(i+j)}$$

(ср. с примером 2 из п. 1 § 4). Алгебра Ли  $(K, [\cdot, \cdot])$  действует на векторном пространстве  $K$  двумя способами: 1)  $(a, f) \mapsto af'$  (*естественное действие*); 2)  $(a, f) \mapsto af' - a'f$  (*действие присоединёнными эндоморфизмами*). В результате получаются два неизоморфных  $(A, [\cdot, \cdot])$ -модуля.

Пример 2. Трёхмерное вещественное пространство

$$\mathfrak{su}(2) = \langle \mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3 \rangle_{\mathbb{R}}$$

косоэрмитовых матриц с нулевым следом наделено структурой алгебры Ли. Соотношения

$$[\mathbf{k}_1 \mathbf{k}_2] = \mathbf{k}_3, \quad [\mathbf{k}_2 \mathbf{k}_3] = \mathbf{k}_1, \quad [\mathbf{k}_3 \mathbf{k}_1] = \mathbf{k}_2$$

в точности повторяют правила векторного произведения векторов в  $\mathbb{R}^3$ .

Из общей теории представлений компактных групп следует, что между неприводимыми представлениями группы  $SU(2)$  и её алгебры Ли  $\mathfrak{su}(2)$  имеется взаимно однозначное соответствие. Интуитивно это можно понять, приняв во внимание непрерывность представления группы и рассмотрев в линейной оболочке операторов  $\Phi(g_t)$  (где  $g_t$  — зависящий дифференцируемым образом от  $t \in \mathbb{R}$  элемент группы  $SU(2)$ ;  $g_0 = e$ ) линейный оператор  $d\Phi(g_t)/dt|_{t=0}$ , уже содержащийся в алгебре  $\mathfrak{su}(2)$ . Чтобы подтвердить полноту списка неприводимых представлений группы  $SU(2)$ , которые были получены в § 6 гл. 3, нам нужно убедиться в том, что для любого натурального  $n$  имеется с точностью до изоморфизма ровно один неприводимый  $\mathfrak{su}(2)$ -модуль размерности  $n$  над  $\mathbb{C}$ . С этой целью удобно перейти с самого начала от вещественной алгебры Ли  $\mathfrak{su}(2)$  к её “комплексификации”, совпадающей с алгеброй Ли  $L = \mathfrak{sl}(2) = \mathfrak{su}(2) \otimes_{\mathbb{R}} \mathbb{C}$  всех комплексных  $2 \otimes 2$ -матриц с нулевым следом. Базисные элементы

$$e_{-1} = \mathbf{k}_1 - i\mathbf{k}_2, \quad e_0 = 2i\mathbf{k}_3, \quad e_1 = \mathbf{k}_1 + i\mathbf{k}_2$$

алгебры  $L$  перемножаются по правилам

$$[e_{-1} e_1] = e_0, \quad [e_0 e_{-1}] = -2e_{-1}, \quad [e_0 e_1] = 2e_1. \quad (1)$$

Забыв на время о происхождении  $L$ , можно считать, что  $L = \langle e_{-1}, e_0, e_1 \rangle$  — абстрактная трёхмерная алгебра Ли над  $\mathbb{C}$  с таблицей умножения (1). Легко проверить, что  $L$  — простая алгебра Ли. Стало быть, любой её неприводимый модуль размерности  $> 1$  будет точным.

**2. Веса и кратности.** Пусть вначале  $V \neq 0$  — произвольный  $L$ -модуль конечной размерности над  $\mathbb{C}$ , и пусть  $E_{-1}, E_0, E_1$  — линейные операторы (или матрицы при фиксированном базисе) на  $V$ , отвечающие соответственно элементам  $e_{-1}, e_0, e_1$ . В теории представлений алгебр Ли установилась своя терминология, которой мы будем придерживаться.

Определение. Собственное подпространство

$$V^\lambda = \{v \in V \mid E_0 v = \lambda v\}$$

оператора  $E_0$  в  $V$  с собственным значением  $\lambda \in \mathbb{C}$  состоит из векторов, о которых принято говорить, что они имеют *вес*  $\lambda$ . Размерность  $\dim V^\lambda$  называется *кратностью веса*  $\lambda$ .

Лемма 1. Если  $v \in V^\lambda$ , то

$$E_1 v \in V^{\lambda+2}, \quad E_{-1} v \in V^{\lambda-2}$$

( $E_1$  — “повышающий” оператор, а  $E_{-1}$  — “понижающий”).

Доказательство. В соответствии с аксиомой L3) имеем

$$E_0(E_1 v) = [E_0 E_1] v + E_1(E_0 v) = 2E_1 v + E_1(\lambda v) = (\lambda + 2)E_1 v,$$

так что по определению  $E_1 v \in V^{\lambda+2}$ . Аналогично,

$$E_0(E_{-1} v) = (\lambda - 2)E_{-1} v. \quad \square$$

**3. Старший вектор.** Из [ВА II] известно, что векторы, отвечающие различным собственным значениям, линейно независимы. Поэтому сумма

$$W = \sum_{\lambda} V^\lambda \subset V$$

прямая. Из леммы 1 следует также, что  $W$  является  $L$ -подмодулем в  $V$ . Так как  $W \neq 0$ , то в случае неприводимого  $L$ -модуля  $V$  должно выполняться равенство  $W = V$ .

Определение. Вектор  $v_0 \in V$  назовём *старшим вектором веса*  $\lambda$ , если  $v_0 \neq 0$  и

$$E_1 v_0 = 0, \quad E_0 v_0 = \lambda v_0.$$

Лемма 2. Любой конечномерный  $L$ -модуль  $V$  обладает старшим вектором.

Доказательство. Возьмём произвольный ( $\neq 0$ ) вектор  $v$  веса  $\mu$  и построим последовательность векторов  $v, E_1 v, E_1^2 v, \dots$  с весами  $\mu, \mu + 2, \mu + 4, \dots$  (см. лемму 1). Так как  $\dim V < \infty$ , то  $E_1^{m+1} v = 0$  для некоторого  $m$ . Взяв  $m$  минимальным, мы можем положить  $v_0 = E_1^m v, \quad \lambda = \mu + 2m$ .  $\square$

Лемма 3. Пусть  $V_n$  — векторное пространство размерности  $n + 1$  над  $\mathbb{C}$  с фиксированным базисом  $(v_0, v_1, \dots, v_n)$ ,  $E_1, E_0, E_1$  —

операторы, определённые формулами

$$\begin{aligned} E_{-1}v_m &= (m+1)v_{m+1}, \\ E_0v_m &= (n-2m)v_m, \\ E_1v_m &= (n-m+1)v_{m-1}, \end{aligned} \tag{2}$$

где  $v_{-1} = 0 = v_{n+1}$ . Тогда  $V_n$  — неприводимый  $L$ -модуль.

**Доказательство.** Прямая проверка показывает, что выполнены соотношения

$$\begin{aligned} E_1(E_{-1}v_m) - E_{-1}(E_1v_m) &= E_0v_m, \\ E_0(E_{-1}v_m) - E_{-1}(E_0v_m) &= -2E_{-1}v_m, \\ E_0(E_1v_m) - E_1(E_0v_m) &= 2E_1v_m, \end{aligned}$$

согласующиеся с таблицей умножения (1) и с аксиомами  $L$ -модуля. Так как  $E_1v_0 = (n+1)v_{-1} = 0$ ,  $E_0v_0 = nv_0$ , то  $v_0$  — старший вектор веса  $n$ , а всё пространство  $V_n$  записывается в виде прямой суммы

$$V_n = V^n \oplus V^{n-2} \oplus \dots \oplus V^{-n} \tag{3}$$

одномерных весовых подпространств  $V^{n-2m} = \langle v_m \rangle$  (каждый вес имеет кратность 1).

Предположив существование подмодуля  $U \neq 0$  в  $V_n$ , мы возьмём любой собственный вектор  $u \in U$  оператора  $E_0$ . Согласно разложению (3)  $u = \lambda v_m$  для некоторого  $m$ . Последовательное применение повышающего оператора  $E_1$  (см. формулы (2)) даст нам включения  $v_{m-1} \in U, \dots, v_0 \in U$ , а посредством понижающего оператора  $E_{-1}$  мы получим из старшего вектора  $v_0$  все остальные векторы. Значит,  $U = V_n$ , и  $V_n$  — неприводимый  $L$ -модуль.  $\square$

Заметим, что  $V_0$  — тривиальный (одномерный) модуль, а  $V_1$  — модуль, соответствующий естественному определению алгебры  $L$ : в базисе  $(v_0, v_1)$  операторы  $E_{-1}, E_0, E_1$  имеют своими матрицами

$$\left\| \begin{array}{cc} 0 & 0 \\ 1 & 0 \end{array} \right\|, \quad \left\| \begin{array}{cc} 1 & 0 \\ 0 & -1 \end{array} \right\|, \quad \left\| \begin{array}{cc} 0 & 1 \\ 0 & 0 \end{array} \right\|.$$

**4. Классификационный результат.** Следующая теорема решает стоящую перед нами задачу.

**Теорема 1.** Всякий неприводимый  $L$ -модуль  $V$  размерности  $n+1$  над  $\mathbb{C}$  изоморден  $V_n$ .

**Доказательство.** По лемме 2 наш модуль  $V$  обладает некоторым старшим вектором  $v_0$  веса  $\lambda$ . Положим

$$v_{-1} = 0, \quad v_m = \frac{1}{m!} E_{-1}^m v_0 = \frac{1}{m!} E_{-1}(\dots(E_{-1}v_0)\dots) \text{ при } m \geq 0.$$

Утверждается, что при любом  $m \geq 0$  справедливы формулы

$$\begin{aligned} E_{-1}v_m &= (m+1)v_{m+1}, \\ E_0v_m &= (\lambda - 2m)v_m, \\ E_1v_m &= (\lambda - m + 1)v_{m-1}. \end{aligned} \tag{2'}$$

Действительно, при  $m = 0$  формулы (2') сводятся к определению старшего вектора  $v_0$  и вектора  $v_1$ , а дальше действуем индукцией по  $m$ .

- а) Формулой  $E_{-1}v_m = (m+1)v_{m+1}$  определяется вектор  $v_{m+1}$ .
- б) Формула  $E_0v_m = (\lambda - 2m)v_m$  следует из леммы 1.
- в) Если уже известно, что  $E_1v_{m-1} = (\lambda - m + 2)v_{m-2}$ , то после сокращения на  $m$  обеих частей равенства

$$\begin{aligned} mE_1v_m &= E_1(E_{-1}v_{m-1}) = [E_1E_{-1}]v_{m-1} + E_{-1}(E_1v_{m-1}) = \\ &= E_0v_{m-1} + (\lambda - m + 2)E_{-1}v_{m-2} = \\ &= \{(\lambda - 2m + 2) + (\lambda - m + 2)(m-1)\}v_{m-1} = m(\lambda - m + 1)v_{m-1} \end{aligned}$$

получается последняя из формул (2').

Если векторы  $v_0, v_1, \dots, v_r$  при каком-то  $r$  отличны от нуля, то, имея различные веса, они должны быть линейно независимыми. С другой стороны, в силу неприводимости  $V$  подмодуль, порождённый вектором  $v_0$ , совпадает с  $V$ , а так как  $\dim V = n+1$ , то  $V = \langle v_0, v_1, \dots, v_n \rangle$  и  $v_{n+1} = v_{n+2} = \dots = 0$ . В частности,

$$0 = E_1v_{n+1} = (\lambda - n)v_n = 0 \implies \lambda = n$$

(обратим внимание на любопытную импликацию  $\dim V < \infty \implies \lambda \in \mathbb{Z}, \lambda \geq 0$ ).

Подставив значение  $\lambda = n$  в формулы (2'), мы придём фактически, с учётом выбранных обозначений, к формулам (2), которыми определялся неприводимый (по лемме 3)  $L$ -модуль  $V_n$ . Значит,  $V \cong V_n$ .  $\square$

### УПРАЖНЕНИЯ

**1.** Задать на  $V_n$  структуру  $\mathfrak{su}(2)$ -модуля, используя формулы (2), возвращаясь к базисным элементам

$$\mathbf{k}_1 = \frac{1}{2}(e_{-1} + e_2), \quad \mathbf{k}_2 = \frac{i}{2}(e_{-1} - e_1), \quad \mathbf{k}_3 = -\frac{i}{2}e_0$$

и ставя им в соответствие линейные операторы  $K_1, K_2, K_3$ .

**2.** Пусть  $L = \langle e_{-1}, e_0, e_1 \rangle$  — простая алгебра Ли с таблицей умножения (1) над алгебраически замкнутым полем  $F$  характеристики  $p > 2$ . Рассмотрим квад-

ратные матрицы порядка  $p$

$$E_{-1} = \begin{vmatrix} 0 & \gamma_1 & 0 & \dots & 0 & 0 \\ 0 & 0 & \gamma_2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & \gamma_{p-2} & 0 \\ 0 & 0 & 0 & \dots & 0 & \gamma_{p-1} \\ \gamma_0 & 0 & 0 & \dots & 0 & 0 \end{vmatrix}, \quad E_1 = \begin{vmatrix} 0 & 0 & \dots & 0 & 0 & \beta \\ 1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & 0 \\ 0 & 0 & \dots & 0 & 1 & 0 \end{vmatrix},$$

$$E_0 = [E_{-1}, E_1] = \text{diag}(\lambda, \lambda + 2, \dots, \lambda + 2(p - 2), \lambda + 2(p - 1)).$$

Проверить, что соответствие  $e_i \mapsto E_i$ ,  $i = -1, 0, 1$ , устанавливает неприводимое матричное представление алгебры Ли  $L$ , зависящее от трёх параметров  $(\lambda, \beta, \gamma_0)$ . При этом

$$\gamma_k = \beta\gamma_0 + k\lambda + k(k - 1), \quad k = 1, 2, \dots, p - 1.$$

(Эта совершенно новая ситуация типична для представлений над полем конечной характеристики.)

# НАЧАЛА ТЕОРИИ ГАЛУА

---

Помимо элементарных сведений о конечных расширениях полей, в частности, о конечных полях и полях алгебраических чисел, приводятся фрагменты теории Галуа, достаточные для того, чтобы доказать классическую теорему о неразрешимости в радикалах алгебраических уравнений степени больше 4. Доказываются также более интересные теоретико-числовые факты. Излагаются начала современного направления в теории Галуа, привлекательность которого для нас обусловлена активным использованием теории характеров на элементарном уровне главы 3.

## § 1. Конечные расширения полей

**1. Примитивные элементы и степени расширений.** Если  $F$  — поле, содержащее подполе  $P$ , то  $F$  называется также расширением поля  $P$  [ВА I, гл. 4, § 3]. Мы ограничимся вначале простейшим случаем, когда расширение  $F = P(\theta)$  получено из поля  $P$  присоединением (внутри заданного поля  $F$ ) единственного элемента  $\theta \in F$ . Говорят, что  $P(\theta)$  — *простое расширение поля  $P$* , а  $\theta$  — *примитивный элемент* этого расширения. По своему смыслу  $P(\theta)$  — поле отношений целостного кольца  $P[\theta]$ . Элемент  $\theta$  *трансцендентен* над  $P$  тогда и только тогда, когда расширение  $P(\theta)$  изоморфно полю рациональных дробей. Если, однако,  $\theta$  — алгебраический элемент, то  $P(\theta) \cong P[X]/(f(X))$  (гл. 4, § 1, теорема 2). Здесь  $f(X)$  — неприводимый многочлен степени  $n > 0$ , корнем которого является  $\theta$ . Обратно: если  $f[X]$  — неприводимый многочлен, то, как мы знаем из гл. 4, каноническим образом строится поле  $F$ , в котором  $f$  обладает хотя бы одним корнем (назовём его  $\theta$ ). Из построения видно, что  $F$  отождествляется с множеством элементов вида

$$a_0 + a_1\theta + \dots + a_{n-1}\theta^{n-1}, \quad a_i \in P, \quad n = \deg f.$$

Для элементов кольца  $P[\theta]$  это очевидно (разделить  $g(X)$  на  $f(X)$  с остатком и подставить  $X = \theta$ ); деление же в  $P[\theta]$  осуществляется так: если  $g(X) = a_0 + a_1X + \dots + a_{n-1}X^{n-1}$ , то неприводимость  $f$  влечёт равенство  $\text{НОД}(f, g)=1$  и существование многочленов  $u(X), v(X)$  степени  $< n$ , для которых  $fu+gv=1$ ; отсюда  $g(\theta)v(\theta)=1$  и  $1/g(\theta)=v(\theta)$ . Число  $n$  можно считать размерностью векторного пространства над  $P$  с базисными элементами  $1, \theta, \dots, \theta^{n-1}$ .

В случае произвольного расширения  $F \supset P$  также целесообразно рассмотреть  $F$  как векторное пространство над  $P$ . Его размерность  $\dim_P F$  (возможно, бесконечную) мы обозначим через  $[F : P]$  и назовём *степенью расширения  $F$  над  $P$* . Если  $F = P(\theta)$ , то  $[F : P]$

называется также *степенью примитивного элемента*. Понятно, что для трансцендентного элемента  $\theta \in F$  семейство  $1, \theta, \theta^2, \dots$  линейно независимо над  $P$  и  $[P(\theta) : P] = \infty$ . С другой стороны, из сказанного выше вытекает следующее утверждение.

**Теорема 1.** *Пусть  $F$  — какое-то расширение поля  $P$ . Элемент  $\theta \in F$  алгебраичен над  $P$  тогда и только тогда, когда  $[P(\theta) : P] < \infty$ . Кроме того, алгебраичность  $\theta$  влечёт равенство  $P(\theta) = P[\theta]$ .*

Назовём  $K \supset F \supset P$  двухэтажной башней расширений. Она позволяет говорить о трёх векторных пространствах:  $K/P$  ( $K$  над  $P$ ),  $K/F$  ( $K$  над  $F$ ) и  $F/P$  ( $F$  над  $P$ ). Их размерности связаны соотношением, аналогичным соотношению для индексов подгрупп.

**Теорема 2.** *В башне расширений  $K \supset F \supset P$  степень  $[K : P]$  конечна тогда и только тогда, когда конечны степени  $[K : F]$  и  $[F : P]$ . В случае их конечности справедливо соотношение*

$$[K : P] = [K : F][F : P].$$

**Доказательство.** Предположив сначала конечность  $[K : F]$  и  $[F : P]$ , выберем  $P$ -базис  $f_1, \dots, f_m$  в  $F/P$  и  $F$ -базис  $e_1, \dots, e_n$  в  $K/F$ . Тогда любой элемент  $x \in K$  записывается в виде  $x = \sum_j \alpha_j e_j$  с  $\alpha_j \in F$ . В свою очередь  $\alpha_j = \sum_i p_{ij} f_i$  с  $p_{ij} \in P$ . Следовательно,  $x = \sum_{i,j} p_{ij} f_i e_j$ , и мы видим, что  $m n$  элементов  $f_i e_j$  линейно порождают  $K$  над  $P$ . Предположим наличие линейной зависимости  $\sum_{i,j} p_{ij} f_i e_j = 0$  при некоторых  $p_{ij} \in P$ . Тогда

$$0 = \sum_{i,j} p_{ij} f_i e_j = \sum_j \left( \sum_i p_{ij} f_i \right) e_j \implies \sum_i p_{ij} f_i = 0 \implies p_{ij} = 0$$

для всех  $i = 1, \dots, m$ ;  $j = 1, \dots, n$ , поскольку  $e_1, \dots, e_n$  линейно независимы над  $F$ , а  $f_1, \dots, f_m$  линейно независимы над  $P$ . Стало быть,  $m n$  элементов  $f_i e_j$  составляют базис векторного пространства  $K/P$  и  $[K : P] = m n = [K : F][F : P]$ .

Обратно неравенство  $[K : P] < \infty$  влечёт конечность  $[F : P]$ , поскольку  $F/P$  — подпространство пространства  $K/P$ . Если  $(a_1, \dots, a_r)$  —  $P$ -базис для  $K$ , то произвольный элемент  $x \in K$  будет линейной комбинацией  $a_1, \dots, a_r$  с коэффициентами в  $P$  и тем более — с коэффициентами в  $F$ . Над  $F$  число линейно независимых элементов среди  $a_1, \dots, a_r$  может лишь уменьшиться. Таким образом,  $[K : F] < \infty$ .  $\square$

**Следствие.** *Пусть  $F$  — расширение поля  $P$ ,  $A$  — множество всех тех элементов из  $F$ , которые алгебраичны над  $P$ . Тогда  $A$  — подполе в  $F$ , содержащее  $P$ .*

**Доказательство.** Каждый элемент  $t \in P$  является корнем линейного многочлена  $X - t \in P[X]$ , так что  $P \subset A$ . Пусть, далее,

$u, v \in A$ . Тогда по теореме 1 имеем  $[P(u) : P] < \infty$ . Элемент  $v$ , алгебраический над  $P$ , будет алгебраическим и над  $P(u)$ , т.е.

$$[P(u, v) : P(u)] = [P(u)(v) : P(u)] < \infty.$$

Согласно теореме 2

$$[P(u, v) : P] = [P(u, v) : P(u)][P(u) : P] < \infty.$$

Так как  $u - v, uv \in P(u, v)$ , то снова по теореме 1 имеем  $u - v, uv \in A$ , т.е.  $A$  — подкольцо в  $F$ . Оно является полем, поскольку

$$0 \neq u \in A \implies [P(u^{-1}) : P] = [P(u) : P] < \infty. \quad \square$$

Расширение  $F \supset P$  называется *алгебраическим над  $P$* , если все элементы из  $F$  алгебраичны над  $P$ . Каждый элемент  $\alpha$  алгебраического расширения является корнем некоторого отличного от нуля нормализованного (т. е. со старшим коэффициентом 1) многочлена  $f \in P[X]$ , зависящего от  $\alpha$ . Если  $f(\alpha) = 0$  и  $g(\alpha) \neq 0$  для любого  $0 \neq g \in P[X]$  с  $\deg g < \deg f$ , то  $f = f_\alpha$  называется *минимальным многочленом элемента  $\alpha$* . Минимальный многочлен неприводим над  $P$ , однозначно определён и его степень совпадает со степенью элемента  $\alpha$  (часто многочлен, получающийся из минимального умножением на константу, также называется минимальным). Все различные корни многочлена  $f_\alpha$  считаются *сопряжёнными с  $\alpha$* . Объяснение этой терминологии даёт ниже теорема 3. Если  $\text{char } P = 0$ , то число различных корней совпадает с  $\deg f_\alpha$  (см. [ВА I, гл. 6]), но в общем случае это не так (см. упр. 4 и 5).

Согласно полученным результатам расширение  $F \supset P$  конечной степени  $[F : P]$  является *конечным алгебраическим*, т. е. оно получается из  $P$  присоединением конечного числа алгебраических элементов  $\alpha_1, \dots, \alpha_m$ . Обратно: *всякое конечное алгебраическое расширение  $F = P(\alpha_1, \dots, \alpha_m)$  имеет конечную степень*. В самом деле,  $f_k(\alpha_k) = 0$ ,  $1 \leq k \leq m$ ,  $f_k \in P[X]$ . Элемент  $\alpha_k$ , алгебраический над  $P$ , будет, естественно, алгебраическим и над  $P(\alpha_1, \dots, \alpha_{k-1})$ . Значит,  $[P(\alpha_1, \dots, \alpha_k) : P(\alpha_1, \dots, \alpha_{k-1})] < \infty$  и в соответствии с теоремой 2

$$\begin{aligned} [F : P] &= [P(\alpha_1, \dots, \alpha_m) : P] = \\ &= \prod_{k=1}^m [P(\alpha_1, \dots, \alpha_k) : P(\alpha_1, \dots, \alpha_{k-1})] < \infty. \quad \square \end{aligned}$$

Пример. Поле  $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$  как векторное пространство над  $\mathbb{Q}$  четырёхмерно:  $F = \langle 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \rangle_{\mathbb{Q}}$ , т. е. каждый элемент  $\alpha \in F$  записывается в виде линейной комбинации  $\alpha = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$  с рациональными координатами  $a, b, c, d$ . С другой стороны,

$$F = \langle 1, \theta, \theta^2, \theta^3 \rangle_{\mathbb{Q}}, \quad \text{где } \theta = \sqrt{2} + \sqrt{3}.$$

Действительно,

$$\sqrt{2} = -\frac{9}{2}\theta + \frac{1}{2}\theta^3, \quad \sqrt{3} = \frac{11}{2}\theta - \frac{1}{2}\theta^3, \quad \sqrt{6} = -\frac{5}{2} + \frac{1}{2}\theta^2.$$

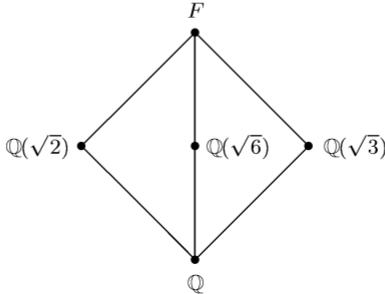
Примитивный элемент  $\theta$  имеет минимальный многочлен  $f_\theta(X) = X^4 - 10X^2 + 1$  с корнями

$$\begin{aligned} \theta^{(1)} &= \theta = \sqrt{2} + \sqrt{3}, & \theta^{(2)} &= \sqrt{2} - \sqrt{3}, \\ \theta^{(3)} &= -\sqrt{2} + \sqrt{3}, & \theta^{(4)} &= -\sqrt{2} - \sqrt{3}. \end{aligned}$$

Обратим внимание на тот факт, что  $F$  является полем разложения многочлена  $f_\theta(X)$ , причём

$$F = \mathbb{Q}(\theta^{(1)}, \theta^{(2)}, \theta^{(3)}, \theta^{(4)}) = \mathbb{Q}(\theta^{(i)}), \quad i = 1, 2, 3, 4.$$

В общей теории Галуа такое поле было бы названо *нормальным*. Диаграмма подполей поля  $F$



похожа на диаграмму подгрупп четверной группы  $V_4$ , и это не случайно. Если мы рассмотрим произвольный автоморфизм  $\Phi : F \rightarrow F$ , то из соотношений

$$\Phi(x+y) = \Phi(x) + \Phi(y), \quad \Phi(xy) = \Phi(x)\Phi(y) \quad \forall x, y \in F,$$

следует, что  $\Phi$  полностью определяется своим действием на примитивный элемент  $\theta$ . Далее,  $\Phi(a) = a \quad \forall a \in \mathbb{Q}$ , поэтому

$$\Phi(\theta)^4 - 10\Phi(\theta)^2 + 1 = \Phi(\theta^4 - 10\theta^2 + 1) = \Phi(0) = 0.$$

Значит,  $\Phi(\theta)$  — один из корней  $\theta^{(i)}$ ,  $i = 1, 2, 3, 4$ , и мы приходим к заключению, что группа всех автоморфизмов  $\text{Aut}(F/\mathbb{Q})$ , называемая также *группой Галуа*  $G(F/\mathbb{Q})$  или  $G(f_\theta)$ , имеет порядок  $4 = [F : \mathbb{Q}]$ . Группы порядка 4 с точностью до изоморфизма всего две: циклическая  $Z_4$  и  $Z_2 \times Z_2 \cong V_4$ . Непосредственные вычисления показывают, что  $\text{Aut}(F/\mathbb{Q}) \cong V_4$ .

Легче всего в этом убедиться, рассмотрев представление  $\text{Aut}(F/\mathbb{Q})$  перестановками на множестве  $\Omega = \{1, 2, 3, 4\}$ , элементами которого нумеруются корни  $\theta^{(i)}$ . Если, например,  $\Phi(\theta^{(1)}) = \theta^{(2)}$ , то

$$\begin{aligned} \theta^{(1)}\theta^{(2)} &= -1 \implies \theta^{(2)}\Phi(\theta^{(2)}) = -1 \implies \\ &\implies \Phi(\theta^{(2)}) = \theta^{(1)}, \quad \Phi(\theta^{(3)}) = -\Phi(\theta^{(2)}) = -\theta^{(1)} = \theta^{(4)} \end{aligned}$$

т.е.  $\Phi \approx (12)(34) = \sigma$ . Аналогично получаются автоморфизмы  $(13)(24) = \tau$  и  $(14)(23) = \sigma\tau$ .

Остается добавить к сказанному, что циклическая подгруппа  $\langle \sigma \rangle$  оставляет поэлементно неподвижным промежуточное подполе  $\mathbb{Q}(\sqrt{2})$  и  $\langle \sigma \rangle$  является группой  $G = F/(\mathbb{Q}(\sqrt{2}))$  всех автоморфизмов (группой Галуа) поля  $F$  относительно

подполя  $\mathbb{Q}(\sqrt{2})$ . Аналогично, полями инвариантов для  $\langle\tau\rangle$  и  $\langle\sigma\tau\rangle$  служат соответственно  $\mathbb{Q}(\sqrt{3})$  и  $\mathbb{Q}(\sqrt{6})$ , а группами Галуа  $G = F/(\mathbb{Q}(\sqrt{3}))$ ,  $G = F/(\mathbb{Q}(\sqrt{6}))$  будут в свою очередь  $\langle\tau\rangle$  и  $\langle\sigma\tau\rangle$ . Мы проверили на частном примере справедливость биективного соответствия Галуа между подполями нормального поля  $F$  и подгруппами его группы автоморфизмов.

**2. Изоморфизм полей разложения.** В § 1 гл. 4, где определено и построено поле разложения  $F$  над  $P$  нормализованного многочлена, отмечалось, что в построении имеются элементы произвола. Повторяя сейчас эту конструкцию, мы могли бы лишь сказать, что  $[F : P] \leq n!$  (постарайтесь понять, почему). Но на самом деле все поля разложения над  $P$  данного многочлена  $f$  изоморфны. Чтобы уточнить это высказывание, рассмотрим несколько более общую ситуацию. Согласно теореме 3 § 2, гл. 5 из [ВА I] любое изоморфное отображение  $\varphi$  поля  $P$  на поле  $\tilde{P}$  продолжается единственным образом до изоморфизма  $P[X]$  на  $\tilde{P}[X]$ , так что

$$\begin{aligned} f(X) = x^n + a_1 X^{n-1} + \dots + a_n &\mapsto \tilde{f}(X) = \varphi_X f = \\ &= X^n + \varphi(a_1) X^{n-1} + \dots + \varphi(a_n). \end{aligned}$$

**Теорема 3.** Пусть  $\varphi : P \rightarrow \tilde{P}$  — изоморфизм полей;  $f \in P[X]$  — нормализованный многочлен степени  $n > 0$ ,  $\tilde{f} = \varphi_X f$  — его образ при изоморфизме  $\varphi_X$ ;  $F, \tilde{F}$  — поля разложения многочленов  $f, \tilde{f}$  над  $P$  и над  $\tilde{P}$  соответственно. Тогда  $\varphi$  продолжается до изоморфизма  $\Phi : F \rightarrow \tilde{F}$   $k \leq [F : P]$  способами, причём  $k = [F : P]$ , если все корни многочлена  $f(X)$  различны.

**Доказательство.** Этап I. Вначале рассмотрим случай произвольных расширений  $K \supset P$ ,  $\tilde{K} \supset \tilde{P}$ . Пусть  $\theta \in K$  — алгебраический элемент с минимальным многочленом  $g = g_\theta \in P[X]$ . Утверждается, что изоморфизм  $\varphi : P \rightarrow \tilde{P}$  продолжается до мономорфизма  $\rho : P(\theta) \rightarrow \tilde{K}$  в точности тогда, когда  $\tilde{g}$  обладает корнем в  $K$ , причём число продолжений совпадает с числом различных корней многочлена  $\tilde{g}$  в  $\tilde{K}$ .

Действительно, из существования  $\rho$  следует, что элемент  $\rho(\theta)$  должен быть корнем  $\tilde{g}$ :

$$g(\theta) = 0 \implies \tilde{g}(\rho(\theta)) = \rho(g(\theta)) = 0.$$

Обратно: если  $g(\omega) = 0$ , то  $\text{Ker } \psi \supset g(X)P[X]$ , где  $\psi : P[X] \rightarrow \tilde{K}$  — гомоморфизм, определённый соответствием  $u(X) \mapsto \tilde{u}(\omega)$ . Как и в случае групп,  $\psi$  индуцирует гомоморфизм

$$\overline{\psi} : P[X]/g(X)P[X] \rightarrow \tilde{K}$$

$(u(X) + g(X)P[X]) \mapsto \tilde{u}(\omega)$ ; если это не совсем ясно, то нужно снова обратиться к результатам гл. 4). Заметим, что ввиду неприводимос-

ти  $g(X)$  факторкольцо  $P[X]/g(X)P[X]$  — поле, так что  $\bar{\psi}$  — мономорфизм. Точно таким же способом определяется изоморфизм полей  $\bar{\sigma} : P[X]/g(X)P[X] \rightarrow P(\theta)$  ( $u(X) + g(X)P[X] \mapsto u(\theta)$ ). Композиция  $\rho = \bar{\psi} \circ \bar{\sigma}^{-1}$  является мономорфным отображением  $P(\theta)$  в  $\tilde{K}$  ( $\rho(u(\theta)) = \tilde{u}(\omega)$ ). Так как  $P(\theta)$  порождается над  $P$  элементом  $\theta$ , то  $\rho$  — единственное продолжение  $\varphi$ , переводящее  $\theta$  в  $\omega$ . Это и означает, что число различных мономорфизмов  $\rho$  с ограничением  $\rho|_P = \varphi$  равно числу различных корней многочлена  $\tilde{g}(X)$  в  $\tilde{K}$ .

Этап II. Поле разложения строилось последовательным присоединением корней неприводимых многочленов. Используем далее индукцию по размерности  $[F : P]$ . При  $[F : P] = 1$  многочлен  $f$  разлагается на линейные множители уже в  $P[X] : f(X) = (X - c_1) \dots (X - c_n)$ . В таком случае  $\tilde{f}(X) = (\varphi_X f)(X) = (X - \tilde{c}_1) \dots (X - \tilde{c}_n)$ . Корни  $\tilde{c}_1, \dots, \tilde{c}_n$  многочлена  $\tilde{f}$  содержатся в  $\tilde{P}$ , а поскольку  $\tilde{F}$  порождается ими над  $\tilde{P}$ , то  $\tilde{F} = \tilde{P}$ , так что  $\Phi = \varphi_X$  — единственное продолжение.

При  $[F : P] > 1$  разложим  $f(X)$  над  $P$  на нормализованные неприводимые множители, среди которых должен быть хотя бы один многочлен степени  $m > 1$ . Обозначим его  $g(X)$ . Так как

$$f(X) = g(X)h(X) \implies \tilde{f}(X) = (\varphi_X f)(X) = \tilde{g}(X)\tilde{h}(X),$$

то над полями разложения  $F$  и  $\tilde{F}$  имеют место разложения многочленов

$$g(X) = (X - \theta_1) \dots (X - \theta_m),$$

$$\tilde{g}(X) = (X - \omega_1) \dots (X - \omega_m), \quad m \leq n.$$

Ввиду неприводимости  $g(X)$  является минимальным многочленом элемента  $\theta_1$  над  $P$  и  $[P(\theta_1) : P] = m$ .

Если среди  $\omega_1, \dots, \omega_m$  имеется  $l$  различных, то согласно этапу I найдётся  $l$  мономорфных отображений  $\rho_1, \dots, \rho_l$  расширения  $L = P(\theta_1)$  в  $\tilde{F}$  с ограничением  $\rho_i|_P = \varphi$ . Конструкция поля разложения такова, что  $F$  можно считать полем разложения над  $L$  многочлена  $f \in L[X]$ , а  $\tilde{F}$  можно считать полем разложения над  $\rho_i(L)$  многочлена  $\tilde{f}(X)$  при любом  $i = 1, 2, \dots, l$ . По теореме 2 имеем неравенство

$$[F : L] = \frac{[F : P]}{m} < F : P],$$

так что по предположению индукции каждый из  $\rho_i$  можно продолжить до изоморфизма  $\Phi_{i,j} : F \rightarrow \tilde{F}$ , причём число таких продолжений (число индексов  $j$ ) не превосходит  $[F : L]$  и равно этой верхней границе, если все корни в  $\tilde{F}$  многочлена  $\tilde{f}$  различны. Так как

$$\Phi_{i,j}|_L = \rho_i, \quad 1 \leq j \leq [F : L], \quad \rho_i|_P = \varphi,$$

то  $\Phi_{i,j}$  — продолжение  $\varphi$ , причём

$$\rho_i \neq \rho_s \implies \Phi_{i,j} \neq \Phi_{s,t} \text{ при } i \neq s.$$

Стало быть, всего получается  $k \leq m[F : L] = [F : P]$  продолжений изоморфизма  $\varphi$ . Это неравенство переходит в равенство, если все корни многочлена  $\tilde{f}$  различны.

**Этап III.** Пусть, наконец,  $\Phi : F \rightarrow \tilde{F}$  — произвольное продолжение изоморфизма  $\varphi$ . Как и в этапе II, ограничение  $\Phi|_L$ , будучи мономорфным отображением  $L$  в  $\tilde{F}$ , совпадает с одним из  $\rho_i$ , а в таком случае  $\Phi$  совпадает с одним из  $\Phi_{i,j}$ .  $\square$

**Следствие 1.** *Любые два поля разложения  $F$ ,  $\tilde{F}$  над  $P$  многочлена  $f \in P[X]$  изоморфны.*

Действительно, достаточно положить  $\tilde{P} = P$  в теореме 3 и взять за  $\varphi$  единичное отображение поля  $P$  на себя.  $\square$

**Следствие 2.** *Группа автоморфизмов  $\text{Aut } F/P$  любого поля разложения  $F$  над  $P$  многочлена  $f \in P[X]$  конечна и имеет порядок  $\leq [F : P]$ . Если все корни многочлена  $f(X)$  различны, то  $|\text{Aut } F/P| = [F : P]$ .*

**Доказательство** непосредственно следует из теоремы 3.  $\square$

**Замечание.** Хотя поле разложения  $F$  над  $\mathbb{Q}$  (или над любым другим числовым полем) многочлена  $f \in \mathbb{Q}[X]$  можно считать вложенным в поле  $\mathbb{C}$  комплексных чисел и тем самым однозначно определённым, следствие 2 показывает, что и в этом случае имело смысл разобрать доказательство теоремы 3.

Расширение  $\overline{P}/P$  называется *алгебраическим замыканием поля  $P$* , если оно алгебраично и поле  $\overline{P}$  алгебраически замкнуто. Сравнительно нетрудно доказать, что всякое поле  $P$  обладает алгебраически замкнутым расширением, однозначно определённым с точностью до  $P$ -изоморфизма. Любое алгебраическое расширение  $F/P$  можно вложить  $\leq [F : P]$  способами в алгебраическое замыкание  $\overline{P}$  поля  $P$ .

**3. Существование примитивного элемента.** Многочлен из  $P[X]$  называется *сепарабельным*, если его неприводимые множители имеют различные корни. Поле  $P$  называется *совершенным*, коль скоро каждый многочлен  $f \in P[X]$  сепарабельный. Понятно, что любое поле  $P$  нулевой характеристики будет совершенным. С другой стороны, верна

**Теорема 4.** *Пусть  $P$  — поле характеристики  $p > 0$ . Тогда  $P$  будет совершенным в точности при  $P = P^p$  (множество  $p$ - степеней всех элементов из  $P$ ).*

**Доказательство.** Если  $P^p \subsetneq P$  и  $a \in P \setminus P^p$ , то многочлен  $X^p - a$  неприводим (см. ниже упр. 4). Кроме того,  $(X^p - a)' = pX^{p-1} = 0$ , так что  $X^p - a$  — несепарабельный многочлен, а значит,  $P$  — несовершенное поле.

Обратно: предположим, что  $f(X)$  — несепарабельный неприводимый многочлен в  $P[X]$ , т.е.  $\text{НОД}(f, f') \neq 1$ . Тогда  $f(X) =$

$= a_0 + a_p X^p + a_{2p} X^{2p} + \dots$ . Если  $a_i = b_i^p$  для любого  $i$ , то  $f(X) = (b_0 + b_1 X + b_2 X^2 + \dots)^p$  — противоречие с неприводимостью  $f(X)$ . Следовательно,  $a_i \notin P^p$  для некоторого  $i$ , а поэтому  $P^p \neq P$ .  $\square$

Конечное алгебраическое расширение  $F \supset P$ , получающееся при соединением к  $P$  конечного числа сепарабельных элементов (корней неприводимых сепарабельных многочленов), называется *сепарабельным расширением*. Если не привлекать к рассмотрению алгебраические замыкания  $\bar{P}$  поля  $P$ , то можно ограничиться полями алгебраических чисел, вложенными по определению в  $\mathbb{C}$ .

**Теорема 5.** *Пусть  $F$  — конечное расширение поля  $P$ . Примитивный элемент  $\theta \in F$  (когда  $F = P(\theta)$ ) существует в точности тогда, когда число промежуточных полей  $E$  ( $F \supset E \supset P$ ) конечно. Если  $F$  сепарабельно над  $P$ , то примитивный элемент  $\theta$  существует.*

**Доказательство.** Для конечного поля  $P$  всё ясно, поскольку  $F^* = \langle \theta \rangle$ , и  $\theta$  будет примитивным элементом. Считаем  $P$  бесконечным.

Предположим сначала, что число промежуточных полей конечно. Пусть  $\alpha, \beta \in F$ . Заставив  $c$  пробегать по элементам из  $P$ , мы получим по условию лишь конечное число полей типа  $P(\alpha + c\beta)$ . Следовательно, найдутся  $c_1, c_2 \in P$ ,  $c_1 \neq c_2$ , такие, что

$$E := P(\alpha + c_1\beta) = P(\alpha + c_2\beta).$$

Заметим, что

$$\alpha + c_1\beta, \alpha + c_2\beta \in E \implies (c_1 - c_2)\beta \in E \implies \beta \in E \implies \alpha \in E,$$

т.е.  $P(\alpha, \beta) = E = P(\alpha + c_1\beta)$ . Действуя по индукции, приходим к выводу, что если  $F = P(\alpha_1, \dots, \alpha_n)$ , то найдутся  $c_2, \dots, c_n \in P$ , для которых

$$F = P(\theta), \quad \theta = \alpha_1 + c_2\alpha_2 + \dots + c_n\alpha_n.$$

Это доказывает половину первого утверждения.

Обратно: предположим, что  $F = P(\theta)$  для некоторого  $\theta$  и  $f = f_\theta(X)$  — минимальный многочлен для  $\theta$ . Пусть  $P \subset E \subset F$ , и пусть  $g_{E,\theta}$  — минимальный многочлен для  $\theta$  над  $E$ . Очевидно,  $g_{E,\theta}$  делит  $f_\theta$ . Но  $F[X]$  — факториальное кольцо; любой нормализованный многочлен из  $F[X]$ , делящий  $f(X)$ , равен произведению некоторого числа множителей  $X - \alpha_i$ , где  $\alpha_1, \dots, \alpha_n$  — корни  $f$ . Следовательно, имеется лишь конечное число таких многочленов. Мы получаем отображение  $E \mapsto g_E$  из множества промежуточных полей в конечное множество многочленов.

Пусть  $E_0$  — подполе в  $E$ , порождённое над  $P$  коэффициентами в  $g_E(X)$ . Тогда  $g_E$  имеет коэффициенты в  $E_0$  и является неприводимым над  $E_0$ , поскольку он неприводим над  $E$ . Стало быть, степень

элемента  $\theta$  над  $E_0$  совпадает со степенью  $\theta$  над  $E$ , а это даёт равенство  $E = E_0$ . Таким образом, наше поле  $E$  однозначно определяется ассоциированным с ним многочленом  $g_E$ . Поэтому отображение  $E \mapsto \mapsto g_E$  инъективно. Это завершает доказательство первого утверждения теоремы.

Что касается утверждения относительно сепарабельных расширений, то, действуя по индукции, мы можем без потери общности предполагать, что  $F = P(\alpha, \beta)$ , где  $\alpha, \beta$  сепарабельны над  $P$ . Пусть  $\varphi_1, \dots, \varphi_n$  — различные вложения  $P(\alpha, \beta)$  в алгебраическое замыкание  $\overline{P}$  поля  $P$ . Положим

$$f(X) = \prod_{i \neq j} (\varphi_i \alpha + X \varphi_i \beta - \varphi_j \alpha - X \varphi_j \beta).$$

Тогда  $f(X) \neq 0$ , и поэтому найдётся  $c \in P$ , для которого  $f(c) \neq 0$ . Элементы  $\varphi_i(\alpha + c\beta)$  при  $i = 1, \dots, n$  различны, откуда следует, что  $[P(\alpha + c\beta) : P] \geq n$ . Но  $[P(\alpha, \beta) : P] = n$ , поэтому

$$P(\alpha, \beta) = P(\alpha + c\beta).$$

Другими словами,  $\theta = \alpha + c\beta$  — примитивный элемент.  $\square$

### УПРАЖНЕНИЯ

1. Показать, что расширение  $F \supset P$  простой степени не имеет собственных ( $\neq P, F$ ) подполяй.
2. Найти примитивный элемент расширения  $\mathbb{Q}(\sqrt{p}, \sqrt{q})$ , где  $p$  и  $q$  — простые числа.
3. Найти размерность над  $\mathbb{Q}$  поля разложения многочлена  $X^p - 2$ .
4. Показать, что над полем  $P$  характеристики  $p > 0$  для многочлена  $X^p - a$  имеются лишь две возможности: быть неприводимым или же быть  $p$ -й степенью линейного многочлена.
5. Пусть  $Z_p(Y)$  — поле рациональных дробей характеристики  $p$ . Показать, что  $X^p - Y$  — неприводимый над  $Z_p(Y)$  многочлен, все корни которого совпадают.

## § 2. Конечные поля

**1. Существование и единственность.** Помимо  $Z_p = \mathbb{Z}/p\mathbb{Z}$ , нам встречались и другие примеры конечных полей. Настало время включить их в общую теорию. Первые очевидные замечания относятся к произвольному конечному расширению конечного поля.

**Предложение 1.** Пусть  $F$  — поле с числом элементов  $q$  и  $K \supset F$  — расширение степени  $[K : F] = n$ . Тогда  $|K| = q^n$ .

**Доказательство.** Действительно, после выбора базиса векторное пространство  $K$  над  $F$  отождествляется с пространством  $F^n$  строк  $(\alpha_1, \dots, \alpha_n)$  длины  $n$ . Все координаты  $\alpha_i$  независимо друг от друга принимают  $q$  значений из  $F$ . Значит,  $|K| = |F^n| = q^n$ .  $\square$

**Предложение 2.** *Любое конечное поле  $F$  имеет конечную характеристику  $p$  ( $p$  — простое число) и  $|F|$  является степенью  $p$ .*

**Доказательство.** В самом деле, простое подполе  $P \subset F$  в силу конечности  $F$  должно быть изоморфно некоторому полю  $Z_p = \mathbb{Z}/p\mathbb{Z}$ . Согласно предложению 1 конечное расширение  $F \supset P$  с  $|P| = p$  имеет мощность  $|F| = p^m$ .  $\square$

**Теорема 1.** *Для каждого конечного поля  $F$  и для каждого целого положительного числа  $n$  существует одно и, с точностью до изоморфизма, только одно расширение  $K \supset F$  степени  $[K : F] = n$ .*

**Доказательство.** Единственность. Пусть  $K \supset F$  — расширение степени  $n$ . Согласно предложению 2  $|F| = q \implies q = p^m$ ,  $p$  простое и  $|K| = q^n$ . Следовательно, мультипликативная группа  $K^* = K \setminus \{0\}$  имеет порядок  $q^n - 1$ , а порядок каждого её элемента по теореме Лагранжа делит  $q^n - 1$ :  $t^{q^n - 1} = 1 \quad \forall t \neq 0$ . Это значит, что все элементы поля  $K$  (включая  $t = 0$ ) являются различными корнями многочлена  $X^{q^n} - X$  и имеет место разложение

$$X^{q^n} - X = \prod_{t \in K} (X - t).$$

Ни над каким собственным подполем поля  $K$  с числом элементов  $< q^n$  такого разложения на линейные множители быть не может, поэтому  $K$  — поле разложения многочлена  $X^{q^n} - X$ . Обращаясь к следствию 1 теоремы 3 из § 1, мы приходим к требуемому заключению.

**Существование.** Рассуждения при доказательстве единственности подсказывают возможный путь построения  $K$ . Возьмём за  $K$  поле разложения над  $P \cong Z_p$  многочлена  $f(X) = X^{q^n} - X$ . Так как  $q = p^m$ , то  $q \cdot 1 = 0$  в  $K$ . Поэтому  $f'(X) = q^n \cdot 1 \cdot X^{q^n - 1} - 1 = -1$  и по известному критерию [ВА I, гл. 6, § 1, теорема 4]  $f(X)$  не имеет кратных корней. Это значит, что подмножество  $K_f \subset K$  корней многочлена  $f(X)$  имеет мощность  $|K_f| = q^n$ .

Так как  $K_f \subset K$  и  $\text{char } K = p$ , то согласно [ВА I, гл. 4, § 3, упр. 6]  $(x + y)^{p^s} = x^{p^s} + y^{p^s}$  для любых  $x, y \in K_f$  и  $s = 0, 1, 2, \dots$  (отметим, что  $F \subset K_f$ ). В частности,

$$x, y \in K_f \implies (x \pm y)^{q^n} = x^{q^n} \pm y^{q^n} = x \pm y \implies x \pm y \in K_f.$$

Кроме того,

$$1 \in K_f; \quad (xy)^{q^n} = x^{q^n}y^{q^n} = xy \implies xy \in K_f;$$

$$0 \neq x \in K_f \implies (x^{-1})^{q^n} = x^{-1} \implies x^{-1} \in K_f.$$

Таким образом,  $K_f$  — подполе в  $K$ , содержащее  $F$  и все корни многочлена  $f(X)$ . В соответствии с определением поля разложения должно выполняться равенство  $K_f = K$ . Степень  $[K : F]$  равна  $n$ , поскольку  $q^{[K:F]} = |K| = |K_f| = q^n$ .  $\square$

**Следствие.** Для каждого простого числа  $p$  и для каждого цепного положительного числа  $n$  существует одно и, с точностью до изоморфизма, только одно поле с числом элементов  $p^n$ .

Доказательство заключается в применении теоремы 1 к частному случаю  $|F| = p$ .  $\square$

**2. Под поля и автоморфизмы конечного поля.** Как уже отмечалось в [ВА I, гл. 4, § 3], конечное поле с числом элементов  $q = p^n$  принято обозначать символом  $\mathbb{F}_q$  или, в честь Э. Галуа, символом  $GF(p^n)$ . Установим ряд свойств конечных полей.

**Теорема 2.** Справедливы следующие утверждения.

i) Мультипликативная группа  $F_q^*$  конечного поля  $\mathbb{F}_q$  является циклической группой порядка  $q - 1$ .

ii) Группа автоморфизмов  $\text{Aut } \mathbb{F}_q$  конечного поля  $\mathbb{F}_q$  с числом элементов  $q = p^n$  циклическая порядка  $n$ , причём

$$\text{Aut } \mathbb{F}_q = \langle \Phi \mid \Phi(t) = t^p \quad \forall t \in \mathbb{F}_q \rangle.$$

iii) Если  $\mathbb{F}_{p^d}$  — подполе поля  $\mathbb{F}_{p^n}$ , то  $d \mid n$ . Обратно: каждому делителю  $d$  числа  $n$  отвечает ровно одно подполе  $\{t \in \mathbb{F}_{p^n} \mid \Phi^d(t) = t\} = \mathbb{F}_{p^d}$ . Автоморфизмы, оставляющие это подполе поэлементно неподвижным, образуют группу  $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) = \langle \Phi^d \rangle$ . Таким образом, имеется биективное соответствие между подполями конечного поля  $\mathbb{F}_q$  и подгруппами его группы автоморфизмов (соответствие Галуа).

iv) Если  $q = p^n$  и  $\mathbb{F}_q^* = \langle \theta \rangle$ , то  $\theta$  — примитивный элемент поля с минимальным многочленом  $h(X)$  степени  $n$  и  $\mathbb{F}_q$  — поле разложения над  $\mathbb{F}_p$  многочлена  $h(X)$ .

v) Для любого натурального числа  $t$  существует хотя бы один неприводимый многочлен степени  $t$  над  $\mathbb{F}_q$ .

Доказательство. i) См. теорему 11 из § 3 гл. 2.

ii) Будем смотреть на  $\mathbb{F}_q$  как на конечное расширение  $\mathbb{F}_q \supset \mathbb{F}_p$  степени  $n$  своего простого под поля  $\mathbb{F}_p \cong Z_p$ . Так как  $\mathbb{F}_q$  — поле разложения многочлена  $X^q - X$ , все корни которого различны, то согласно следствию 2 теоремы 3 из § 1  $|\text{Aut } \mathbb{F}_q| = n$ . Из соотношений  $(x + y)^p = x^p + y^p$ ,  $(xy)^p = x^p y^p$ ,  $1^p = 1$ , отмеченных в ходе доказательства теоремы 1, видно, что отображение  $\Phi : t \mapsto t^p$  является автоморфизмом поля  $\mathbb{F}_q$  (конечность  $\mathbb{F}_q$  существенна). Если  $\Phi^s : t \mapsto t^{p^s}$  — единичный автоморфизм, то  $t^{p^s} - t = 0$  для всех  $t \in \mathbb{F}_q$ , откуда следует неравенство  $s \geq n$ . Но при  $s = n$  мы действительно получаем единичный автоморфизм, так что  $|\langle \Phi \rangle| = n$  и  $\langle \Phi \rangle = \text{Aut } \mathbb{F}_q$ .

iii) Согласно предложению 1  $p^n = (p^d)^r$ , где  $r$  — степень расширения  $\mathbb{F}_{p^n} \supset \mathbb{F}_{p^d}$ . Поэтому  $n = dr$ . Обратно: для любого  $d \mid n$  введём подмножество  $F = \{t \in \mathbb{F}_{p^n} \mid t^{p^d} = t\}$ . Так как  $n = dr \implies p^n - 1 =$

$= (p^d)^r - 1 = (p^d - 1)k$ , то

$$X^{p^n-1} - 1 = X^{(p^d-1)k} - 1 = (X^{p^d-1} - 1)g(X),$$

$$X^{p^n} - X = (X^{p^d} - X)g(X).$$

Так как  $\mathbb{F}_{p^n}$  — поле разложения многочлена  $X^{p^n} - X$ , то ровно  $p^d$  элементов из  $\mathbb{F}_{p^n}$  будут корнями многочлена  $X^{p^d} - X$ . Из них как раз и состоит подмножество  $F$ , которое можно теперь отождествить с  $\mathbb{F}_{p^d}$ . Этим рассуждением, дуальным теореме 1, устанавливается также единственность подполя с  $p^d$  элементами.

Заметим, что по построению

$$\mathbb{F}_{p^d} = \{t \in \mathbb{F}_{p^n} \mid \Phi^d(t) = t\}$$

— множество всех элементов, остающихся на месте при действии  $\langle \Phi^d \rangle$ . Так как группа  $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \Phi \rangle$  циклическая, то непосредственно видно, что любой автоморфизм  $\Phi^l$ , не принадлежащий  $\langle \Phi^d \rangle$ , действует на  $\mathbb{F}_{p^d}$  неединичным образом (достаточно применить  $\Phi^l$  к образующей группы  $\mathbb{F}_{p^d}^*$ ). Это означает, что группа относительных автоморфизмов  $\text{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})$  совпадает с  $\langle \Phi^d \rangle$ . Заключительная фраза в утверждении iii) имеет тот же смысл, что и в примере п. 1.

iv) Совершенно очевидно, что  $\mathbb{F}_q = \mathbb{F}_p(\theta)$ ,  $q = p^n$ . Пусть  $h(X) = X^n + a_1X^{n-1} + \dots + a_n$  — минимальный многочлен примитивного элемента  $\theta$ . Так как элементы простого под поля  $\mathbb{F}_p$  неподвижны при всех автоморфизмах, а  $a_i \in \mathbb{F}_p$ , то, стало быть, корнями  $h(X)$  являются  $\theta, \theta^p, \theta^{p^2}, \dots, \theta^{p^{n-1}}$ . Все они содержатся в нашем поле и

$$\mathbb{F}_p(\theta, \dots, \theta^{p^{n-1}}) = \mathbb{F}_p(\theta) = \mathbb{F}_{p^n}$$

— поле разложения над  $\mathbb{F}_p$  многочлена  $h(X)$ .

v) Опираясь на теорему 1, построим расширение  $K \supset \mathbb{F}_q$  степени  $m$ . Согласно i)  $K^*$  — циклическая группа. Если  $K^* = \langle \theta \rangle$  и  $h(X)$  — минимальный многочлен примитивного элемента  $\theta$ , то  $K = \mathbb{F}_q(\theta)$  и  $\deg h(X) = [\mathbb{F}_q(\theta) : \mathbb{F}_q] = [K : \mathbb{F}_q] = m$ . Минимальный многочлен по определению неприводим (над  $\mathbb{F}_q$ ), поэтому мы имеем то, что нужно.  $\square$

После несложных теоретико-числовых приготовлений мы получим точную формулу для числа неприводимых многочленов степени  $t$  над  $\mathbb{F}_q$ .

**3. Формула обращения Мёбиуса и ее применения.** Теоретико-числовая функция  $\mu$ , определённая правилами

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n = p_1 \dots p_k, \text{ } p_i \text{ различные простые,} \\ 0, & \text{если } n \text{ делится на квадрат } > 1, \end{cases}$$

называется *функцией Мёбиуса*. Ясно, что  $\mu$  — *мультипликативная функция* в том смысле, что  $\mu$  не равна тождественно нулю и  $\mu(mn) = \mu(m)\mu(n)$  для любых взаимно простых  $m$  и  $n$ . Ясно также, что если  $n = p_1^{m_1} \dots p_r^{m_r}$ , то

$$\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d),$$

где  $n_0 = p_1 \dots p_r$  — свободный от квадратов максимальный делитель числа  $n$ . В свою очередь число делителей  $d = p_{i_1} \dots p_{i_s}$  числа  $n_0$  с фиксированным  $s$  равно  $\binom{r}{s}$ . Таким образом, при  $n > 1$  имеем

$$\sum_{d|n} \mu(d) = \sum_{d|n_0} \mu(d) = \sum_{s=0}^r \binom{r}{s} (-1)^s = (1 - 1)^r = 0$$

(суммирование в левой части ведётся по всем делителям  $d \geq 1$  целого числа  $n$ ). Окончательно получаем формулу

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n > 1. \end{cases} \quad (1)$$

Полезна также её модификация

$$\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & \text{если } d = m, \\ 0, & \text{если } d | m, d < m \end{cases} \quad (2)$$

(суммирование ведётся по  $n$ , делящим  $m$  и делящимся на  $d$ ). Положив  $m = dt$ ,  $n = dl$  и заставив  $l$  пробегать делители числа  $t$ , мы легко перейдём от (2) к (1), и обратно.

Формулу (1) (или (2)) можно было бы взять за определение функции Мёбиуса по индукции. Её ценность для нас заключена в следующем утверждении.

Пусть  $f$  и  $g$  — две произвольные функции из  $\mathbb{N}$  в  $M$  ( $M$  равно  $\mathbb{Z}$ ,  $\mathbb{R}$ ,  $F[X]$  и т.д.), связанные соотношением

$$f(n) = \sum_{d|n} g(d). \quad (3)$$

Тогда

$$g(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) f(d). \quad (4)$$

В самом деле, с учётом (2) непосредственное суммирование по  $n$ , делящим  $m$ , обеих частей (3), умноженных на  $\mu(m/n)$ , даёт

$$\sum_{n|m} \mu\left(\frac{m}{n}\right) f(n) = \sum_{n|m} \mu\left(\frac{m}{n}\right) \sum_{d|n} g(d) = \sum_{d|m} g(d) \sum_{d|n|m} \mu\left(\frac{m}{n}\right) = g(m).$$

Простая замена обозначений приводит к формуле (4), называемой *формулой обращения Мёбиуса*. Аналогичным образом совершается переход от (4) к (3).  $\square$

Имеется ещё мультиплекативный аналог формулы обращения Мёбиуса: если  $f(n) = \prod_{d|n} g(d)$ , то

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)}. \quad (5)$$

Для доказательства нужно провести те же формальные выкладки:

$$\begin{aligned} \prod_{n|m} f(n)^{\mu(m/n)} &= \prod_{n|m} \prod_{d|n} g(d)^{\mu(m/n)} = \prod_{d|m} \prod_{d|n|m} g(d)^{\mu(m/n)} = \\ &= \prod_{d|m} g(d)^{\sum_{d|n|m} \mu(m/n)} = g(m), \end{aligned}$$

а затем слегка изменить обозначения.

Приведём три примера на применение формулы обращения Мёбиуса.

1) *Функция Эйлера*  $\varphi$ . По определению  $\varphi(n)$  — число взаимно простых с  $n$  чисел ряда  $1, 2, \dots, n - 1$ , или, что равносильно,  $\varphi(n) = |U(Z_n)|$  — порядок группы обратимых элементов кольца  $Z_n = \mathbb{Z}/n\mathbb{Z}$ . Из упр. 5 § 1 гл. 3 нам известно соотношение

$$n = \sum_{d|n} \varphi(d). \quad (6)$$

Непосредственно по формуле (4) получаем

$$\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)d = \sum_{d|n} \mu(d)\frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Если  $n = p_1^{m_1} \dots p_r^{m_r}$ , то

$$\begin{aligned} \sum_{d|n} \frac{\mu(d)}{d} &= 1 - \sum_i \frac{1}{p_i} + \sum_{i < j} \frac{1}{p_i p_j} - \dots + (-1)^r \frac{1}{p_1 p_2 \dots p_r} = \\ &= \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

Таким образом,

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right)$$

— формула, которую мы приводили ещё в [ВА I] и из которой непосредственно вытекает мультиплекативность функции  $\varphi$ .

2) *Круговые многочлены.* Поле разложения  $\Gamma_n$  над  $\mathbb{Q}$  многочлена  $X^n - 1$  называется *круговым* или *циклотомическим*. Так как все корни степени  $n$  из 1 образуют циклическую группу порядка  $n$ , то круговое поле имеет вид  $\Gamma_n = \mathbb{Q}(\zeta)$ , где  $\zeta$  — один из примитивных корней ( $\zeta \in \mathbb{C}$ ). Мы хотели бы найти степень  $[\Gamma_n : \mathbb{Q}]$  и минимальный многочлен элемента  $\zeta$  над  $\mathbb{Q}$ .

Обозначим символом  $P_n$  множество мощности  $|P_n| = \varphi(n)$  примитивных корней степени  $n$  из 1. Подгруппы циклической группы порядка  $n$  находятся в биективном соответствии с делителями  $d$  числа  $n$ , а каждый корень  $\zeta^i$  попадает в некоторое множество  $P_d$ . Поэтому имеет место разбиение на непересекающиеся классы:

$$\{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\} = \bigcup_{d|n} P_d \quad (7)$$

(перейдя к мощностям множеств, мы снова пришли бы к соотношению (6)). *Круговым многочленом*, отвечающим  $\Gamma_n$ , называется многочлен

$$\Phi_n(X) = \prod_{\zeta} (X - \zeta)$$

степени  $\varphi(n)$ . В соответствии с разбиением (7) мы приходим к разложению

$$X^n - 1 = \prod_{i=0}^{n-1} (X - \zeta^i) = \prod_{d|n} \left\{ \prod_{\zeta \in P_d} (X - \zeta) \right\} = \prod_{d|n} \Phi_d(X). \quad (8)$$

Применяя к (8) мультипликативную формулу обращения Мёбиуса (5), получаем явное выражение для  $\Phi_n$ :

$$\Phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}. \quad (9)$$

При небольших значениях  $n$  имеем

$$\begin{aligned} \Phi_1(X) &= X - 1, & \Phi_2(X) &= X + 1, & \Phi_3(X) &= X^2 + X + 1, \\ \Phi_4(X) &= X^2 + 1, & \Phi_6(X) &= X^2 - X + 1, & \Phi_8(X) &= X^4 + 1, \\ \Phi_9(X) &= X^6 + X^3 + 1, & \Phi_{10}(X) &= X^4 - X^3 + X^2 - X + 1, \\ \Phi_{12}(X) &= X^4 - X^2 + 1. \end{aligned}$$

Заметим, что

$$\Phi_n(X) \in \mathbb{Z}[X], \quad \Phi_n(0) = 1, \quad n > 1. \quad (10)$$

Чтобы прийти к (10), можно, минуя (9), действовать по индукции. Для небольших  $n$  это проверено, а далее рассуждаем следующим образом. Считая

$$g(X) = \prod_{d|n, d \neq n} \Phi_d(X)$$

нормализованным многочленом с целочисленными коэффициентами и применяя алгоритм деления с остатком (см. [ВА I]), мы получаем однозначно определённые многочлены  $q, r \in \mathbb{Z}[X]$  такие, что

$$X^n - 1 = q(X)g(X) + r(X), \quad \deg r(X) < \deg g(X).$$

Но  $X^n - 1 = \Phi_n(X)g(X)$  в  $\mathbb{Q}[X]$ , и мы видим, что  $\Phi_n(X) = q(X) \in \mathbb{Z}[X]$ , причём нормализованность  $g(X)$  влечёт нормализованность  $\Phi_n(X)$ .

Ещё в [ВА I] была установлена неприводимость многочлена

$$\Phi_p(X) = (X^p - 1)/(X - 1) = X^{p-1} + X^{p-2} + \dots + 1,$$

где  $p$  — произвольное простое число. К вопросу о неприводимости  $\Phi_n(X)$  при любом  $n$  мы вернёмся в следующем параграфе.

3) *Неприводимые многочлены над  $\mathbb{F}_q$ .* Пусть  $\Psi_d(q)$  — общее число неприводимых нормализованных многочленов степени  $d$  над  $\mathbb{F}_q$ ,  $q = p^n$ , и пусть  $f(X)$  — один из этих многочленов. Его поле разложения над  $\mathbb{F}_q$  изоморфно как факторкольцу  $\mathbb{F}_q[X]/(f(X))$ , так и полю разложения многочлена  $X^{q^d} - X$  (следствие теоремы 1). Существование общего корня  $\theta$  у многочленов  $X^{q^d} - X$  и  $f(X)$  влечёт, в силу неприводимости  $f(X)$ , делимость  $X^{q^d} - X$  на  $f(X)$ . Так как  $X^{q^d} - X$  — делитель многочлена  $X^{q^m} - X$  при любом  $m = rd$  и так как  $X^{q^d} - X$  не имеет кратных корней, то мы приходим к выводу, что в разложение  $X^{q^m} - X$  над  $\mathbb{F}_q$  входят все унитарные неприводимые многочлены

$$f_{d,1}, f_{d,2}, \dots, f_{d,\Psi_d(q)}(X)$$

любой степени  $d \mid m$ , причём ровно по одному разу:

$$X^{q^m} - X = \prod_{d|m} \left\{ \prod_{k=1}^{\Psi_d(q)} f_{d,k}(X) \right\}. \quad (11)$$

Вычисление степеней многочленов, стоящих в обеих частях равенства (11), приводит нас к соотношению

$$q^m = \sum_{d|m} d \Psi_m(q),$$

из которого прямым применением формулы обращения Мёбиуса (4) получается выражение для  $\Psi_m(q)$ :

$$\Psi_m(q) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d. \quad (12)$$

Пусть, например,  $q = 2$ . Тогда

$$\Psi_2(2) = \frac{1}{2}(2^2 - 2) = 1, \quad \Psi_3(2) = \frac{1}{3}(2^3 - 2) = 2,$$

$$\Psi_4(2) = \frac{1}{4}(2^4 - 2^2) = 3, \quad \Psi_5(2) = \frac{1}{5}(2^5 - 2) = 6,$$

$$\Psi_6(2) = \frac{1}{6}(2^6 - 2^3 - 2^2 + 2) = 9.$$

Формула (12) показывает, что с вероятностью, близкой к  $1/m$ , случайно выбранный нормализованный многочлен степени  $m$  над  $\mathbb{F}_q$  окажется неприводимым. Однако нет удовлетворительных критериев неприводимости конкретно взятого многочлена. Что можно сказать, например, о неприводимости трёхчлена  $X^m + X^k + 1$ ? Вопросы такого рода постоянно возникают в алгебраической теории кодирования и при построении псевдослучайных последовательностей.

### УПРАЖНЕНИЯ

- Доказать, что при любом  $d | n$ ,  $d < n$ , имеет место соотношение  $X^n - 1 = (X^d - 1)\Phi_n(X)h_d(X)$ , где  $h_d \in \mathbb{Z}[X]$ .
- Пусть  $q$  — целое положительное число  $> 1$ . Согласно (10)  $\Phi_n(q) \in \mathbb{Z}$ . Показать, что  $\Phi_n(q)|(q - 1) \implies n = 1$ .
- Проверить, что круговой многочлен

$$\Phi_{15}(X) = X^8 - X^7 + X^5 - X^4 + X^3 - X + 1,$$

рассматриваемый над полем  $\mathbb{F}_2$ , является произведением двух неприводимых многочленов  $X^4 + X^3 + 1$  и  $X^4 + X + 1$ . Используя это обстоятельство, доказать неприводимость  $\Phi_{15}(X)$  над  $\mathbb{Q}$  (ср. с упр. 11 из [ВА I, гл. 6, § 1]).

- Проверить следующие свойства круговых многочленов.

Если  $p$  — простое число и  $p | n$ , то  $\Phi_{pn}(X) = \Phi_n(X^p)$ ; если же  $p \nmid n$ , то  $\Phi_{pn}(X) = \Phi_n(X^p)/\Phi_n(X)$ .

- Исходя из цепочки естественных включений

$$GF(p) \subset GF(p^{2!}) \subset GF(p^{3!}) \subset \dots,$$

ввести так называемое предельное поле  $\Omega_p = GF(p^{\infty!})$ , полагая

$$\alpha \in \Omega_p \iff \{\alpha \in GF(p^{n!}) \text{ при достаточно большом } n\}.$$

Опираясь на основные свойства конечных полей, доказать, что  $\Omega_p$  — алгебраически замкнутое поле. Таким образом получаются, с учётом поля комплексных чисел  $\mathbb{C}$ , примеры алгебраически замкнутых полей любой характеристики.

- Пусть  $q = p^n$ . Показать, что при  $p = 2$  все элементы поля  $\mathbb{F}_q$  являются квадратами, а при  $p > 2$  квадраты группы  $\mathbb{F}_q^*$  образуют в ней подгруппу  $\mathbb{F}_q^{*2}$  индекса 2, причём  $\mathbb{F}_q^{*2} = \text{Ker}(t \mapsto t^{(q-1)/2})$ .

**7** (M. Aschbacher). Пусть  $\mathbb{F}_q$  — конечное поле с нечётным числом  $q = p^n$  элементов. Если  $q$  не равно 3 или 5, то “на окружности”  $x^2 + y^2 = 1$  найдётся точка с координатами  $x, y \in \mathbb{F}_q^*$ . Доказать это утверждение при  $p > 5$ .

- Всякий ли примитивный элемент поля  $\mathbb{F}_q$  является образующей мультиплекативной группы  $\mathbb{F}_q^*$ ?

**9.** Пусть  $A(q) = \text{Ass}_F(X_1, \dots, X_q)$  — свободная ассоциативная алгебра над полем  $F$ , порождённая  $q$  свободными образующими — некоммутирующими переменными  $X_1, \dots, X_q$ . Положив

$$A_m(q) = \langle X_{i_1} X_{i_2} \dots X_{i_m} \mid 1 \leq i_j \leq q \rangle_F, \quad \dim A_m(q) = q^m,$$

мы замечаем, что  $A(q)$  — градуированная алгебра:

$$A(q) = F \cdot 1 \oplus A_1(q) \oplus A_2(q) \oplus A_3(q) \oplus \dots$$

В  $A(q)$  содержится свободная алгебра Ли  $L(q) = \text{Lie}(X_1, \dots, X_q)$  с теми же свободными образующими и операцией коммутирования  $[UV] = UV - VU$ . Алгебра  $L(q)$  также градуирована:

$$L(q) = L_1(q) \oplus L_2(q) \oplus L_3(q) \oplus \dots,$$

где

$$L_1(q) = \langle X_1, \dots, X_q \rangle_F, \quad L_2(q) = \langle [X_i, X_j] \mid i < j \rangle_F, \quad \dots$$

Используя тождество Якоби, убедиться в том, что

$$L_3(q) = \langle [[X_i, X_j], X_k] \rangle, \quad i < j, k \leq j; \quad \dim L_3(q) = \frac{1}{3}(q^3 - q).$$

На самом деле справедлива общая формула Витта

$$\dim L_m(q) = \Psi_m(q) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d, \quad (12')$$

в точности совпадающая с формулой (12). Существенная разница лишь в том, что в (12')  $q$  — произвольное натуральное число, а в (12) — степень простого числа.

Число ожерелий из задачи 2 в преамбуле к гл. 3 выражается такой же формулой.

### § 3. Соответствие Галуа

**1. Предварительные результаты.** Пусть  $F \supset P$  — поле разложения некоторого неприводимого над  $P$  многочлена  $f(X)$ ,  $\text{Aut } F/P$  — множество всех автоморфизмов  $\eta$  поля  $F$  таких, что  $\eta(a) = a \forall a \in P$ . Как мы знаем из §1,  $|\text{Aut } F/P| \leq [F : P]$ , причём  $|\text{Aut } F/P| = [F : P]$ , если все корни многочлена  $f$  различны.

**Определение.** Группу  $\text{Aut } F/P$  принято называть *группой Галуа* расширения  $F/P$  и обозначать  $\text{Gal } F/P$ . Этот термин уже был использован в ряде мест, включая § 1.

В дальнейшем поле  $P$  будет предполагаться совершенным, так что

$$|\text{Gal } F/P| = [F : P].$$

Пусть  $H \subset \text{Gal } F/P$  — любая подгруппа группы Галуа. Положим

$$F^H = \{a \in F \mid \varphi(a) = a \quad \forall \varphi \in H\}.$$

Таким образом,  $F^H$  — подполе в  $F$  всех элементов, остающихся не-подвижными при действии  $H$ . Имеем два отображения:

1)  $H \mapsto K = F^H$  — из множества подгрупп  $H \subset \text{Gal } F/P$  во множество подполей  $F \supset K \supset P$ ;

2)  $K \mapsto H = \text{Gal } F/K$  — из множества промежуточных подполей  $F \supset K \supset P$  во множество подгрупп  $H \subset \text{Gal } F/P$ .

Очевидные свойства:

- i)  $G = \text{Gal } F/P \supset G_1 \supset G_2 \implies F^{G_1} \subset F^{G_2}$ ;
- ii)  $F \supset P_1 \supset P_2 \supseteq P \implies \text{Gal } F/P_1 \subset \text{Gal } F/P_2$ ;
- iii)  $F^{\text{Gal } F/P} \supset P$ ;
- iv)  $\text{Gal } F/F^H \supset H$  для любой подгруппы  $H \subset G$ .

Будем временно понимать под  $K \supset P$  произвольное расширение поля  $P$  (не обязательно поле разложения).

**Лемма (Э. Артин).** Пусть  $G$  — конечная группа автоморфизмов поля  $K$  и  $P = K^G$ . Тогда

$$[K : P] \leq |G|.$$

**Доказательство.** Положим  $n = |G|$ . Нам нужно показать, что любые  $m > n$  элементов из  $K$  линейно зависимы над  $P$ . Пусть

$$G = \{\varphi_1 = e, \varphi_2, \dots, \varphi_n\}, \quad u_1, u_2, \dots, u_m \in K, \quad m > n.$$

Однородная система из  $n$  линейных уравнений от  $m$  неизвестных  $x_1, x_2, \dots, x_m$

$$\sum_{j=1}^m \varphi_i(u_j)x_j = 0, \quad 1 \leq i \leq n,$$

имеет нетривиальное решение  $(a_1, \dots, a_m) \neq (0, \dots, 0)$ . Среди всех решений выбираем такое  $(b_1, \dots, b_m)$ , у которого число ненулевых компонент наименьшее. Без ограничения общности считаем  $b_1 \neq 0$  и даже  $b_1 = 1$ . Достаточно показать, что  $b_j \in K^G \forall j$ , поскольку первое соотношение, отвечающее  $\varphi_1 = e$ , будет иметь вид  $\sum_{j=1}^m u_j b_j = 0$ .

Предположим, что  $b_j \notin P$  для некоторого  $j$ . После возможного переобозначения считаем  $b_j = b_2$ . Применим  $\varphi_k$  к системе уравнений, выбрав  $k$  таким, чтобы  $\varphi_k(b_2) \neq b_2$ . Получим

$$\sum_j (\varphi_k \varphi_i)(u_j) \varphi_k(b_j) = 0, \quad 1 \leq i \leq n,$$

или, что то же самое,

$$\sum_j \varphi_i(u_j) \varphi_k(b_j) = 0, \quad 1 \leq i \leq n,$$

поскольку  $\varphi_k \varphi_i$ ,  $i = 1, \dots, n$ , при фиксированном  $k$  пробегают все элементы группы  $G$ . Следовательно,  $(1, \varphi_k(b_2), \dots, \varphi_k(b_m))$  — тоже решение системы. Вычитая его из  $(1, b_2, \dots, b_m)$ , получим решение

$$(0, b_2 - \varphi_k(b_2), \dots, b_m - \varphi_k(b_m)),$$

которое также нетривиально, поскольку  $b_2 - \varphi_k(b_2) \neq 0$  ввиду выбора  $\varphi_k$ . Однако число ненулевых компонент у него меньше, чем у  $(b_1, b_2, \dots, b_m)$ , вопреки выбору последнего.  $\square$

**Определение.** Расширение  $F/P$  называется *нормальным алгебраическим*, если каждый неприводимый многочлен  $f \in P[X]$ , имеющий хотя бы один корень в  $F$ , является произведением линейных множителей в  $F[X]$ . Другими словами,  $F$  содержит поле разложения минимального многочлена  $f_a$  каждого элемента  $a \in F$ .

По определению свойство “нормальность плюс сепарабельность” эквивалентно тому, что каждый неприводимый многочлен из  $P[X]$ , имеющий корень в  $F$ , является произведением различных линейных множителей в  $F[X]$ . Нормальное и сепарабельное алгебраическое расширение  $F \supset P$  называется также *расширением Галуа*. Если  $F$  — поле разложения многочлена  $f \in P[X]$ , то  $\text{Gal } F/P$  называется также *группой Галуа многочлена  $f(X)$  над  $P$*  (или уравнения  $f(X) = 0$ ) и обозначается  $\text{Gal}(f)$ .

**Теорема 1.** Следующие условия на расширение  $F/P$  эквивалентны:

- 1)  $F$  — поле разложения некоторого сепарабельного многочлена  $f(X)$  над  $P$ ;
- 2)  $P = F^G$  для некоторой конечной группы  $G \subseteq \text{Aut } F$ ;
- 3)  $F$  — конечномерное нормальное и сепарабельное расширение над  $P$ .

Справедливы также следующие дополнения к утверждениям 1) и 2):

- Д1) если  $F$  и  $P$  такие же, как в 1), и  $G = \text{Gal } F/P$ , то  $P = F^G$ ;
- Д2) если  $F$  и  $P$  такие же, как в 2), то  $G = \text{Gal } F/P$ .

**Доказательство.** 1)  $\implies$  2). Положим в 1)  $G = \text{Gal } F/P$  и  $P' = F^G$ . Тогда  $P'$  — подполе в  $F$ , содержащее  $P$ . Ясно также, что  $F$  — поле разложения над  $P'$  многочлена  $f(X)$ , причём  $G = \text{Gal } F/P'$ .

В силу сепарабельности  $f$  имеем  $|G| = [F : P']$  так же, как  $|G| = [F : P]$ . Но  $F \supset P' \supseteq P \implies [F : P] = [F : P'][P' : P] \implies [P' : P] = 1 \implies P' = P$ , а это и есть 2). Мы доказали также, что  $P = F^G$  для  $G = \text{Gal } F/P$ , т.е. Д1).

2)  $\implies$  3). По лемме Артина

$$P = F^G \implies [F : P] \leq |G|$$

и, таким образом,  $F$  конечномерно над  $P$ . Пусть  $f$  — неприводимый многочлен в  $P[X]$ , имеющий корень  $r \in F$ . Будем считать, что

$$\{r_1 = r, r_2, \dots, r_m\} = \{\varphi(r) \mid \varphi \in G\}$$

—  $G$ -орбита с представителем  $r$ . Если  $\psi \in G$ , то  $\{\psi(r_1), \dots, \psi(r_m)\}$  — перестановка корней  $r_1, \dots, r_m$ . Разумеется,  $f(r) = 0 \implies f(r_i) = 0$ . Значит,  $f(X)$  делится на  $X - r_i$ , а поскольку  $r_i$ ,  $1 \leq i \leq m$ , различны,  $f(X)$  делится на  $g(X) = \prod_{i=1}^m (X - r_i)$ .

Применим к  $g(X)$  автоморфизм кольца  $F[X]$ , для которого  $X \mapsto$

$\mapsto X$  и  $a \mapsto \psi(a)$ ,  $a \in F$ . Тогда

$$\psi \cdot g(X) = \prod_{i=1}^m (X - \psi(r_i)) = \prod_{i=1}^m (X - r_i) = g(X),$$

и мы видим, что коэффициенты многочлена  $g(X)$  являются  $G$ -инвариантными. Следовательно,  $g(X) \in P[X]$ , поскольку  $F^G = P$ . Но  $f$  предполагался неприводимым над  $P$ . Значит,

$$f(X) = g(X) = \prod_{i=1}^m (X - r_i)$$

— произведение различных линейных множителей в  $F[X]$ , т.е. расширение  $F$  сепарабельно и нормально над  $P$ , как и утверждает 3).

3)  $\Rightarrow$  1). Так как  $[F : P] < \infty$ , то  $F = P(r_1, \dots, r_k)$ , где  $r_i$  алгебраичны над  $P$ . Пусть  $f_i(X)$  — минимальный многочлен для  $r_i$  над  $P$ . По условию  $f_i(X)$  — произведение различных линейных множителей в  $F[X]$ . Отсюда следует, что  $f(X) = \prod f_i(X)$  сепарабелен, а  $F$  — поле разложения над  $P$  для  $f(X)$ . Следовательно, мы пришли к 1).

Остается доказать Д2). Мы видели, что в условиях 2) по лемме Артина  $[F : P] \leq |G|$ , а поскольку по только что доказанному условию 3) имеет место,  $|\text{Gal } F/P| = [F : P]$ . Так как  $F^G = P \Rightarrow G \subset \text{Gal } F/P$  и  $|G| \geq [F : P] = |\text{Gal } F/P|$ , то  $G = \text{Gal } F/P$ .  $\square$

**2. Фундаментальное соответствие Галуа.** Теперь мы готовы доказать центральное утверждение.

**Теорема 2.** Пусть  $F$  — расширение поля  $P$ , удовлетворяющее любому из условий теоремы 1. Пусть  $G = \text{Gal } F/P$  — группа Галуа,  $\Gamma = \{H\}$  — множество подгрупп в  $G$  и  $\Sigma$  — множество промежуточных полей между  $F$  и  $P$ . Тогда отображения

$$\begin{cases} H \mapsto F^H, \\ K \mapsto \text{Gal } F/K \end{cases}$$

являются биекциями  $\Gamma$  на  $\Sigma$  и  $\Sigma$  на  $\Gamma$ . Кроме того, это соответствие Галуа обладает следующими свойствами:

- i)  $H_1 \supset H_2 \iff F^{H_1} \subset F^{H_2}$ ;
- ii)  $|H| = [F : F^H]$ ,  $(G : H) = [F^H : P]$ ;
- iii)  $H \triangleleft G \iff F^H$  нормально над  $P$ . В последнем случае

$$\text{Gal}(F^H/P) \cong G/H.$$

**Доказательство.** Итак, пусть  $G = \text{Gal } F/P$ ,  $H \in \Gamma$ . Так как  $P = F^G$ , то  $P \subset F^H$  и  $K = F^H$  — подполе в  $F$ , содержащее  $P$ . Это даёт отображение  $\Gamma \mapsto \Sigma$ . Применяя теорему 1, Д2) с  $H$  вместо  $G$ , мы видим, что  $\text{Gal } F/F^H = H$ , откуда вытекает первая часть утверждения ii):  $|H| = |\text{Gal } F/F^H| = [F : F^H]$ .

Пусть теперь  $K$  — любое подполе между  $F$  и  $P$ . Положим  $H = \text{Gal } F/K$ . Тогда  $H \subset G = \text{Gal } F/P$ , так что  $H$  — подгруппа в  $G$ .

Ясно также, что  $F$  — поле разложения над  $K$  некоторого сепарабельного многочлена, поскольку оно является таковым над  $P$ . Стало быть, теорема 1, Д1), применённая к паре  $F$  и  $K$ , показывает, что  $K = F^H$ . Мы убедились, что выделенные скобкой  $\{$  в формулировке теоремы отображения биективны.

В начале параграфа отмечалось в качестве очевидного свойства, что если  $H_1 \supset H_2$ , то  $F^{H_1} \subset F^{H_2}$ . Обратно: если  $F^{H_1} \subset F^{H_2}$ , то  $H_1 = \text{Gal } F/F^{H_1} \supset \text{Gal } F/F^{H_2} = H_2$ . Это даёт i).

Первая часть свойства i) отмечалась ранее. Так как

$$|G| = [F : P] = [F : F^H][F^H : P] = |H|[F^H : P]$$

и  $|G| = |H|[G : H]$ , то, очевидно,  $[F^H : P] = [G : H]$ , а это доказывает вторую часть свойства i).

Установим, наконец, справедливость свойства ii). Если  $H \in \Gamma$  и  $K = F^H$  — соответствующее подполе, то подполе  $K'$ , отвечающее сопряжённой подгруппе  $\psi H \psi^{-1}$ , есть  $\psi(K)$  (для наглядности сопрягающие элементы из  $G$  обозначены греческими буквами). Это видно сразу, поскольку условие  $\varphi(x) = x \forall x \in K$  эквивалентно  $(\psi\varphi\psi^{-1})\psi(x) = \psi(x)$ , т.е.  $\psi(x) \in K'$ . Отсюда следует, что

$$H \triangleleft G \iff \psi(K) = K = F^H \quad \forall \psi \in G.$$

Предположим, что  $\psi(K) = K$  для каждого элемента  $\psi \in G$ . В таком случае ограничение  $\bar{\psi} = \psi|_K$  является автоморфизмом поля  $K$  над  $P$ , и мы пришли к гомоморфизму ограничения  $\psi \mapsto \bar{\psi}$  группы  $G = \text{Gal } F/P$  в  $\text{Gal } K/P$ . Образ  $\bar{G}$  является группой автоморфизмов в  $K$  и, очевидно,  $F^{\bar{G}} = P$ . Стало быть,  $\bar{G} = \text{Gal } K/P$ .

Ядром гомоморфизма  $\psi \mapsto \bar{\psi}$  служит множество таких  $\psi \in G$ , что  $\psi|_K = 1_K$ . Соответствие Галуа даёт, что этим множеством является  $\text{Gal } F/K = H$ . Следовательно,  $\bar{G} = \text{Gal } K/P \cong G/H$ .

Так как  $P = F^{\bar{G}}$ , то по теореме 1, 3)  $K$  нормально над  $P$ . Обратно, предположив, что поле  $K$  нормально над  $P$ , рассмотрим минимальный многочлен  $f_a$  над  $P$  любого элемента  $a \in K$ . Тогда  $f(X) = (X - a_1)(X - a_2) \dots (X - a_m)$  в  $K[X]$ , где  $a_1 = a$ . Если  $\varphi \in G$ , то  $f(\varphi(a)) = 0$ , откуда  $\varphi(a) = a_i$  для некоторого  $i$ . Таким образом,  $\varphi(a) \in K$  и  $\varphi(K) \subset K$ . Как и ранее, это означает, что  $\varphi H \varphi^{-1} \subset H$  для каждой подгруппы  $H$ , отвечающей  $K$  в соответствии Галуа. Значит,  $H \triangleleft G$ . Это завершает доказательство iii).  $\square$

**3. Иллюстрации к соответствию Галуа.** Поле  $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ , а также конечные поля  $\mathbb{F}_q$ , рассмотренные в первых двух параграфах, служили прелюдией к теории Галуа. Расширим иллюстративный материал.

**A) Круговое поле  $\Gamma_n$ .** Рассмотрим нормальное расширение  $\Gamma_n = \mathbb{Q}(\zeta)$ ,  $\zeta^n = 1$ , связанное с круговым многочленом  $\Phi_n(X)$  (см. § 2)

степени  $\varphi(n)$ , корнями которого являются все примитивные корни из 1 степени  $n$  и только они. Убедимся прежде всего в том, что справедлива

**Теорема 3.** Круговой многочлен  $\Phi_n(X)$  неприводим над  $\mathbb{Q}$  и, таким образом,  $[\Gamma_n : \mathbb{Q}] = \varphi(n)$ .

**Доказательство.** Как нам известно,  $\Phi_n \in \mathbb{Z}[X]$ . Неприводимость в  $\mathbb{Q}[X]$  по лемме Гаусса эквивалентна неприводимости в  $\mathbb{Z}[X]$ . Предположим, что

$$\Phi_n(X) = g(X)h(X),$$

где  $g, h \in \mathbb{Z}[X]$ , причём многочлен  $h(X)$  степени  $\geq 1$  неприводим в  $\mathbb{Z}[X]$  (и в  $\mathbb{Q}[X]$ ). Пусть  $p$  — простое число, не делящее  $n$ , и  $h(\lambda) = 0$ . Так как  $\text{НОД}(p, n) = 1$ , то  $\lambda^p$  — примитивный корень степени  $n$  из 1.

Если  $h(\lambda^p) \neq 0$ , то  $g(\lambda^p) = 0$ . Стало быть,  $\lambda$  — корень многочленов  $g(X^p)$  и  $h(X)$ . Ввиду неприводимости  $h$  имеем  $h(X) | g(X^p)$ , т.е.

$$g(X^p) = h(X)l(X), \quad l \in \mathbb{Z}[X].$$

У нас

$$X^n - 1 = \Phi_n(X)d(X) = d(X)g(X)h(X).$$

Перейдём к сравнениям по  $(\text{mod } p)$ , т.е. будем действовать в  $\mathbb{Z}_p[X]$ :

$$X^n - \bar{1} = \bar{d}(X)\bar{g}(X)\bar{h}(X) \tag{*}$$

$$(f(X) = a_0X^m + a_1X^{m-1} + \dots \in \mathbb{Z}[X] \implies \bar{f}(X) = \bar{a}_0X^m + \bar{a}_1X^{m-1} + \dots \in \mathbb{F}_p[X].)$$

Аналогично,  $\bar{g}(X^p) = \bar{h}(X)\bar{l}(X)$ . Но

$$\bar{f}(X)^p = \bar{a}_0X^{pm} + \bar{a}_1X^{p(m-1)} + \dots = \bar{f}(X^p)$$

для любого  $f \in \mathbb{Z}[X]$ . Таким образом,  $\bar{g}(X)^p = \bar{g}(X^p) = \bar{h}(X)\bar{l}(X)$ , откуда, конечно, следует, что  $\text{НОД}(\bar{g}, \bar{h}) \neq 1$ .

В соответствии с (\*) приходим к заключению, что  $X^n - \bar{1}$  имеет кратные корни в своём поле разложения над  $\mathbb{Z}_p$ . Но это не так, поскольку  $(X^n - \bar{1})' = \bar{n}X^{n-1}$  и  $\bar{n} \neq 0$ , так что  $\text{НОД}(X^n - \bar{1}, (X^n - \bar{1})') = \bar{1}$ . Полученное противоречие показывает, что  $h(\lambda) = 0 \implies h(\lambda^p) = 0$  для каждого простого числа  $p \nmid n$ . Повторение этого рассуждения показывает, что  $\lambda^r$  — корень многочлена  $h(X)$  для любого натурального  $r$ , взаимно простого с  $n$ . Но каждый примитивный корень степени  $n$  из 1 имеет вид  $\lambda^r$ ,  $\text{НОД}(r, n) = 1$ . Стало быть,  $h(X)$  делится на  $X - \lambda'$ , где  $\lambda'$  — любой примитивный корень степени  $n$ . В таком случае  $h(X) = \Phi_n(X)$ , т.е.  $\Phi_n$  неприводим.  $\square$

Пусть  $G = \text{Gal } \Gamma_n / \mathbb{Q}$ . Тогда  $\sigma \in G \implies \sigma(\zeta) = \zeta^m$  для некоторого целого  $m = \tilde{m}(\sigma)$ , причём  $\text{НОД}(\tilde{m}(\sigma), n) = 1$  и  $(\sigma(\zeta))^n = 1$ . Далее,

$$\sigma, \tau \in G \implies (\sigma\tau)(\zeta) = \zeta^{\tilde{m}(\sigma\tau)} = \sigma(\zeta^{\tilde{m}(\tau)}) = \zeta^{\tilde{m}(\sigma)\tilde{m}(\tau)},$$

т.е.  $\tilde{m}(\sigma\tau) = \tilde{m}(\sigma)\tilde{m}(\tau)$ , и, таким образом,  $\tilde{m} : G \longrightarrow U(Z_n)$  — гомоморфизм группы Галуа поля  $\Gamma_n$  в мультиликативную группу  $U(Z_n)$  целых чисел по  $\text{mod } n$ , взаимно простых с  $n$ . Этот гомоморфизм инъективен, поскольку показатель  $\tilde{m}(\sigma)$  однозначно определён по  $\text{mod } n$  автоморфизмом  $\sigma$ , а действие  $\sigma$  на  $\mathbb{Q}(\zeta)$  определено действием на  $\zeta$ . Так как по теореме 3  $[\Gamma_n : \mathbb{Q}] = \varphi(n) = |U(Z_n)|$ , то  $G \cong U(Z_n)$ .

Нами доказана

**Теорема 4.** Круговое поле  $\Gamma_n$  обладает абелевой группой Галуа, изоморфной  $U(Z_n)$ .

Если заменить  $\mathbb{Q}$  на какое-то поле  $P$ , то, вообще говоря, имеется лишь вложение  $G \hookrightarrow U(Z_n)$ , но не изоморфизм. Строение группы  $U(Z_n)$  было исследовано в гл. 4. Заметим дополнительно, что подгруппы в  $G$  нормальны. Каждое подполе в  $\Gamma_n$  также нормально.

**Пример 1.** Круговое поле  $\Gamma_{17} = \mathbb{Q}(\zeta)$ ,  $\zeta^{17} = 1$ , с циклической группой Галуа  $G = \text{Gal } \Gamma_{17}/\mathbb{Q} = \langle \Phi \mid \Phi^{16} = 1 \rangle$ , порождённой отображением  $\Phi : \zeta \mapsto \zeta^3$ , имеет прямое отношение к конструктивным числовым полям [ВА I, гл. 5, § 1]. Выделим следующий ряд подгрупп:

$$G = G_1 = \langle \Phi \rangle \supset G_2 = \langle \Phi^2 \rangle \supset G_3 = \langle \Phi^4 \rangle \supset G_4 = \langle \Phi^8 \rangle \supset G_5 = 1.$$

По теореме 2 соответствие Галуа приводит к возрастающей цепочке подполей:

$$\mathbb{Q} = F_1 \subset F_2 \subset F_3 \subset F_4 \subset F_5 = F = \mathbb{Q}(\zeta),$$

где  $F_i = F^{G_i}$ . По определению  $\Phi(\zeta) = \zeta^3$ ,  $\Phi^i(\zeta) = \zeta^{3^i}$ . Положим  $z_1 = \sum_{i=1}^8 \Phi^{2i}(\zeta)$ . Тогда  $\Phi^2(z_1) = z_1$ ,  $\Phi(z_1) \neq z_1$ , т.е.  $z_1 \in F_2$ ,  $z_1 \notin F_1$ . Так как  $[G : G_2] = 2$ , то  $[F_2 : F_1] = 2$  и  $F_2 = F_1(z_1)$ . Аналогично,  $z_2 = \sum_{i=1}^4 \Phi^{4i}(\zeta)$ ,  $z_3 = \sum_{i=1}^2 \Phi^{8i}(\zeta) = \zeta^{-1} + \zeta$ ,  $F_3 = F_2(z_2)$ ,  $F_4 = F_3(z_3)$ .

Если найти минимальные многочлены комплексных чисел  $z_1, z_2, z_3$  соответственно над  $F_1, F_2, F_3$  и выразить эти числа через корни квадратных уравнений, то станет ясно, что они являются конструктивными. А в таком случае конструктивно и число  $\zeta$ , дающее возможность построить правильный 17-угольник при помощи циркуля и линейки.

Сделаем ещё несколько замечаний о конструктивных числовых полях. Если исходить из заданного поля

$$P = \mathbb{Q}(z_1, \bar{z}_1, \dots, z_m, \bar{z}_m),$$

где  $z_1, \dots, z_m \in \mathbb{C}$ , то  $P$ -конструктивность комплексного числа  $z$  означает, что

$$z \in F = P(u_1, \dots, u_r), \quad u_i^2 \in P(u_1, \dots, u_{i-1}), \quad 1 \leq i \leq r. \quad (1)$$

*Башня (1) квадратичных расширений над  $P$*  имеет, очевидно, степень  $[F : P] = 2^s$ ,  $s \leq r$ . Таким образом, комплексное число  $\lambda$ , обладающее свойством делимости  $[\mathbb{Q}(\lambda) : \mathbb{Q}]$  на нечётное простое число, не может быть конструктивным.

*Правильные  $n$ -угольники.* При простом  $n = p$  построение правильного  $p$ -угольника равносильно построению комплексного числа  $\zeta = \cos 2\pi/p + i \sin 2\pi/p$ ,  $\zeta^{p-1} + \zeta^{p-2} + \dots + 1 = 0$ ,  $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ . Необходимое условие, следовательно, сводится к равенству

$p - 1 = 2^s$  для некоторого натурального числа  $s$ . Как отмечалось в [BA I, гл. 1], таких простых чисел Ферма известно пока всего 5: 3, 5, 17, 257, 65537.

Из выражения для  $[\Gamma_n : \mathbb{Q}] = \varphi(n)$ , приведённого в § 2, видно, что  $\varphi(n) = 2^s$  в том и только том случае, когда все нечётные простые делители числа  $n$  являются простыми числами Ферма и их кратность в разложении равна 1. Это и есть необходимое условие для построения правильного  $n$ -угольника при помощи циркуля и линейки. Условие является также достаточным, но мы на этом не останавливаемся.

В) *Трисекция угла*. Каждый ли угол можно разделить при помощи циркуля и линейки на три равные части? Утверждается, что этого нельзя сделать даже для угла в  $60^\circ$ , т.е. точка  $z = (\cos 20^\circ, \sin 20^\circ)$  не может быть построена, исходя из точек  $z_1 = 0$ ,  $z_2 = 1$ ,  $z_3 = \cos 60^\circ + i \sin 60^\circ = 1/2 + i\sqrt{3}/2$ . Другими словами, надо убедиться в том, что присоединение  $\cos 20^\circ$  к полю  $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(z_1, z_2, z_3, \bar{z}_1, \bar{z}_2, \bar{z}_3)$  (а это — расширение степени 2 над  $\mathbb{Q}$ ) даст расширение степени  $\neq 2^s$  над  $\mathbb{Q}$ .

Действительно, положив  $u = \cos 20^\circ$ , перепишем тригонометрическое тождество  $\cos 3\varphi = 4\cos^3 \varphi - 3\cos \varphi$  при  $\varphi = 20^\circ$  в виде  $4u^3 - 3u - 1/2 = 0$ , или, что то же самое, в виде  $(2u)^3 - 3(2u) - 1 = 0$ . Но многочлен  $X^3 - 3X - 1$  неприводим над  $\mathbb{Q}$ , поэтому  $[\mathbb{Q}(u) : \mathbb{Q}] = 3$ , а это доказывает требуемое утверждение.

Г) *Удвоение куба*. Речь идёт о построении стороны куба, имеющего объём 2, т.е. о конструктивности числа  $\sqrt[3]{2}$ . Отрицательный ответ напрашивается сразу, поскольку многочлен  $X^3 - 2$  неприводим над  $\mathbb{Q}$  и, стало быть,  $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ .

В Б)-Г) речь шла, скорее, не о группах Галуа, а о степенях расширений. Приведём пару примеров, где группу Галуа найти сравнительно несложно.

Пример 2. Пусть  $P$  — несовершенное поле характеристики  $p > 0$ ,  $a \in P \setminus P^p$ . Тогда, как мы знаем,  $X^p - a$  — неприводимый многочлен над  $P$ . Если  $F = P(u)$ ,  $u^p = a$ , то  $[F : P] = p$ . Кроме того,  $X^p - a = (X - u)^p$ , т.е.  $F$  — поле разложения над  $P$  несепарабельного многочлена  $X^p - a$ . Для  $\sigma \in \text{Gal } F/P$  имеем  $(\sigma(u))^p = a$ , так что  $\sigma(u) = u$ . Это значит, что  $\sigma = 1$  и  $\text{Gal } F/P$  — единичная группа.

Пример 3. Пусть  $F = P(t)$ , где  $t$  — трансцендентный элемент над  $P$ . Можно показать, что

$$F = P(u) \iff u = \frac{at + b}{ct + d}, \quad a, b, c, d \in P; \quad ad - bc \neq 0.$$

Отображение  $\sigma : \frac{f(t)}{g(t)} \mapsto \frac{f(u)}{g(u)}$  является элементом группы Галуа  $G = \text{Gal } F/P$  в самом общем виде, поэтому  $G \cong \text{PGL}(2, P)$ .

## УПРАЖНЕНИЯ

**1.** Пусть  $P$  — поле характеристики 0,  $p$  — простое число,  $\zeta$  — примитивный корень степени  $p$  из 1. Показать, что многочлен  $X^p - a \in P[X]$ , не имеющий корней в поле  $P$ , неприводим над  $P(\zeta)$ .

**2.** Найти группы Галуа многочленов: а)  $X^3 - 12X + 8$ ; б)  $X^3 - 2X - 2$ ; в)  $X^3 + X + 1$ ; г)  $X^4 + 4X^2 + 2$ ; д)  $X^4 + 3X^3 - 3X + 3$ .

## § 4. Вычисление группы Галуа

**1. Действие группы  $\text{Gal}(f)$  на корнях многочлена  $f$ .** Группа Галуа может быть отождествлена с группой перестановок корней. Пусть  $f \in P[X]$  — многочлен степени  $\geq 1$  с различными корнями  $\theta_1, \dots, \theta_n$  в поле разложения  $F = P(\theta_1, \dots, \theta_n)$ . Первоначально Э.Галуа рассматривал исключительно группу  $\text{Gal}(f)$  многочлена  $f$  (или уравнения  $f(X) = 0$ ): каждый автоморфизм интерпретировался как элемент симметрической группы  $S_n$ . Лишь гораздо позднее творец теории идеалов Р. Дедекинд заметил, что  $\text{Gal}(f)$  отождествляется с группой Галуа  $\text{Gal } F/P$ . В настоящее время имеются готовые пакеты программ (типа Maple-V) для вычисления на ЭВМ группы Галуа неприводимых многочленов  $f \in \mathbb{Z}[X]$  небольших степеней.

Вообще говоря,  $\text{Gal}(f)$  — собственная подгруппа в  $S_n$ . Обсудим сначала следующий вопрос: какое подполе в  $F \supset P$  отвечает подгруппе  $\text{Gal}(f) \subset A_n$ , где  $A_n$  — знакопеременная группа?

**Теорема 1.** Пусть  $P$  — поле характеристики  $\neq 2$ ,  $f$  — нормализованный многочлен положительной степени в  $P[X]$  с различными корнями  $\theta_i$  в поле разложения  $F \supset P$ . Пусть

$$\Delta(f) = \prod_{i < j} (\theta_i - \theta_j).$$

Тогда подполем в  $F$ , отвечающим  $\text{Gal}(f) \cap A_n$ , является  $P(\Delta(f))$ .

**Доказательство.** Пусть  $\pi \in S_n$ . Посмотрим сначала на кольцо  $P[X_1, \dots, X_n]$ . Его автоморфизм  $\Phi_\pi : X_i \mapsto X_{\pi(i)}$ , оставляющий каждый элемент из  $P$  на месте, продолжается до автоморфизма, обозначаемого также  $\Phi_\pi$ , поля отношений  $P(X_1, \dots, X_n)$ . Понятно, что группа  $G$  всех таких автоморфизмов изоморфна  $S_n$ . Используя соответствие Галуа, нетрудно заметить, что  $F^G = P(s_1, \dots, s_n)$ , где  $s_k$  — элементарная симметрическая функция от  $X_1, \dots, X_n$ . Кстати,  $\text{Gal } P(X_1, \dots, X_n)/P(s_1, \dots, s_n) \cong S_n$ .

Положим  $\Delta_n = \prod_{i < j} (X_i - X_j)$ . Известно и легко проверяется, что  $\Phi_\pi(\Delta_n) = \varepsilon_\pi \Delta_n$ . Если  $\psi : X_i \mapsto \theta_i$  — гомоморфизм  $P[X_1, \dots, X_n]$  в  $F$ , то  $\psi(\Phi_\pi(\Delta_n)) = \pi(\Delta(f)) = \pm \Delta(f)$ , где теперь  $\pi \in \text{Gal}(f) \cap S_n$ .

Следовательно, подгруппа в  $\text{Gal}(f) \cong \text{Gal } F/P$ , оставляющая на месте элементы подполя  $P(\Delta(f)) \subset F$ , есть подгруппа чётных пере-

становок. В силу соответствия Галуа подполем в  $F/P$ , отвечающим  $\text{Gal}(f) \cap A_n$ , будет  $P(\Delta(f)) = F^{\text{Gal}(f) \cap A_n}$ .  $\square$

Из доказательства видно, что  $\pi(\Delta(f)) = \pm\Delta(f)$  для любой перестановки  $\pi \in \text{Gal}(f)$ . Поэтому дискриминант  $D(f) = \Delta(f)^2$  многочлена  $f$  при действии  $\pi$  остаётся неподвижным и, стало быть,  $D(f) \in P$ . Согласно теореме 1 включение  $\text{Gal}(f) \subset A_n$  имеет место в точности тогда, когда  $P(\Delta(f)) = P$ , т.е.  $\Delta(f) \in P$ . Итак, справедливо

**Следствие.** Пусть  $f \in P[X]$  — нормализованный многочлен степени  $n \geq 1$ ,  $D(f) = \prod_{i < j} (\theta_i - \theta_j)^2$  — его дискриминант. Тогда

$$\text{Gal}(f) \subset A_n \iff D(f) — квадрат элемента из P.$$

**Теорема 2** (критерий неприводимости). Пусть корни  $\theta_i$ ,  $i = 1, \dots, n$ , многочлена  $f \in P[X]$  все различны. Тогда неприводимость  $f$  над  $P$  эквивалентна транзитивности  $\text{Gal}(f)$  на  $\{\theta_1, \dots, \theta_n\}$ .

**Доказательство.** По поводу определения транзитивности см. гл. 1. Предположим, что  $f$  неприводим. Из теоремы 3 в § 1 вытекает существование изоморфизма  $P(\theta_i)/P \rightarrow P(\theta_j)/P$ , каковы бы ни были индексы  $i \neq j$ . Так как  $F = P(\theta_1, \dots, \theta_n)$  — поле разложения над  $P(\theta_i)$  и над  $P(\theta_j)$  многочлена  $f(X) = \prod_k (X - \theta_k)$ , то по построению поля разложения этот изоморфизм может быть продолжен до автоморфизма  $\sigma$  расширения  $F \supset P$ . Значит,  $\sigma \in \text{Gal } F/P = \text{Gal}(f)$  и  $\sigma(\theta_i) = \theta_j$ , т.е.  $\text{Gal}(f)$  транзитивна.

Обратно: предположим, что  $\text{Gal}(f)$  транзитивна на корнях. Пусть  $f(X) = g(X)h(X)$  — разложение с неприводимым множителем  $g(X)$  положительной степени. Если  $g(\theta_i) = 0$  для какого-то  $i$ , а  $\theta_j$  — любой другой корень многочлена  $f$  и  $\sigma(\theta_i) = \theta_j$  для некоторого  $\sigma \in \text{Gal}(f)$ , то  $g(\theta_i) = 0 \implies 0 = \sigma(g(\theta_i)) = g(\theta_j)$ . Это показывает, что каждый корень многочлена  $f$  является корнем его множителя  $g$  и, следовательно,  $f = g$  неприводим.  $\square$

**Пример 1.** Как показано в [ВА I, гл. 5, § 2], дискриминантом неполного кубического уравнения  $f(x) = x^3 + ax + b = 0$  служит выражение  $D(f) = -4a^3 - 27b^3$ . Пусть  $f$  не имеет корней в основном поле  $\mathbb{Q}$ , т.е.  $f$  неприводим и сепарабелен. Таковыми являются многочлены  $f_1(X) = X^3 - X - 1$  и  $f_2(X) = X^3 - 3X + 1$  с дискриминантами  $D(f_1) = -23$ ,  $D(f_2) = 81 = 9^2$ . Из теорем 1, 2 следует, что  $\text{Gal}(f_1) \cong S_3$ , а  $\text{Gal}(f_2) \cong A_3$ .

**Пример 2.** Многочлен  $f(X) = x^3 - 2$ , неприводимый над  $\mathbb{Q}$ , имеет вещественный корень  $\alpha = \sqrt[3]{2}$ . Его полем разложения, однако, будет

$$F = \mathbb{Q}(\alpha, \varepsilon) = \langle 1, \alpha, \alpha^2, \varepsilon, \varepsilon\alpha, \varepsilon\alpha^2 \rangle_{\mathbb{Q}} = \mathbb{Q}(\theta).$$

Здесь

$$\varepsilon^2 + \varepsilon + 1 = 0, \quad \theta = \alpha + \varepsilon, \quad g(\theta) = 0, \quad g(X) = X^6 + 3X^5 + 6X^4 + 3X^3 + 9X + 9.$$

Строение группы Галуа довольно очевидно:

$$G = \text{Gal } F/\mathbb{Q} = \langle \sigma, \tau \mid \sigma^3 = e = \tau^2, \tau\sigma\tau = \sigma^2 \rangle \cong S_3,$$

где

$$\sigma(\varepsilon) = \varepsilon, \quad \sigma(\alpha) = \varepsilon\alpha, \quad \sigma(\varepsilon\alpha) = \varepsilon^2\alpha; \quad \tau(\alpha) = \alpha, \quad \tau(\varepsilon) = \varepsilon^2.$$

Под каждой подгруппой  $H \subseteq G$  выпишем отвечающее ей в силу соответствия Галуа неподвижное подполе:

$G$	$\langle \sigma \rangle$	$\langle \tau \rangle$	$\langle \sigma\tau \rangle$	$\langle \sigma^2\tau \rangle$	$\{e\}$
$\mathbb{Q}$	$\mathbb{Q}(\varepsilon)$	$\mathbb{Q}(\alpha)$	$\mathbb{Q}(\varepsilon^2\alpha)$	$\mathbb{Q}(\varepsilon\alpha)$	$F$

так что  $\langle \sigma \rangle = \text{Gal } F/\mathbb{Q}(\varepsilon)$ ,  $\langle \tau \rangle = \text{Gal } F/\mathbb{Q}(\alpha)$ ,  $\langle \sigma\tau \rangle = \text{Gal } F/\mathbb{Q}(\varepsilon^2\alpha)$ ,  $\langle \sigma^2\tau \rangle = \text{Gal } F/\mathbb{Q}(\varepsilon\alpha)$ . Так как  $\langle \sigma \rangle \triangleleft G$ , то  $\mathbb{Q}(\varepsilon)$  нормально над  $\mathbb{Q}$  и  $\text{Gal } \mathbb{Q}(\varepsilon)/\mathbb{Q} \cong G/\langle \sigma \rangle \cong Z_2$ .

**2. Многочлены и группы простой степени.** В общем вычисление группы Галуа конкретного многочлена  $f \in P[X]$  — довольно трудная задача даже при  $P = \mathbb{Q}$ . Она привлекала внимание крупных математиков. Отметим два результата И. Шура (1931 г.):

$$f(X) = \sum_{m=0}^n X^m/m! \implies \text{Gal}(f) = \begin{cases} A_n, & \text{если } n \equiv 0 \pmod{4}; \\ S_n, & \text{если } n \not\equiv 0 \pmod{4}. \end{cases}$$

Пусть  $H_n(X)$  —  $n$ -й многочлен Эрмита (см. [ВА II]). Положим  $H_{2n}(X) = K_n^{(0)}(X^2)$ ,  $H_{2n+1}(X) = XK_n^{(1)}(X^2)$ . Тогда при  $n > 12$  имеет место изоморфизм  $\text{Gal}(K_n^{(j)}(X)) \cong S_n$ ,  $j = 0, 1$ . Основным полем является  $\mathbb{Q}$ .

Симметрические группы в дальнейшем будут возникать неоднократно, поэтому приведём относящиеся к ним два простых утверждения, развивающие упр. 10 из [ВА I, гл. 4, § 3].

**Предложение 1.** *Транзитивная группа перестановок степени  $n$ , содержащая один двойной цикл и один цикл длины  $n - 1$ , является симметрической.*

**Доказательство.** Пусть  $(12\dots n-1)$  — данный  $(n-1)$ -циклический перестановки. Транспозицию  $(ij)$  в силу транзитивности группы можно перевести в  $(kn)$ , где  $k$  — один из символов от 1 до  $n-1$ . Сопряжение  $(kn)$  при помощи цикла  $(12\dots n-1)$  и его степеней даёт транспозиции  $(1n)$ ,  $(2n)$ ,  $\dots$ ,  $(n-1, n)$ , а они порождают  $S_n$ .  $\square$

**Предложение 2.** *Пусть  $p$  — простое число. Если  $G \subseteq S_p$ , причём  $G$  содержит элемент порядка  $p$  и какую-то транспозицию, то  $G = S_p$ .*

**Доказательство.** По условию  $G$  содержит  $p$ -циклическую перестановку  $\sigma = (i_1 i_2 \dots i_p)$ , где  $\{i_1, i_2, \dots, i_p\} = \{1, 2, \dots, p\}$ . При надлежащем упорядочении считаем, что  $(12) \in G$ . Так как  $\sigma^s = (12\dots)$  при некотором  $s$ , то считаем с самого начала  $\sigma = (12\dots p)$ ,  $(12) \in G$ . Тогда  $G$  содержит  $\sigma(12)\sigma^{-1} = (23)$ ,  $\sigma(23)\sigma^{-1} = (34)$ ,  $\dots$ ,  $\sigma(p-2, p-1)\sigma^{-1} = (p-1, p)$ . Но  $\langle (12), (23), \dots, (p-1, p) \rangle = S_p$ .  $\square$

**Теорема 3.** Пусть  $f$  — неприводимый многочлен простой степени  $p$  над  $\mathbb{Q}$ . Предположим, что  $f$  имеет в точности два невещественных корня в  $\mathbb{C}$ . Тогда  $\text{Gal}(f) = S_p$ .

**Доказательство.** Положим

$$f(X) = \prod_{i=1}^p (X - \theta_i), \quad F = \mathbb{Q}(\theta_1, \dots, \theta_p) \subset \mathbb{C}.$$

Так как

$$F \supset \mathbb{Q}(\theta_1), \quad [\mathbb{Q}(\theta_1) : \mathbb{Q}] = \deg f = p,$$

то степень  $|\text{Gal}(f)| = [F : \mathbb{Q}]$  делится на  $p$ . По теореме Силова (см. гл. 2, § 2)  $\text{Gal}(f)$  содержит элемент порядка  $p$ . Автоморфизм сопряжения  $z \mapsto \bar{z}$  поля  $\mathbb{C}$ , продолженный на  $\mathbb{C}[X]$ , переводит  $f$  в себя. Следовательно, он переставляет корни  $\theta_i$  многочлена  $f$ .

Пусть  $\theta_1, \theta_2$  — невещественные корни. Тогда по условию теоремы  $\theta_2 = \bar{\theta}_1$  и  $\bar{\theta}_i = \theta_i$  при  $i > 2$ . Приходим к выводу, что ограничение автоморфизма сопряжения на  $F$  является элементом в  $\text{Gal}(f)$ , а именно транспозицией. Стало быть,  $\text{Gal}(f)$  содержит элемент порядка  $p$  и транспозицию. Остаётся применить предложение 2.  $\square$

**Теорема 4** (Р. Брауэр). Для любого простого числа  $p$  можно построить сколь угодно много неприводимых многочленов степени  $p$  с группой Галуа  $S_p$ .

**Доказательство.** Пусть  $m; n_1, \dots, n_{k-2}$  — целые чётные числа,  $m$  положительно,  $n_1 < n_2 < \dots < n_{k-2}$  и  $k > 3$  нечётно. Рассмотрим многочлен

$$g(X) = (X^2 + m)(X - n_1)(X - n_2) \dots (X - n_{k-2})$$

с вещественными корнями  $n_1, n_2, \dots, n_{k-2}$ .

График  $y = g(x)$  имеет  $(k-3)/2$  относительных максимумов, а так как  $|g(h)| > 2$  для любого нечётного целого  $h$ , то ясно, что значения этих относительных максимумов будут  $> 2$ . Это означает, что график  $y = f(x) = g(x) - 2$  имеет  $(k-3)/2$  положительных относительных максимумов между  $n_1$  и  $n_{k-2}$ . Следовательно,  $f(X)$  имеет  $k-3$  вещественных корней на интервале  $(n_1, n_{k-2})$ . Так как  $f(n_{k-2}) = -2$  и  $f(N) > M$  при любом  $M > 0$  для достаточно большого натурального  $N$ , то существует также вещественный корень  $> n_{k-2}$ . Получаем  $k-2$  вещественных корня многочлена  $f(X)$ . Если

$$f(X) = \prod_{i=1}^k (X - \theta_i) = (X^2 + m)(X - n_1) \dots (X - n_{k-2}) - 2,$$

то, сравнивая коэффициенты, будем иметь

$$\sum_{i=1}^k \theta_i = \sum_{l=1}^{k-2} n_l, \quad \sum_{i < j} \theta_i \theta_j = \sum_{l < q} n_l n_q + m.$$

Следовательно,

$$\sum_i \theta_i^2 = \left( \sum_i \theta_i \right)^2 - 2 \sum_{i < j} \theta_i \theta_j = \sum_l n_l^2 - 2m.$$

Если выбрать  $m$  достаточно большим, то  $\sum_i \theta_i^2 < 0$ , что означает существование невещественных корней. В случае  $\theta_1 \notin \mathbb{R}$  будет  $\bar{\theta}_1 \neq \theta_1$ , и мы имеем по крайней мере два невещественных корня, а по построению этих корней должно быть ровно 2. Заметим теперь, что

$$f(X) = X^k + a_1 X^{k-1} + \dots + a_k, \quad a_i \in 2\mathbb{Z}.$$

Так как постоянный член у  $g(X)$  делится на 4, то у  $f(X)$  он делится на 2, но не делится на 4. Из критерия Эйзенштейна, применённого к  $f$  с простым числом 2, следует, что  $f$  неприводим над  $\mathbb{Q}$ . Таким образом, условия теоремы 2 удовлетворяются для каждого простого  $p = k \geq 5$ . При  $p = 2$  и  $p = 3$  см. примеры.  $\square$

**3. Метод приведения по модулю  $p$ .** Важным вспомогательным средством для вычисления  $\text{Gal}(f)$ ,  $f \in \mathbb{Z}[X]$ , служит приведение (редукция) по модулю  $p$ , где  $p$  будет пробегать различные простые числа. Редукция коэффициентов многочлена  $f$  приводит к каноническому гомоморфизму  $\mathbb{Z}[X] \rightarrow Z_p[X]$ . Пишем  $f_p(X)$  для образа многочлена  $f(X)$  при этом гомоморфизме. Так как дискриминант  $D(f)$  — полиномиальная функция (от коэффициентов  $f$ ) с коэффициентами из  $\mathbb{Z}$ , то  $D(f) \in \mathbb{Z}$  и  $D(f_p) = D(f)_p$ . Если  $D(f_p) \neq 0$ , то  $D(f) \neq 0$  и оба многочлена  $f$ ,  $f_p$  (одинаковой степени) имеют различные корни. В этом случае справедлива

**Теорема 5** (Р. Дедекинда). *Пусть  $f \in \mathbb{Z}[X]$  — нормализованный многочлен степени  $n$ ,  $p$  — простое число,  $D(f_p) \neq 0$ . Пусть  $f_p(X)$  разлагается в произведение неприводимых над  $Z_p$  множителей степеней  $n_1, n_2, \dots, n_r$  ( $\sum_i n_i = n$ ).*

*Тогда группа Галуа  $\text{Gal}(f)$  содержит перестановку на множестве корней многочлена  $f$  с цикловой структурой*

$$(1, 2, \dots, n_1)(n_1 + 1, \dots, n_1 + n_2)(n_1 + n_2 + 1, \dots, n_1 + n_2 + n_3) \dots$$

*при надлежащем упорядочении корней.*

Доказательству этой важной теоремы будут предшествовать несколько вспомогательных утверждений. Начнём с классического результата о линейной независимости характеров. Пусть  $H$  — моноид,  $K$  — поле. Под *характером*  $\chi$  из  $H$  в  $K$  (или под  *$K$ -характером* моноида  $H$ ) понимается гомоморфизм  $H \rightarrow K^*$  ( $\chi(1) = 1$ ,  $\chi(ab) = \chi(a)\chi(b)$ ).

**Лемма 1** (лемма Дедекинда–Артина о независимости). *Различные характеристики  $\chi_1, \chi_2, \dots, \chi_n$  моноида  $H$  в поле  $K$  линейно незави-*

симы над  $K$ , т.е.

$$\sum_i a_i \chi_i(h) = 0, \quad a_i \in K, \quad \forall h \in H \implies a_i = 0, \quad 1 \leq i \leq n.$$

**Доказательство** проводим индукцией по  $n$ . Если  $n = 1$ , то результат очевиден, поскольку  $a\chi(h) = 0$ ,  $a \neq 0$ , означает  $\chi(h) = 0$  для любого  $h \in H$ , в то время как по условию  $\chi(1) = 1$ .

Пусть теперь  $n > 1$ , и пусть для  $n - 1$  независимость установлена. Считаем все  $a_i \neq 0$ , иначе действует предположение индукции. Так как  $\chi_1 \neq \chi_2$ , то  $\chi_1(h') \neq \chi_2(h')$  для некоторого  $h' \in H$ . Заменим в предполагаемом соотношении линейной зависимости  $h$  на  $h'h$ . Это приводит к соотношению

$$a_1 \chi_1(h') \chi(h) + a_2 \chi_2(h') \chi_2(h) + \dots + a_n \chi_n(h') \chi_n(h) = 0.$$

С другой стороны, умножая исходное соотношение на  $\chi_1(h')$ , будем иметь

$$a_1 \chi_1(h') \chi(h) + a_2 \chi_1(h') \chi_2(h) + \dots + a_n \chi_1(h') \chi_n(h) = 0.$$

Вычитая последнее соотношение из первого, получим

$$a'_2 \chi_2(h) + \dots + a'_n \chi_n(h) = 0,$$

где

$$a'_i = a_i (\chi_i(h') - \chi_1(h')), \quad 2 \leq i \leq n.$$

Так как  $f'_2 = a_2(\chi_2(h') - \chi_1(h')) \neq 0$ , то имеем противоречие с предположением индукции.  $\square$

**Следствие 1.** Пусть  $K_1, K_2$  — два поля и  $\eta_1, \dots, \eta_n$  — различные мономорфизмы  $K_1 \rightarrow K_2$ . Тогда они линейно независимы над  $K_2$ .

**Доказательство.** Ограничить  $\eta_i$  на  $K_1^*$  и положить  $H = K_1^*$ .  $\square$

**Следствие 2** (теорема Артина). Пусть  $G$  — конечная группа автоморфизмов поля  $F$ . Тогда  $F$  является расширением Галуа над своим подполем  $P$  неподвижных относительно  $G$  элементов и  $\text{Gal } F/P = G$ .  $\square$

Основу доказательства теоремы 5 составляет

**Лемма 2.** Пусть  $f \in \mathbb{Z}[X]$  — нормализованный многочлен степени  $n$ ,  $F$  — его поле разложения над  $\mathbb{Q}$ ,  $p$  — простое число такое, что  $D(f_p) \neq 0$ , т.е.  $f_p$  имеет различные корни в своём поле разложения  $F_{(p)}$  над  $Z_p$ . Пусть  $L$  — подкольцо в  $F$ , порождённое корнями многочлена  $f$ .

Тогда:

- а) существует гомоморфизм  $\psi: L \rightarrow F_{(p)}$ ;
- б) любой такой гомоморфизм устанавливает биекцию множества  $R$  корней многочлена  $f$  в  $F$  на множество  $R_p$  корней  $f_p$  в  $F_{(p)}$ ;

в) если  $\psi, \psi'$  — два таких гомоморфизма, то  $\psi' = \psi \cdot \sigma$ , где  $\sigma \in \text{Gal } F/\mathbb{Q}$ .

Доказательство. По условию

$$F = \mathbb{Q}(\theta_1, \dots, \theta_n), \quad f(X) = \prod_{i=1}^n (X - \theta_i) \text{ в } F[X].$$

По определению  $L = \mathbb{Z}[\theta_1, \dots, \theta_n]$ . Положим

$$L' = \sum_{0 \leq k_i \leq n-1} \mathbb{Z} \theta_1^{k_1} \dots \theta_n^{k_n}$$

— множество  $\mathbb{Z}$ -линейных комбинаций элементов

$$\theta^{k_1} \dots \theta^{k_n}, \quad 0 \leq k_i \leq n-1.$$

Так как  $f(\theta_i) = 0$ , то  $\theta_i^n$  —  $\mathbb{Z}$ -линейная комбинация степеней  $1, \theta_i, \theta_i^2, \dots, \theta_i^{n-1}$ . Следовательно,  $\theta_i L' \subset L'$  и по итерации  $\theta_1^{k_1} \dots \theta_n^{k_n} L' \subset L'$  для любых положительных показателей  $k_1, \dots, k_n$ . Значит,  $L'$  — подкольцо в  $L$ , содержащее по определению  $\theta_1, \dots, \theta_n$  и, таким образом, совпадающее с  $L$ .

Это показывает, что  $L$  — конечно порождённый  $\mathbb{Z}$ -модуль. Так как  $\text{char } F = 0$ , то кручение  $\text{Tor } L$  равно нулю и  $L$  — свободный  $\mathbb{Z}$ -модуль конечного ранга с каким-то базисом  $(u_1, \dots, u_m)$ :  $L = \mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_m$ .

Утверждается, что  $(u_i)$  — базис для расширения  $F/\mathbb{Q}$  и, следовательно,  $[F : \mathbb{Q}] = m$ . Линейная независимость над  $\mathbb{Q}$  элементов  $u_i$  очевидна, поскольку нетривиальное  $\mathbb{Q}$ -линейное соотношение между  $u_i$  приводит (при умножении на некоторое целое число) к нетривиальному  $\mathbb{Z}$ -линейному соотношению, которое на самом деле отсутствует. Рассмотрим теперь  $\mathbb{Q}L = \sum_i \mathbb{Q}u_i$  — подкольцо в  $F$ , содержащее  $\mathbb{Q}$ . Из алгебраичности  $F$  следует, что  $\mathbb{Q}L$  — подполе в  $F$  (см. следствие теоремы 2 из § 1). Так как оно содержит все  $\theta_i$ ,  $1 \leq i \leq n$ , то  $\mathbb{Q}L = F$ . Стало быть,  $(u_i)$  — базис для  $F/\mathbb{Q}$ .

Введём в рассмотрение идеал  $pL = \sum_{i=1}^m \mathbb{Z}(pu_i)$  кольца  $L$ . Ясно, что  $|L/pL| = p^m$ . Так как факторкольцо  $L/pL$  конечно, то оно заведомо содержит максимальный собственный идеал вида  $M/pL$ , где  $M$  — максимальный идеал в  $L$ , содержащий  $pL$ . В таком случае  $L/M$  — поле, являющееся гомоморфным образом кольца  $L/pL$ , поскольку по одной из теорем об изоморфизме (см. гл. 4) имеем  $(L/pL)/(M/pL) \cong L/M$ . Из построения видно, что  $\text{char } L/M = p$  и  $Z_p$  — простое подполе в  $L/M$ , а  $|L/M| = p^{m'}$ , где  $m' \leq m$ .

а) Канонический гомоморфизм  $\nu: L \rightarrow L/M$  отображает  $\mathbb{Z}$  на простое поле  $Z_p$  (или, если угодно,  $\mathbb{F}_p$ ), а так как  $L = \mathbb{Z}[\theta_1, \dots, \theta_n]$  и  $f(X) = \prod_{i=1}^n (X - \theta_i)$  в  $L[X]$ , то  $L/M = Z_p[\bar{\theta}_1, \dots, \bar{\theta}_n]$ , где  $\bar{\theta}_i = \nu(\theta_i) = \theta_i + M$ . Далее, из  $f \in \mathbb{Z}[X]$  следует, что коэффициенты многочлена  $\bar{f}(X) = \prod_{i=1}^n (X - \bar{\theta}_i)$  лежат в  $Z_p$  и  $\bar{f}(X) = f_p(X)$ . Таким образом,

$L/M$  — поле разложения для  $f_p(X)$  над  $Z_p$ , и мы имеем изоморфизм  $\mu : L/M \rightarrow F_{(p)}$ . В итоге мы пришли к нужному эпиморфизму  $\psi = \mu \circ \nu : L \rightarrow F_{(p)}$ .

б) Пусть  $\psi$  — гомоморфизм типа, установленного в а). Тогда ограничение  $\psi|_{\mathbb{Z}}$  будет гомоморфизмом  $\mathbb{Z}$  на простое подполе в  $F_{(p)}$ ,  $\psi(1) = 1_{F_{(p)}}$ , так что  $\psi|_{\mathbb{Z}}$  — канонический гомоморфизм  $\mathbb{Z}$  на  $Z_p$ . В таком случае  $f_p(X) = \psi(f(X)) := \prod_i (X - \psi(\theta_i))$ . Следовательно,  $\psi(\theta_i)$  — корни многочлена  $f_p(X)$  в  $F_{(p)}$  и  $\psi|_R$  — биекция  $R$  на  $R_p$ .

в) Зафиксируем гомоморфизм  $\psi : L \rightarrow F_{(p)}$ . Пусть  $\sigma \in G = \text{Gal } F/\mathbb{Q}$ . Тогда  $\sigma$  переставляет  $\theta_i$  и, следовательно,  $\sigma$  переводит  $L$  в себя. Далее,  $\sigma|_L$  — гомоморфизм  $L$  в  $L$  (на самом деле автоморфизм), а  $\psi \circ \sigma$  — гомоморфизм  $L$  в  $F_{(p)}$ . Различные  $\sigma, \sigma' \in G$  дают различные перестановки корней  $\theta_i$ , а поскольку  $\psi|_R$  — биекция на  $R_p$ ,  $\psi \circ \sigma$  и  $\psi \circ \sigma'$  различны. Таким способом мы получаем  $m = [F : \mathbb{Q}]$  различных гомоморфизмов  $\psi_j = \psi \circ \sigma_j$ , если  $G = \{\sigma_1, \dots, \sigma_m\}$ .

Утверждается, что других гомоморфизмов больше нет. Действительно, пусть  $\psi_{m+1}$  отличен от  $\psi_j$ ,  $1 \leq j \leq m$ . По лемме 1, применённой к мультиликативному моноиду  $H$  области  $L$  и полю  $K = F_{(p)}$ , все  $\psi_j$ , включая  $\psi_{m+1}$ , линейно независимы над  $F_{(p)}$ . С другой стороны, рассмотрим систему уравнений

$$\sum_{i=1}^{m+1} x_i \psi_i(u_j) = 0, \quad 1 \leq j \leq m.$$

Так как неизвестных  $x_i$  больше, чем уравнений, то эта однородная линейная система с коэффициентами  $\psi_i(u_j) \in F_{(p)}$  имеет нетривиальное решение  $(a_1, \dots, a_{m+1})$ ,  $a_i \in F_{(p)}$ . Пусть теперь  $y \in L$ . Тогда  $y = \sum_j n_j u_j$ ,  $n_j \in \mathbb{Z}$ , и

$$\psi_i(y) = \sum_j \bar{n}_j \psi_i(u_j), \quad \bar{n}_j = n_j + p\mathbb{Z};$$

$$\sum_i a_i \psi_i(y) = \sum_j \bar{n}_j \left( \sum_i a_i \psi_i(u_j) \right) = \sum_j \bar{n}_j(0) = 0.$$

Это противоречит независимости  $\psi_i$  и завершает доказательство в).  $\square$

Наконец, мы готовы дать

**Доказательство теоремы 5.** Так как  $F_{(p)}$  — поле с  $p^m$  элементами, то отображение  $\pi : a \mapsto a^p$ ,  $a \in F_{(p)}$  — автоморфизм. Если  $\psi : L \rightarrow F_{(p)}$  — любой гомоморфизм, то и  $\pi \circ \psi$  — гомоморфизм. Соответственно мы имеем единственный элемент  $\sigma = \sigma(\psi) \in \text{Gal}(f)$ , такой, что

$$\pi \circ \psi = \psi \circ \sigma(\psi).$$

Автоморфизм  $\sigma = \sigma(\psi)$  называется *p-автоморфизмом Фробениуса* на  $F/\mathbb{Q}$ , отвечающим  $\psi$ .

Если мы ограничим  $\psi$  и  $\sigma$  на  $R$  и используем тот факт, что  $\psi$  — биекция из  $R$  на  $R_p$ , то получим соотношение  $\sigma = \psi^{-1} \circ \pi \circ \psi$ . Это означает, что орбиты на  $R_p$  относительно  $\langle \pi \rangle$  отображаются посредством  $\psi^{-1}$  в орбиты на  $R$  относительно  $\langle \sigma \rangle$ .

Но орбиты на  $R_p$  относительно  $\langle \pi \rangle$  — это множества корней неприводимых множителей многочлена  $f_p \in Z_p[X]$ . Если  $n_1, \dots, n_r$  — степени этих многочленов, то мощности орбит на  $R$  относительно  $\langle \sigma \rangle$  будут  $n_1, \dots, n_r$ , и, следовательно,  $\sigma$  как перестановка на  $R$  имеет цикловое разложение

$$(12 \dots n_1)(n_1 + 1, \dots, n_1 + n_2) \dots$$

при надлежащем упорядочении корней.  $\square$

Пример 3. Пусть  $f(X) = X^6 + 22X^5 + 21X^4 + 12X^3 - 37X^2 - 29X - 15$ . Сначала используем редукцию по  $\text{mod } 2$ , чтобы получить

$$f_2(X) = X^6 + X^4 + X^2 + X + 1.$$

Делимости на неприводимые многочлены  $X^2 + X + 1$ ,  $X^3 + X^2 + 1$ ,  $X^3 + X + 1$  степени  $\leqslant 3$  нет, поэтому  $f_2(X)$  неприводим. Следовательно,  $\text{Gal}(f)$  содержит 6-цикл, так что  $\text{Gal}(f)$  транзитивна. Далее,

$$f_3(X) = X(X^5 + X^4 - X + 1),$$

причём  $X^5 + X^4 - X + 1$  неприводим по  $\text{mod } 3$ . Стало быть,  $\text{Gal}(f)$  содержит 5-цикл. Наконец,

$$f_5(X) = X(X - 1)(X + 1)(X + 2)(X^2 + 2)$$

и  $X^2 + 2$  неприводим по  $\text{mod } 5$ . Следовательно,  $\text{Gal}(f)$  содержит 2-цикл. В соответствии с предложением 1 приходим к заключению, что  $\text{Gal}(f) \cong S_6$ .

Чтобы на основании теоремы 5 построить многочлен  $f \in \mathbb{Z}[X]$  степени  $n > 3$  с  $\text{Gal}(f) \cong S_n$ , выберем сначала неприводимый по  $\text{mod } 2$  многочлен  $u \in \mathbb{Z}[X]$  степени  $n$ ; затем — многочлен  $v \in \mathbb{Z}[X]$ , который по  $\text{mod } 3$  разлагается в произведение неприводимого множителя степени  $n - 1$  и линейного множителя; наконец, выберем многочлен  $w \in \mathbb{Z}[X]$ , который по  $\text{mod } 5$  разлагается в произведение неприводимого множителя степени 2 и одного или нескольких неприводимых множителей нечётных степеней. Всё это возможно, поскольку по модулю любого простого числа существует неприводимый многочлен любой наперёд заданной степени.

В заключение выберем многочлен  $f$  так, чтобы выполнялись условия

$$f \equiv u \pmod{2}, \quad f \equiv v \pmod{3}, \quad f \equiv w \pmod{5}.$$

Достаточно положить

$$f = -15u + 10v + 6w$$

(все многочлены нормализованы).

Группа  $\text{Gal}(f)$  будет тогда транзитивной (неприводимость  $f$  по  $\text{mod } 2$ ), будет содержать цикл типа  $(1, 2, \dots, n - 1)$  и транспозицию, умноженную на независимые циклы нечётной длины. Если это последнее произведение возвести в подходящим образом подобранную нечётную степень, то получится чистая транспозиция. В силу предложения 1 получаем  $\text{Gal}(f) \cong S_n$ .

Упомянутые в самом начале п. 2 результаты И. Шура, относящиеся к конкретным многочленам с группой Галуа, изоморфной  $S_n$ , не обесценивают теорему 5. Основанные на ней вычисления применяются в самых разных ситуациях.

**4. Нормальный базис.** Пусть  $F$  — произвольное расширение Галуа над  $P$  с  $\text{Gal } F/P = G = \{\eta_i \mid 1 \leq i \leq n\}$ ,  $n = [F : P]$ . Если  $z \in F$  и  $\{z_1, z_2, \dots, z_m\} = Gz$  — орбита при действии  $G$ , то минимальным многочленом для  $z$  над  $P$  будет  $\prod_1^m (X - z_i)$ . Следовательно,  $z$  будет примитивным элементом ровно тогда, когда  $m = |Gz| = n$ . Более сильное свойство: элементы  $\eta_1(z), \eta_2(z), \dots, \eta_n(z)$  не только различны, но и линейно независимы над  $P$ . Если это так, то  $(\eta_1(z), \dots, \eta_n(z))$  — базис для  $F/P$ . Он называется *нормальным базисом* данного расширения. Доказательство существования нормального базиса основано на следующем критерии.

**Предложение 3.** Пусть  $K/P$  — конечномерное сепарабельное расширение,  $L/P$  — его нормальное замыкание. Тогда:

- 1) число мономорфизмов  $K/P \rightarrow L/P$  равно  $n = [K : P]$ ;
- 2) если  $1 = \eta_1, \eta_2, \dots, \eta_n$  — эти мономорфизмы, то набор  $(u_1, u_2, \dots, u_n)$ ,  $u_i \in K$ , является базисом для  $K/P$  в том и только том случае, когда

$$\begin{vmatrix} u_1 & u_2 & \dots & u_n \\ \eta_2(u_1) & \eta_2(u_2) & \dots & \eta_2(u_n) \\ \dots & \dots & \dots & \dots \\ \eta_n(u_1) & \eta_n(u_2) & \dots & \eta_n(u_n) \end{vmatrix} \neq 0.$$

**Доказательство.** 1) Пусть  $G = \text{Gal } L/P$ , и пусть  $H \subset G$  — подгруппа, фиксирующая  $K$ . Тогда  $n = [K : P] = (G : H)$ , и мы можем написать  $G = \theta_1 H \cup \dots \cup \theta_n H$ ;  $\theta_1 = 1$  — разложение в левые смежные классы. Положим  $\eta_i = \theta_i|_K$ . Тогда  $\eta_i$  — мономорфное вложение  $K/P \hookrightarrow L/P$  и  $\eta_i \neq \eta_j$  при  $i \neq j$ . Действительно, если  $\eta_i = \eta_j$ , то  $\theta_i^{-1}(\theta_j(u)) = u \quad \forall u \in K$ . В таком случае  $\theta_i^{-1}\theta_j \in H$ , вопреки предположению.

Пусть теперь  $\eta$  — любой мономорфизм  $K/P \hookrightarrow L/P$ . Так как  $L$  — поле разложения над  $P$  некоторого многочлена  $f \in P[X]$ , то  $L$  будет полем разложения того же многочлена над  $K$  и над  $\eta(K)$ . Следовательно (по теореме об изоморфизмах полей разложения), изоморфизм

$\eta : K \rightarrow \eta(K)$  может быть продолжен до автоморфизма  $\theta$  расширения  $L/P$ . Другими словами,  $\theta \in \text{Gal } L/P$  и, стало быть,  $\theta = \theta_i \mu$  для некоторого  $\mu \in H$ . Но тогда  $\eta = \theta|_K = \theta_i|_K = \eta_i$ , т.е  $\eta_1 = 1, \dots, \eta_n$  — полный комплект мономорфизмов  $K/P \hookrightarrow L/P$ .

2) Предположив линейную зависимость  $\sum_i a_i u_i = 0$ ,  $a_i \in P$ , элементов  $u_1, \dots, u_n \in K$  и применяя  $\eta_j$ , мы получаем линейную однородную систему

$$\sum_{i=1}^n a_i \eta_j(u_i) = 0, \quad 1 \leq j \leq n,$$

порядка  $n$  с ненулевым решением  $(a_1, \dots, a_n)$ , что означает  $\det(\eta_j(u_i)) = 0$ .

Обратно: предположим, что  $\det(\eta_j(u_i)) = 0$ . В таком случае существует ненулевое решение  $(a_1, \dots, a_n)$ ,  $a_i \in L$ , однородной системы  $\sum_j \eta_j(u_i)x_j = 0$ ,  $1 \leq i \leq n$ , а это означает, что  $(u_1, \dots, u_n)$  базисом для  $K$  не является: если любой элемент  $u \in K$  записывается в виде  $\sum_i c_i u_i$ ,  $c_i \in P$ , и

$$\sum_j a_j \eta_j(u) = \sum_{i,j} a_j c_i \eta_j(u_i) = \sum_i \left( \sum_j a_j \eta_j(u_i) \right) = 0,$$

то это противоречит независимости мономорфизмов  $\eta_1, \dots, \eta_n$  (следствие 1 леммы Дедекинда–Артина).  $\square$

*Предложение 4.* *Расширение Галуа  $L/P$  с конечным  $P$  обладает нормальным базисом.*

*Доказательство.* В случае конечного поля  $P$  расширение  $L/P$  будет циклическим и

$$G = \text{Gal } L/P = \langle \sigma \rangle = \{1, \sigma, \sigma^2, \dots, \sigma^{m-1}\},$$

где  $m = [L : P]$ . Интерпретируем  $\sigma$  как линейный оператор в  $L$  над  $P$ , поскольку

$$\sigma(u + v) = \sigma(u) + \sigma(v), \quad \sigma(au) = a\sigma(u), \quad a \in P.$$

Известно, что  $P[X]$ -модуль, определённый линейным оператором, является прямой суммой циклических подпространств с аннуляторами — инвариантными множителями  $d_1(X), \dots, d_s(X)$ , где  $d_s(X)$  — минимальный многочлен линейного оператора (произведение всех инвариантных множителей суть характеристический многочлен). Весь  $P[X]$ -модуль является циклическим в точности тогда, когда характеристический многочлен совпадает с минимальным, т.е. степень минимального многочлена совпадает с размерностью всего пространства.

Именно так обстоит дело в случае с  $\sigma$ . Так как  $\sigma^m = 1$ , то  $X^m - 1$  — характеристический многочлен. С другой стороны,

если

$$f(X) = X^k + a_1 X^{k-1} + \dots + a_k, \quad a_i \in P, \quad k < m,$$

то  $f(\sigma) \neq 0$ , поскольку автоморфизмы  $1, \sigma, \dots, \sigma^k$  различны, следовательно, линейно независимы над  $L$  и, тем более, над  $P$ .

Тот факт, что  $L$  циклическое (как  $P[X]$ -модуль), означает, что  $L/P$  имеет базис вида  $(u, \sigma(u), \dots, \sigma^{m-1}(u))$ . Но это и есть нормальный базис для  $L/P$ .  $\square$

**Определение.** Пусть  $K, L$  — два поля. Семейство  $\eta_1, \eta_2, \dots, \eta_n$  мономорфизмов  $K \hookrightarrow L$  называется *алгебраически независимым над  $L$* , если

$$f \in L[X_1, \dots, X_n], \quad f(\eta_1(u), \dots, \eta_n(u)) = 0 \quad \forall u \in K \implies f = 0.$$

**Предложение 5.** Пусть  $P$  — бесконечное поле,  $K$  — конечно-мерное сепарабельное расширение над  $P$ ,  $L$  — нормальное замыкание расширения  $K/P$ . Пусть  $\eta_1, \dots, \eta_n = n = [K : P]$  различных мономорфизмов  $K/P \hookrightarrow L/P$ . Тогда  $\eta_i$  алгебраически независимы над  $L$ .

**Доказательство.** Предположим, что  $f(\eta_1(u), \dots, \eta_n(u)) = 0 \quad \forall u \in K$  для некоторого  $f \in f \in L[X_1, \dots, X_n]$ . Пусть  $(u_i)$  — базис для  $K/P$ . Тогда при любом выборе  $a_i \in P$  имеем

$$\begin{aligned} 0 = f\left(\eta_1\left(\sum_i a_i u_i\right), \dots, \eta_n\left(\sum_i a_i u_i\right)\right) &= \\ &= f\left(\sum_i a_i \eta_1(u_i), \dots, \sum_i a_i \eta_n(u_i)\right). \end{aligned}$$

Если положить

$$g(X_1, \dots, X_n) = f\left(\sum \eta_1(u_i) X_i, \dots, \sum \eta_n(u_i) X_i\right),$$

то  $g(a_1, \dots, a_n) = 0$  при любых  $a_i \in P$ . Пусть  $(v_1, v_2, \dots, v_m)$  — базис для  $L/P$ . Тогда можно написать

$$g(X_1, \dots, X_n) = \sum_{j=1}^m g_j(X_1, \dots, X_n) v_j,$$

где  $g_j(X_1, \dots, X_n) \in P[X_1, \dots, X_n]$ . Условие  $g(a_1, \dots, a_n) = 0$  выражается в виде  $g_j(a_1, \dots, a_n) = 0 \quad \forall j$ . Поскольку это справедливо при всех  $a_i \in P$ , из соответствия между полиномиальными функциями и многочленами над бесконечным полем вытекает, что  $g_j(X_1, \dots, X_n) = 0$ , и, стало быть,  $g(X_1, \dots, X_n) = 0$ .

В силу предложения 3  $\det(\eta_j(u_i)) \neq 0$ , так что матрица  $(\eta_j(u_i))$  имеет обратную  $(v_{ij}) \in M_n(L)$ . Значит,

$$g\left(\sum_{j,k} v_{1j} \eta_j(u_k) X_k, \dots, \sum_{j,k} v_{nj} \eta_j(u_k) X_k\right) = f(X_1, \dots, X_n).$$

Поэтому  $g(X_1, \dots, X_n) = 0 \implies f(X_1, \dots, X_n) = 0$ , что и доказывает алгебраическую независимость  $\eta_i$  над  $L$ .  $\square$

Мы подошли к центральному результату.

**Теорема 6.** *Любое конечномерное расширение Галуа  $L/P$  имеет нормальный базис.*

**Доказательство.** В силу предложения 4 поле  $P$  можно считать бесконечным. Как показывает предложение 5, автоморфизмы  $\eta_1, \dots, \eta_n$  расширения  $L/P$  алгебраически независимы над  $L$ .

Мы видели также, что если  $u \in L$ , то

$$(\eta_1(u), \dots, \eta_n(u)) — базис \iff \det((\eta_i \eta_j)(u)) \neq 0.$$

Положим  $\eta_i \eta_j = \eta_{i(j)}$ . Тогда  $j \mapsto i(j)$  — перестановка на  $\{1, 2, \dots, n\}$ . Рассмотрим теперь алгебру многочленов  $L[X_1, \dots, X_n]$  и матрицу  $X = (x_{i(j)})$ . Утверждается, что  $\det X \neq 0$ . С этой целью выберем специализацию  $x_1 = 1, x_i = 0, i > 1$ . Так как перестановки  $j \mapsto i(j)$  при различных  $i$  различны, то  $x_1$  появляется один и только один раз в каждой строке и в каждом столбце матрицы  $X$ . Следовательно,  $\det X(x_1 = 1, x_i = 0, i > 1) = \pm 1$ . Тем более  $\det X \neq 0$  при любом  $X$ .

В силу алгебраической независимости  $\eta_i$  над  $L$  найдётся  $u \in L$ , для которого  $\det((\eta_i \eta_j)(u)) \neq 0$ . В таком случае  $(\eta_1(u), \dots, \eta_n(u))$  — нормальный базис.  $\square$

На языке теории представлений теорема о нормальном базисе утверждает, что представление группы Галуа на аддитивной группе поля  $L$  (на векторном пространстве) является регулярным. Можно также сказать, что  $L$  — свободный модуль размерности 1 над групповым кольцом  $P[G]$ . Такой результат можно рассматривать как первый шаг в гораздо более тонких исследованиях в алгебраической теории чисел. Именно, пусть  $L$  — числовое поле (конечное расширение поля  $\mathbb{Q}$ ) и  $O_L$  — кольцо в  $L$  целых алгебраических чисел. Строение  $O_L$  как  $\mathbb{Z}[G]$ -модуля — трудная задача.

Казалось бы, теорема о нормальном базисе обесценивает теоретико-групповую часть теории Галуа: регулярное представление не очень интересно. Но надо иметь в виду также мультиплекативную структуру поля и то обстоятельство, что группа Галуа реализуется как группа перестановок корней исходного многочлена, а это действие может обладать свойствами примитивности, кратной транзитивности и т.д.

### УПРАЖНЕНИЯ

**1.** Найти нормальный базис расширения  $\mathbb{F}_8/\mathbb{F}_2$ . Для определённости считаем  $\mathbb{F}_8 = \mathbb{F}_2(\theta)$ ,  $\theta^3 + \theta + 1 = 0$ .

**2.** Найти нормальный базис расширения  $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ .

## § 5. Расширения Галуа и смежные вопросы

**1. Простые числа в арифметической прогрессии.** Из определения круговых многочленов в § 2 мы получим сейчас два простых утверждения, оформленных в виде лемм.

*Лемма 1. Пусть  $a \neq 0$  — целое число,  $n$  — натуральное число, не делящееся на простое число  $p$ . Тогда*

$$p \mid \Phi_n(a) \iff \{a \text{ имеет период } n \text{ в } Z_p^*\}$$

(эквивалентно:  $a^n \equiv 1 \pmod{p}$ ,  $a^m \not\equiv 1 \pmod{p} \quad \forall m < n$ ).

*Доказательство.* Рассматриваем разложение

$$X^n - 1 = \Phi_n(X) \prod_{d|n, d < n} \Phi_d(X) \in Z_p^*[X]. \quad (*)$$

1) Если  $\Phi_n(a) = 0$  в  $Z_p$ , то согласно (\*) имеем  $a^n - 1 = 0$  в  $Z_p$ . Если, кроме того,  $\Phi_m(a) = 0$  для некоторого  $m | n$ ,  $m < n$ , то  $X^n - 1 = (X - a)^2 f(X)$ . Но производная  $(X^n - 1)' = nX^{n-1}$  взаимно проста с  $X^n - 1$ , поскольку  $n \neq 0$  в  $Z_p$ . Поэтому  $X^n - 1$  не имеет кратных корней. Это означает также, что  $a$  не может быть корнем многочлена  $X^m - 1$ ,  $m < n$ ,  $m | n$ , поскольку  $X^m - 1 = \prod_{d|m, d < n} \Phi_d(X)$ . Значит,  $a$  имеет период  $n$ .

2) Пусть теперь, обратно,  $a$  имеет период  $n$  в  $Z_p^*$ . Если  $\Phi_d(a) = 0$  для некоторого  $d | n$ ,  $d < n$ , то, как мы уже видели в 1),  $a^d \equiv 1 \pmod{p}$  — противоречие. Остается единственная возможность  $\Phi_n(a) = 0$ , (т.е.  $p \mid \Phi_n(a)$ ).  $\square$

*Лемма 2. Пусть  $n \in \mathbb{Z}$ ,  $p$  — простое число, не делящее  $n$ . Тогда*

$$\Phi_n(a) \equiv 0 \pmod{p} \text{ для некоторого } a \in \mathbb{Z} \iff p \equiv 1 \pmod{n}.$$

*Доказательство.* По лемме 1  $\Phi_n(a) \equiv 0 \pmod{p} \iff a^n \equiv 1 \pmod{p}$ , причём  $n$  — период элемента  $a$ . Но тогда  $n \leq p - 1$ , поскольку всегда  $a^{p-1} \equiv 1 \pmod{p}$ , и  $n | (p - 1)$ , т.е.  $p \equiv 1 \pmod{n}$ .

Обратно: если  $p \equiv 1 \pmod{n}$ , то в силу цикличности  $Z_p^*$  найдётся  $a \in \mathbb{Z}$  периода  $n$  в  $Z_p^*$ . Снова по лемме 1 имеем  $\Phi_n(a) \equiv 0 \pmod{p}$ .  $\square$

**Теорема 1** (частный случай теоремы Дирихле). *В арифметической прогрессии  $kn + 1$ ,  $k = 1, 2, \dots$ , существует бесконечно много простых чисел.*

*Доказательство.* Действительно, при любом фиксированном  $n > 1$  имеем

$$\Phi_n(a) = a^m + \alpha_1 a^{m-1} + \dots + \alpha_{m-1} a + 1, \quad m = \varphi(n).$$

Предположим, что существует лишь конечное множество  $M = \{p_1, p_2, \dots, p_s\}$  простых чисел таких, что  $\Phi_n(a) \equiv 0 \pmod{p_i}$ ,  $i = i(a)$ ,

для всех достаточно больших натуральных чисел  $a$ . Однако для  $a = (p_1 p_2 \dots p_s)^N$ ,  $N >> 0$ , будет  $\Phi_n(a) \equiv 1 \pmod{p_i}$ ,  $1 \leq i \leq s$ , — противоречие.

Стало быть, существует бесконечно много простых чисел  $p$  таких, что  $\Phi_n(a) \equiv 0 \pmod{p}$  при подходящем выборе натурального числа  $a = a_p$ . По лемме 2 получаем  $p \equiv 1 \pmod{n}$  для каждого такого простого  $p$ .  $\square$

**2. Расширения с абелевой группой Галуа.** Говорят о циклических, абелевых, разрешимых расширениях, когда соответствующие группы Галуа циклические, абелевы или разрешимые. Конечных абелевых групп данного порядка, в общем, довольно много, поэтому интересно посмотреть на них с точки зрения теории Галуа.

Теорема 2. Пусть  $A$  — произвольная конечная абелева группа. Тогда существует нормальное расширение  $F/\mathbb{Q}$  с группой Галуа

$$\text{Gal } F/\mathbb{Q} \cong A.$$

Доказательство. По основной теореме о строении конечных абелевых групп (гл. 2, § 3, теорема 10)

$$A = A_1 \times A_2 \times \dots \times A_k,$$

где  $A_j = \langle u_j \rangle$  — циклическая группа порядка  $m_j$ ,  $1 \leq j \leq k$ , причём  $m_1 | m_2, \dots, m_{k-1} | m_k$ . Целые числа  $m_j$  называются *инвариантными множителями* группы  $A$ . Очевидно,

$$|A| = m_1 m_2 \dots m_k.$$

По теореме 1 найдутся попарно различные простые числа

$$p_1, p_2, \dots, p_k \quad (p_i \neq p_j, \text{ даже если } m_i = m_j)$$

такие, что

$$p_j - 1 = n_j m_j.$$

Рассмотрим круговое поле  $\Gamma_n = \mathbb{Q}(\zeta)$ ,  $\zeta^n = 1$ , отвечающее целому числу  $n = p_1 p_2 \dots p_k$ , так что

$$\begin{aligned} [\Gamma_n : \mathbb{Q}] &= \varphi(n) = \varphi(p_1) \varphi(p_2) \dots \varphi(p_k) = \\ &= (p_1 - 1)(p_2 - 1) \dots (p_k - 1) = n_1 m_1 n_2 m_2 \dots n_k m_k. \end{aligned}$$

Заметим, что если  $F_1$ ,  $F_2$  — два под поля в поле  $F$ , то наименее поле, содержащее  $F_1$  и  $F_2$ , обозначается  $F_1 \cdot F_2$  и называется *композитом* полей  $F_1$ ,  $F_2$ . Далее,

$$\Gamma_s \cap \Gamma_t = \mathbb{Q} \text{ при НОД}(s, t) = 1 \text{ и } \Gamma_s \Gamma_t = \Gamma_{st}.$$

В нашем случае

$$\Gamma_n = \Gamma_{p_1} \cdot \Gamma_{p_2} \dots \Gamma_{p_k},$$

где

$$\Gamma_{p_j} = \mathbb{Q}(\zeta_j), \quad \zeta_j = \zeta^{p_1 \dots p_j \dots p_k}, \quad \zeta_j^{p_j} = 1.$$

Теперь очевидно, что

$$\left\{ \text{Gal } \Gamma_{p_j}/\mathbb{Q} \right\} \cap \left\{ \prod_{i \neq j} \text{Gal } \Gamma_{p_i}/\mathbb{Q} \right\} = \langle 1 \rangle.$$

Поэтому

$$\text{Gal } \Gamma_n/\mathbb{Q} = \text{Gal } \Gamma_{p_1}/\mathbb{Q} \times \dots \times \text{Gal } \Gamma_{p_k}/\mathbb{Q} = \langle \sigma_1 \rangle \times \dots \times \langle \sigma_k \rangle := G,$$

$$\begin{aligned} \sigma_j: \zeta_j &\mapsto \zeta_j^{a_j}, \quad \langle a_j \rangle = Z_{p_j}^*, \quad |\langle \sigma_j \rangle| = n_j m_j; \\ \sigma_j: \zeta_i &\mapsto \zeta_i, \quad i \neq j. \end{aligned}$$

В группе  $G$  содержится подгруппа

$$H = \langle \sigma_1^{m_1} \rangle \times \dots \times \langle \sigma_k^{m_k} \rangle$$

порядка  $n_1 \dots n_k$ . Понятно, что  $H \triangleleft G$  и факторгруппа

$$G/H = \langle \bar{\sigma}_1 \rangle \times \dots \times \langle \bar{\sigma}_k \rangle, \quad \bar{\sigma}_j = \sigma_j \langle \sigma_j^{m_j} \rangle,$$

являющаяся прямым произведением циклических групп порядков  $m_1, m_2, \dots, m_k$ , изоморфна  $A$ . Если теперь  $F = \Gamma_n^H$  — подполе  $H$ -инвариантов (неподвижных при действии  $H$  элементов) в  $\Gamma_n$ , то в силу соответствия Галуа

$$\text{Gal } F/\mathbb{Q} \cong G/H \cong A. \quad \square$$

**3. Норма и след.** Пусть  $F/P$  — расширение Галуа,

$$G = \text{Gal } F/P = \langle \eta_1 = 1, \eta_2, \dots, \eta_n \rangle.$$

Для  $u \in F$  положим

$$T_P^F(u) = \sum_{i=1}^n \eta_i(u), \quad N_P^F(u) = \prod_{i=1}^n \eta_i(u)$$

и назовём их соответственно *следом* и *нормой* элемента  $u$  в  $F/P$ . Очевидно, они неподвижны относительно  $G$ , следовательно, содержатся в  $P$ . Таким образом, мы имеем отображения

$$T_P^F: u \mapsto T_P^F(u), \quad N_P^F: u \mapsto N_P^F(u)$$

из  $F$  в  $P$ . Для  $u, v \in F$ ,  $a \in P$  имеем

$$T_P^F(u+v) = \sum_i \eta_i(u+v) = \sum_i \eta_i(u) + \sum_i \eta_i(v) = T_P^F(u) + T_P^F(v),$$

$$T_P^F(au) = \sum_i \eta_i(au) = a \sum_i \eta_i(u) = a \cdot T_P^F,$$

$$N_P^F(uv) = \prod_i \eta_i(uv) = \prod_i \eta_i(u) \prod_i \eta_i(v) = N_P^F(u) \cdot N_P^F(v),$$

$$N_P^F(au) = \prod_i \eta_i(au) = a^n \prod_i \eta_i(u) = a^n \cdot N_P^F(u).$$

Итак,  $T = T_P^F$  — линейная функция на векторном пространстве  $F$  над  $P$ ;  $N = N_P^F$  — мультиликативное однородное отображение степени  $n$ ;  $N|_{F^*}$  — гомоморфизм из  $F^*$  в  $P^*$ .

Пример 1. Пусть  $m$  — целое число, свободное от квадратов,  $F = \mathbb{Q}(\sqrt{m})$  — квадратичное поле. Тогда  $u = a + b\sqrt{m}$ ,  $a, b \in \mathbb{Q}$ , — общий вид элементов из  $F$  и

$$G = \text{Gal } F/P = \{1, \eta : a + b\sqrt{m} \mapsto a - b\sqrt{m}\},$$

т.е.  $T(a + b\sqrt{m}) = 2a$ ,  $N(a + b\sqrt{m}) = a^2 - mb^2$ . Имеем полную аналогию с расширением  $\mathbb{C}/\mathbb{R}$ ,  $m = -1$ , когда  $N(u) = a^2 + b^2$  — квадрат модуля комплексного числа.

В нашем случае, очевидно,  $T(F) = \mathbb{Q}$ . Информацию о  $N(F^*)$  получить гораздо труднее, поскольку возникает нетривиальный вопрос: для каких рациональных чисел  $r$  уравнение  $x^2 - my^2 = r$  имеет решения в  $\mathbb{Q}$ ?

Имеются две теоремы о  $\text{Ker } N$  и  $\text{Ker } T$ . Наиболее известная из них следующая.

Теорема 3 (теорема 90 Д. Гильберта, 1897 г.). Пусть  $F$  — циклическое расширение Галуа поля  $P$ ,  $G = \text{Gal } F/P = \langle \eta \rangle$ ,  $|G| = n$ . Тогда

$$N_P^F(u) = 1 \text{ для } u \in F \iff u = v(\eta(v))^{-1} \text{ для некоторого } v \in F.$$

В одну сторону результат тривиален: если  $u = v(\eta(v))^{-1}$ , то  $N(u) = N(v) \cdot N(\eta(v)^{-1}) = N(v) \cdot N(v)^{-1} = 1$ . Чтобы доказать обратное, мы установим более общий (и более поздний) результат о расширениях Галуа.

Теорема 4 (А. Шпайзера). Пусть  $F$  — конечномерное расширение Галуа поля  $P$ ,  $G = \text{Gal } F/P$ . Пусть  $\zeta \mapsto u_\zeta$  — отображение  $G$  в  $F^*$ , удовлетворяющее условию

$$u_{\zeta\mu} = \zeta(u_\mu)u_\zeta \quad \forall \mu, \zeta \in G.$$

Тогда найдётся  $0 \neq v \in F$ , для которого

$$u_\mu = v(\mu(v))^{-1} \quad \forall \mu \in G.$$

Доказательство. Так как  $u_\mu \neq 0$ , а автоморфизмы  $\mu \in G$  линейно независимы над  $F$ , то существует элемент  $w \in F$ , для которого

$$v = \sum_{\mu \in G} u_\mu \mu(w) \neq 0.$$

Тогда при любом  $\zeta \in G$  имеем

$$\begin{aligned} \zeta(v) &= \sum_{\mu} \zeta(u_\mu)(\zeta\mu)(w) = \sum_{\mu} u_{\zeta\mu} u_\zeta^{-1} (\zeta\mu)(w) = \\ &= \left( \sum_{\mu} u_{\zeta\mu} (\zeta\mu)(w) \right) u_\zeta^{-1} = \left( \sum_{\mu} u_\mu \mu(w) \right) u_\zeta^{-1} = vu_\zeta^{-1}. \end{aligned}$$

Следовательно,  $u_\zeta = v(\zeta(v))^{-1}$ .  $\square$

**Доказательство теоремы Гильберта.** Пусть  $u \in F$ ,  $N(u) = 1$ . Положим

$$u_\eta := u, \quad u_{\eta^i} := u\eta(u)\eta^2(u)\dots\eta^{i-1}(u), \quad 1 \leq i \leq n.$$

Тогда при  $i + j \leq n$  будем иметь

$$u_{\eta^j} \cdot \eta^j(u_{\eta^i}) = u\eta(u)\dots\eta^{j-1}\eta^j(u)\dots\eta^{i+j-1}(u) = u_{\eta^{i+j}}.$$

То же соотношение имеет место при  $i + j > n$ , поскольку  $u_1 = u_{\eta^n} = N(u) = 1$ . Таким образом, выполнено условие теоремы 4 при  $G = \langle \eta \rangle$ . Отсюда вытекает существование элемента  $v$  с нужным свойством  $u = u_\eta = v(\eta(v))^{-1}$ .  $\square$

Доказанные теоремы имеют аддитивные аналоги.

**Теорема 5** (А. Шпайзера). *Пусть  $F, P, G$  — те же, что и в мультипликативной теореме 4, и пусть  $\mu \mapsto d_\mu$  — отображение  $G \rightarrow F$ , удовлетворяющее условию*

$$d_{\zeta\mu} = d_\zeta + \zeta(d_\mu) \quad \forall \zeta, \mu \in G.$$

Тогда найдётся  $c \in F$ , для которого

$$d_\mu = c - \mu(c), \quad \mu \in G.$$

**Доказательство.** Мы видели, что существует  $u \in F$  с  $T(u) \neq 0$ . Положим

$$c = T(u)^{-1} \sum_\mu d_\mu \mu(u).$$

Тогда

$$\begin{aligned} c - \zeta(c) &= T(u)^{-1} \sum_\mu [d_\mu \mu(u) - \zeta(d_\mu) \cdot \zeta \mu(u)] = \\ &= T(u)^{-1} \sum_\mu [d_\mu \mu(u) + d_\zeta \cdot \zeta \mu(u) - d_{\zeta\mu} \cdot \zeta \mu(u)] = \\ &= T(u)^{-1} d_\zeta \sum_\mu \zeta \mu(u) = d_\zeta T(u)^{-1} \sum_\sigma \sigma(u) = d_\zeta T(u)^{-1} T(u) = d_\zeta. \end{aligned}$$

Элемент  $\zeta \in G$  произвольный.  $\square$

Пусть теперь  $G = \langle \eta \rangle$ ,  $|G| = n$ , и предположим, что  $d \in F$  — элемент, для которого  $T(d) = 0$ . Положим

$$d_\eta := d, \quad d_{\eta^i} := d + \eta(d) + \dots + \eta^{i-1}(d), \quad 1 \leq i \leq n.$$

Тогда, как и в случае норм, для теоремы Гильберта имеет место заключение аддитивной теоремы Шпайзера. Действительно,

$$d_1 = d_{\eta^n} = d + \eta(d) + \dots + \eta^{n-1}(d) = T(d) = 0.$$

Поэтому для любых  $i, j$  имеем

$$\begin{aligned} d_{\eta^i \eta^j} &= d_{\eta^{i+j}} = d + \eta(d) + \dots + \eta^{i-1} + \eta^i [d + \eta(d) + \dots + \eta^{j-1}(d)] = \\ &= d_{\eta^i} + \eta^i(d_{\eta^j}), \end{aligned}$$

т.е.  $d_{\zeta\mu} = d_\zeta + \zeta(d_\mu)$   $\forall \zeta, \mu \in G$  и согласно теореме 5  $d_\mu = c - \mu(c)$ ,  $\mu \in G$ . Стало быть, справедлива

**Теорема 6** (аддитивная форма теоремы 90 Гильберта). *Пусть  $F/P$  — циклическое расширение степени  $n$  с группой  $\text{Gal } F/P = \langle \eta \rangle$ ,  $d \in F$  — элемент со следом 0. Тогда найдётся  $c \in F$  такой, что  $d = c - \eta(c)$ .*

**4. Циклические расширения.** Применим теперь теорему 90 Гильберта и её аддитивный аналог к простейшему типу расширений.

**Теорема 7.** *Пусть  $P$  содержит  $n$  различных корней степени  $n$  из 1. Справедливы следующие утверждения.*

1) *Пусть  $F/P$  —  $n$ -мерное циклическое расширение. Тогда  $F = P(u)$ , где  $u^n \in P$ .*

2) *Пусть  $X^n - a \in P[X]$  и  $u$  — некоторый корень многочлена  $X^n - a$ . Тогда  $P(u)/P$  — циклическое расширение степени  $m$ ,  $m \mid n$  и  $u^m \in P$ .*

**Доказательство.** 1) Из условия теоремы следует, что характеристика поля  $P$  взаимно проста с  $n$ . Пусть  $\zeta \in P$ ,  $\zeta^n = 1$ ,  $\zeta^i \neq 1$ ,  $i < n$ ,  $\eta$  — образующая группы Галуа. По условию имеем  $\eta^i(\zeta) = \zeta$ ,  $0 \leq i \leq n-1$ , так что  $(N_P^F(\zeta)) = \zeta^n = 1$ . Следовательно, по теореме 3 найдётся  $u \in F$ , для которого  $\zeta = u/\eta(u)$ . В таком случае  $\eta(u) = \zeta^{-1}u$  и  $\eta(u^n) = \eta(u)^n = (\zeta^{-1}u)^n = u^n$ , откуда  $u^n = a \in P$ . Кроме того,  $\eta(u) = \zeta^{-1}u \implies \eta^i(u) = \zeta^{-i}u$ , так что  $\text{Gal } F/P$ -орбита элемента  $u$  содержит  $n$  различных элементов. Таким образом, минимальный многочлен элемента  $u$  над  $P$  имеет степень  $n$  и  $F = P(u)$ .

2) Обратно, пусть  $a \in P$ ,  $u^n = a$ ,  $\zeta$  — примитивный корень  $n$ -й степени из 1. Так как  $(\zeta^i u)^n = a$ ,  $i = 0, 1, \dots, n-1$ , то все корни многочлена  $X^n - a$  лежат в  $P(u)$ , т.е.  $P(u)$  нормально над  $P$ .

Положим  $G = \text{Gal } P(u)/P$ . Если  $\eta \in G$ , то  $(\eta(u))^n = a$ , откуда  $\eta(u) = \zeta^{i(\eta)}u$ . Без труда проверяется, что отображение  $\eta \mapsto \zeta^{i(\eta)}$  является инъективным гомоморфизмом  $G$  в группу  $\langle \zeta \rangle$ . Но всякая подгруппа циклической группы циклическая, поэтому  $G$  циклическая, и если  $|G| = m$ , то  $m \mid n$ . Положив  $G = \langle \sigma \rangle$ , мы замечаем, что  $\zeta^{i(\sigma)} = \zeta^{n/m}$  будет примитивным корнем степени  $m$  из 1. Наконец,

$$\sigma(u^m) = (\sigma(u))^m = (\zeta^{n/m}u)^m = u^m,$$

так что  $u^m \in P$ .  $\square$

**Следствие.** *Пусть  $a \neq b^m$ , каковы бы ни были  $m \mid n$ ,  $m \neq 1$ ,  $b \in P$ , и пусть по-прежнему  $\omega^n = 1 \implies \omega \in P$ . Тогда  $G = \text{Gal}(X^n - a)$  — группа порядка  $n$ .*

**Доказательство.** Пусть  $u^n - a = 0$ . Тогда  $\prod_{\eta \in G} \eta(u) \in P$ . Но  $\eta(u) = \zeta^{i(\eta)} u$ , а так как все корни степени  $n$  из 1 лежат в  $P$ , то  $\prod_{\eta \in G} (u) = \omega u^{|G|} \in P \implies u^{|G|} \in P$ . Отсюда  $a = u^n = (u^{|G|})^d$ , где  $d = n/|G|$ . По условию (если положить  $b = u^{|G|}$ ) это возможно только при  $d = 1$ , т.е. при  $|G| = n$ .  $\square$

Фактически мы убедились, что все двучленные уравнения  $X^n - a = 0$ ,  $a \in P$ , при условии  $\zeta \in P$  ( $\zeta^n = 1$ ,  $\zeta^m \neq 1$ ,  $0 < m < n$ ) имеют циклическую группу Галуа. При тех же предположениях верно и обратное утверждение. Более деликатная ситуация затрагивается в следующих двух теоремах.

**Теорема 8.** *Всякое  $p$ -мерное циклическое расширение  $F$  поля  $P$  характеристики  $p > 0$  имеет вид  $F = P(c)$ , где  $c^p - c \in P$ .*

**Доказательство.** Замечая, что  $1 \in P$  и  $T_P^F(1) = [F : P] \cdot 1 = p \cdot 1 = 0$ , воспользуемся теоремой 6:  $\eta(c) = c + 1$  для некоторого  $c \in F$ . В таком случае  $\eta^i(c) = c + i$ , т.е.  $\langle \eta \rangle$ -орбита  $\{c, c + 1, \dots, c + p - 1\}$  состоит из  $p = [F : P]$  элементов. Следовательно,  $F = P(c)$ . Кроме того,

$$\eta(c^p - c) = (\eta(c))^p - \eta(c) = (c + 1)^p - (c + 1) = c^p - c,$$

так что  $c^p - c \in P$ .  $\square$

Этой теореме можно придать более точную форму.

**Теорема 9 (Артин–Шрайер).** *Пусть  $P$  — поле характеристики  $p > 0$ . Тогда справедливы следующие утверждения.*

1) *Если  $F/P$  — циклическое расширение степени  $p$ , то  $F = P(c)$ , где элемент  $c$  удовлетворяет уравнению  $X^p - X - a$  для некоторого  $a \in P$ .*

2) *Обратно: при заданном  $a \in P$  многочлен  $f(X) = X^p - X - a$  либо имеет один корень в  $P$ , и тогда все его корни лежат в  $P$ , либо он неприводим. В последнем случае  $F = P(c)$  — циклическое расширение степени  $p$  над  $P$  для любого корня  $c$ :  $f(c) = 0$ .*

**Доказательство.** Утверждение 1) эквивалентно теореме 8.

Обратно: если  $f(c) = 0$ , то  $f(c+i) = 0$ ,  $i = 1, \dots, p-1$ , т.е. многочлен  $f(X)$  имеет  $p$  различных корней. Если один корень  $c \in P$ , то и  $c+i \in P$ . Предположим теперь, что  $c \notin P$ , и пусть  $f(X) = g(X)h(X)$ ,  $1 \leq \deg g(X) < p$ . Так как

$$f(X) = \prod_{i=0}^{p-1} (X - c - i),$$

то  $g(X)$  — произведение некоторой части линейных множителей. Пусть  $d = \deg g(X)$ . Коэффициент при  $X^{d-1}$  есть  $-\sum_i'(c+i) = -dc + j$ . Но  $d \neq 0$  в  $P$  и, следовательно,  $c \in P$ , поскольку  $g \in P[X]$ , — противоречие.

Таким образом,  $f(X)$  неприводим над  $P$ , а все его корни лежат в  $P(c)$ , так что расширение  $P(c)$  нормально над  $P$ . Поскольку  $f(X)$  не имеет кратных корней,  $P(c)$  — расширение Галуа. Существует автоморфизм  $\sigma$  поля  $P(c)$  над  $P$  такой, что  $\sigma(c) = c + 1$ . Образы  $\sigma^i(c) = c + i$ ,  $i = 0, 1, \dots, p - 1$ , различны и, стало быть, группа Галуа состоит из степеней  $\sigma^i$ , т.е. является циклической.  $\square$

**5. Критерий разрешимости уравнений в радикалах.** Коэффициенты алгебраических уравнений будем предполагать лежащими в поле  $P$  характеристики нуль. Итак, пусть  $f \in P[X]$ .

**Определение.** Говорят, что расширение  $F/P$  *радикально*, если оно обладает башней подполей

$$P = P_0 \subset P_1 \subset P_2 \subset \dots \subset P_{r-1} \subset P_r = F, \quad (1)$$

где

$$P_i = P_{i-1}(u_i), \quad u_i^{n_i} = a_i \in P_{i-1}, \quad 1 \leq i \leq r, \quad n_i \in \mathbb{N},$$

т.е.  $P_i$  получается из  $P_{i-1}$  присоединением некоторого радикала  $\sqrt[n_i]{a_i}$ .

Говорят также, что уравнение  $f(X) = 0$  *разрешимо в радикалах над  $P$* , если существует радикальное расширение типа (1), содержащее все корни многочлена  $f$ .

Заметим, что  $F$  содержит нормальное расширение, а именно поле разложения, но не обязано само быть нормальным. Этот недостаток легко исправляется.

**Теорема 10.** *Каждое радикальное расширение содержится в некотором нормальном радикальном расширении.*

**Доказательство** проводим индукцией по высоте  $r$  башни (1). Если  $r = 1$  и  $F = P(u)$ ,  $u^n = a$ ,  $a \in P$ , а  $\zeta$  — первообразный корень степени  $n$  из 1, то поле разложения  $P(\zeta, u)$  многочлена  $X^n - a$  как раз и будет нормальным радикальным расширением.

Предполагая, что расширение  $P_{r-1} \supset P$  содержится в нормальном радикальном расширении  $K \supset P$  и  $F = P_{r-1}(u)$ ,  $u^n = a \in P_{r-1}$ , рассмотрим минимальный многочлен  $h(X)$  элемента  $a \in P_{r-1}$  над  $P$ . По определению нормальности многочлен  $h(X)$  над полем  $K$  распадается в произведение линейных множителей:

$$h(X) = (X - a_1)(X - a_2) \dots (X - a_m), \quad a_1 = a.$$

Пусть  $L$  — поле разложения над  $P$  многочлена  $h(X^n)$ . Так как пересечение и композит нормальных расширений всегда нормальны, то композит  $K \cdot L = K(\zeta, u_1, \dots, u_m)$ ,  $u_i^n = a_i$ , также нормален.  $\square$

Почти столь же очевидна следующая

**Теорема 11.** *Группа Галуа  $\text{Gal } F/P$  нормального радикального расширения  $F/P$  разрешима.*

**Доказательство.** Без ограничения общности считаем, что  $F$  определено башней (1). Присоединим теперь к полю  $F$  первообразный

корень  $\zeta$  степени

$$n = n_1 n_2 \dots n_{r-1} n_r$$

из 1 и рассмотрим башню

$$P \subset P(\zeta) \subset P_1(\zeta) \subset \dots \subset P_{r-1}(\zeta) \subset P_r(\zeta) = F(\zeta). \quad (2)$$

Группа  $\text{Gal } P(\zeta)/P$  абелева, а остальные последовательные расширения в башне (2) по теореме 7 являются циклическими. В силу соответствия Галуа группа  $G = \text{Gal } F(\zeta)/P$  обладает нормальным рядом

$$G \triangleright G_0 \triangleright G_1 \triangleright \dots \triangleright G_{r-1} \triangleright \{e\},$$

в котором факторгруппа  $G/G_0$  абелева, а остальные последовательные факторгруппы  $G_i/G_{i+1}$  циклические. По теореме 1 из § 2 гл. 2 группа  $G$  должна быть разрешимой. Если  $H = \text{Gal } F(\zeta)/F$ , то  $H \triangleleft G$  (поскольку  $F/P$  — нормальное расширение) и  $\text{Gal } F/P \cong G/H$  — также разрешимая группа.  $\square$

Мы подошли, наконец, к “коронному достижению” Э. Галуа.

**Теорема 12.** *Полиномиальное уравнение  $f(x) = 0$  разрешимо в радикалах тогда и только тогда, когда группа  $\text{Gal}(f)$  разрешима.*

**Доказательство.** 1) Предположим, что все корни  $\lambda_1, \dots, \lambda_m$  многочлена  $f(X)$  (нули уравнения  $f(x) = 0$ ) лежат в нормальном радикальном расширении  $F/P$ . Естественное включение

$$P \subset P(\lambda_1, \dots, \lambda_m) \subset F$$

означает, что группа Галуа уравнения  $f(x) = 0$  является факторгруппой разрешимой (по теореме 11) группы  $\text{Gal } F/P$ . Поэтому она сама разрешима.

2) Пусть  $F$  — поле разложения многочлена  $f \in P[X]$ . Предположим, что группа  $G = \text{Gal } F/P$  разрешима и

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_{k-1} \triangleright G_k = \{e\}$$

— её композиционный ряд. Тогда, как мы знаем, композиционные факторы  $G_i/G_{i+1}$  будут циклическими группами простых порядков. Соответствие Галуа в свою очередь гарантирует существование цепочки подполей

$$P \subset F_1 \subset F_2 \subset \dots \subset F_{k-1} \subset F_k = F,$$

в которой каждое последовательное расширение  $F_{i+1}/F_i$  будет циклическим простой степени.

Присоединим к  $F$  первообразный корень  $\zeta$  степени  $n = |G|$  из 1 и рассмотрим цепочку подполей

$$P \subset P(\zeta) \subset F_1(\zeta) \Longrightarrow_2 (\zeta) \subset \dots \subset F_{k-1}(\zeta) \subset F_k(\zeta) = F(\zeta).$$

Каждое расширение  $F_{i+1}(\zeta)/F_i(\zeta)$  также будет циклическим простой степени  $p_i$ , делящей  $n$ . По теореме 7 поле  $F_{i+1}(\zeta)$  получается присоединением к  $F_i(\zeta)$  корня некоторого двучленного уравнения  $x^{p_i} - a = 0$ ,  $a \in F_i(\zeta)$ . Это и означает, что  $F(\zeta)$  — радикальное расширение

поля  $P$ , содержащее все корни многочлена  $f(X)$ , т.е. полиномиальное уравнение  $f(x) = 0$  разрешимо в радикалах.  $\square$

Выше были приведены примеры нормализованных многочленов  $f \in \mathbb{Z}[X]$  любой степени  $n$  с симметрической группой Галуа. По только что доказанной теореме 12 соответствующие уравнения  $f(x) = 0$  неразрешимы в радикалах.

Предположим теперь, что корни многочлена  $f \in P[X]$ ,  $P \in \mathbb{R}$ , вещественны. Можно ли их получить, присоединяя к  $P$  вещественные значения радикалов из вещественных чисел? Уточним постановку вопроса.

**Определение.** Пусть  $L$  — поле разложения многочлена  $f \in P[X]$ ,  $P \subset L \subset \mathbb{R}$ . Говорят, что уравнение  $f(x) = 0$  разрешимо в вещественных радикалах, если существует поле  $F$ ,  $P \subset L \subset F \subset \mathbb{R}$ , с цепочкой подполей

$$P = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_{m-1} \subset F_m = F, \quad F_{i+1} = F_i(\sqrt[p]{a_i}), \quad (3)$$

где  $a_i \in F_i$  и  $\sqrt[p]{a_i}$  — вещественное значение радикала. Поле  $L$  в этом случае называется вещественным радикальным расширением поля  $P$ .

**Теорема 13.** Конечное нормальное расширение  $L/P$ ,  $P \subset L \subset \mathbb{R}$  будет вещественным радикальным в точности тогда, когда его группа Галуа является 2-группой.

**Доказательство.** 1) Любая конечная 2-группа  $G$  разрешима (см. упр. 2 из § 1 гл. 2). Если теперь  $G = \text{Gal } L/P$  и

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_{n-1} \triangleright G_n = e$$

её композиционный ряд, то  $|G_i/G_{i+1}| = 2$ . Соответствие Галуа даст нам цепочку подполей

$$P = L_0 \subset L_1 \subset L_2 \subset \dots \subset L_{n-1} \subset L_n = L \quad (4)$$

с циклическими степенями 2 последовательными расширениями

$$L_{i+1} = L_i(\sqrt{a_i}), \quad a_i \in L_i.$$

Это и означает, что  $L/P$  — вещественное радикальное расширение.

2) Будем исходить теперь из нормального вещественного радикального расширения  $L/P$ ,  $P \subset L \subset F \subset \mathbb{R}$ , где поле  $F$  обладает цепочкой подполей вида (3) с простыми числами  $p_i$ .

Группа Галуа  $G = \text{Gal } L/P$  разрешима, поэтому в цепочке подполей вида (4), отвечающей какому-то композиционному ряду группы  $G$ , последовательные расширения  $L_{i+1}/L_i$  будут циклическими простых степеней. Без ограничения общности можно считать, что  $L/P$  — циклическое расширение простой степени  $q$  и что  $L \not\subset F_{m-1}$  (в противном случае можно было бы заменить  $F$  на  $F_{m-1}$ ). Тогда композит  $L \cdot F_{m-1}$  является циклическим расширением степени  $q$  над  $F_{m-1}$ . Заменяя  $P$  на  $F_{m-1}$  и  $L$  на  $L \cdot F_{m-1}$  (а потом возвращаясь к прежним

обозначениям), мы редуцируем задачу к случаю, когда

$$P \subset L \subset P(\sqrt[p]{a}) \subset \mathbb{R}, \quad a \in P,$$

и  $L/P$  — циклическое расширение простой степени  $q$ . Подразумевается, что  $\sqrt[p]{a}$  — вещественное значение радикала простой степени  $p$ . В рассматриваемой ситуации ни один из корней многочлена  $X^p - a$  не лежит в поле  $P \subset \mathbb{R}$ . Но известно (см. упр. 1 из § 3), что многочлен  $X^p - a$ , не имеющий корней в поле  $P$ , неприводим над  $P(\zeta)$ ,  $\zeta^p = 1$ . Стало быть,  $[P(\sqrt[p]{a}) : P] = p$ , что возможно лишь при  $q = p$ , и  $L = P(\sqrt[p]{a})$  — расширение Галуа. В таком случае неприводимый многочлен  $X^p - a \in P[X]$  распадается в  $P(\sqrt[p]{a}) \subset \mathbb{R}$  на линейные множители. Так как при нечётном  $p$  не все корни многочлена вещественные, то приходим к выводу, что  $p = 2$ .  $\square$

### УПРАЖНЕНИЯ

**1.** Разрешимо ли в радикалах уравнение

$$x^6 + 2x^5 - 5x^4 + 9x^3 - 5x^2 + 2x + 1 = 0?$$

**2.** Пусть  $\zeta$  — примитивный корень степени 5 из 1,  $a, b \in \mathbb{Q}$ ,  $\alpha_i$  — нули уравнения

$$x^5 - 5ax^3 + 5a^2x - 2b = 0.$$

Показать, что

$$\alpha_i = \zeta^i \sqrt[5]{b + \sqrt{b^2 - a^5}} + \zeta^{5-i} \sqrt[5]{b - \sqrt{b^2 - a^5}}, \quad 0 \leq i \leq 4.$$

**3.** Показать, что если все три корня неприводимого над полем  $P \subset \mathbb{R}$  многочлена  $X^3 + pX + q$  вещественны, то их нельзя выразить посредством вещественных радикалов.

**4.** Ряд утверждений из пп. 3–4 можно доказать, используя понятие *резольвенты Лагранжа*  $\mathcal{L}(u)$  элемента  $u$ . Именно, если  $F = P(u)$  — циклическое расширение степени  $n$  поля  $P$ , содержащего примитивный корень  $\zeta$  степени  $n$  из 1, и если  $\text{Gal } F/P = \langle \sigma \rangle$ ,  $v \in F$ , то по определению

$$\mathcal{L}(v) = u + \zeta^{-1}\sigma(v) + \zeta^{-2}\sigma^2(v) + \dots + \zeta^{-(n-1)}\sigma^{n-1}(v).$$

Проверить, что резольвента Лагранжа обладает следующими свойствами:

а)  $\sigma(\mathcal{L}(v)) = \zeta\mathcal{L}(v)$ ;

б)  $\mathcal{L}(v)^n \in P$ ;

в) существует элемент  $v \in F$ , для которого  $\mathcal{L}(v) \neq 0$ .

## § 6. Жёсткость и рациональность в конечных группах

В этом параграфе теория Галуа напрямую соединяется с теорией характеров. Эскизность изложения частично компенсируется указанием соответствующей литературы.

**1. Определения и формулировка основной теоремы.** Пусть  $G$  — конечная группа с нейтральным элементом  $e$ . Зафиксируем какие-то классы сопряжённости  $\mathcal{K}_1, \dots, \mathcal{K}_m$  в  $G$  и положим

$$\tilde{\mathcal{S}} = \tilde{\mathcal{S}}(\mathcal{K}_1, \dots, \mathcal{K}_m) = \{(g_1, \dots, g_m) \mid g_i \in \mathcal{K}_i, g_1 g_2 \dots g_m = e\}.$$

В  $\tilde{\mathcal{S}}$  выделим подмножество

$$\mathcal{S} = \mathcal{S}(\mathcal{K}_1, \dots, \mathcal{K}_m) = \{(g_1, \dots, g_m) \in \tilde{\mathcal{S}} \mid \langle g_1, \dots, g_m \rangle = G\}.$$

Очевидно,  $G$  действует сопряжением на  $\tilde{\mathcal{S}}$  и на  $\mathcal{S}$ . Считаем далее  $Z(G) = e$ . В таком случае действие  $G$  на  $\mathcal{S}$  свободно. Действительно, если  $g \in G$  оставляет  $(g_1, \dots, g_m)$  на месте, то  $g$  коммутирует со всеми  $g_i$ , а следовательно, со всеми элементами из  $G$ , поскольку  $\langle g_1, \dots, g_m \rangle = G$ . Но тогда  $g = e$ , поскольку  $Z(G) = e$ .

**Определение.** Говорят, что набор  $(\mathcal{K}_1, \dots, \mathcal{K}_m)$  классов сопряжённости *жёсткий*, если  $\mathcal{S}(\mathcal{K}_1, \dots, \mathcal{K}_m) \neq \emptyset$  и  $G$  действует на  $\mathcal{S}$  транзитивно, т.е., в силу свободы действия,  $|\mathcal{S}| = |G|$ .

Набор  $(\mathcal{K}_1, \dots, \mathcal{K}_m)$  называется *сильно жёстким*, если он жёсткий и  $\mathcal{S} = \tilde{\mathcal{S}}$  (вообще говоря,  $\mathcal{S} \subset \tilde{\mathcal{S}}$ ).

Таким образом, сильная жёсткость имеет место, если  $|\tilde{\mathcal{S}}| = |\mathcal{S}| = |G|$ . Заметим теперь, что

$$|\tilde{\mathcal{S}}| = N(\mathcal{K}_1, \dots, \mathcal{K}_m) \tag{1}$$

равно числу решений  $(g_1^0, \dots, g_m^0)$  уравнения

$$g_1 g_2 \dots g_m = e, \quad g_i \in \mathcal{K}_i.$$

Пусть теперь  $\text{Cl}(G) = \{\mathcal{K}_1, \dots, \mathcal{K}_r\}$  — множество всех классов сопряжённости конечной группы  $G$ , а  $n$  — её *показатель* (или *экспоненту*), т.е. НОК порядков всех элементов группы  $G$ . Группа  $U(Z_n)$  действует на  $G$ :  $g \mapsto g^s$ ,  $s \in U(Z_n)$ , и аналогично — на  $\text{Cl}(G)$ . Далее,  $\text{Irr}(G) = \{\chi_1, \chi_2, \dots, \chi_r\}$  — множество неприводимых комплексных характеров группы  $G$ . Мы знаем, что значения  $\chi_i(g)$  лежат в круговом поле  $\Gamma_n = \mathbb{Q}(\zeta)$ ,  $\zeta^n = 1$ . Следовательно, существует естественное действие группы  $\text{Gal } \Gamma_n/\mathbb{Q} \cong U(Z_n)$  на  $\text{Irr}(G)$ . Действия  $U(Z_n)$  на  $\text{Cl}(G)$  и на  $\text{Irr}(G)$  связаны формулой

$$\sigma_s(\chi)(g) = \chi(g^s),$$

где, как обычно,  $\sigma_s(\zeta) = \zeta^s$ .

**Определение.** Класс  $\mathcal{K} \in \text{Cl}(G)$  называется  *$\mathbb{Q}$ -рациональным* (или просто *рациональным*), если выполнены следующие эквивалентные свойства:

- 1)  $\mathcal{K}$  остаётся на месте при действии  $U(Z_n)$ ;
- 2) каждый характер  $\chi \in \text{Irr}(G)$  принимает на  $\mathcal{K}$  значения в  $\mathbb{Q}$  (на самом деле в  $\mathbb{Z}$ ).

Семейство  $\{\mathcal{K}_i \mid 1 \leq i \leq m\}$  классов сопряжённости группы  $G$  рационально, если рационален каждый из классов  $\mathcal{K}_i$ .

Условие рациональности означает, что если  $g \in \mathcal{K}$ , то все образующие циклической группы  $\langle g \rangle$  лежат в  $\mathcal{K}$ , т.е. сопряжены с  $g$ . Например, в симметрической группе  $S_n$  каждый класс сопряжённости рационален.

Более общо, пусть  $F$  — любое поле,  $\mathcal{K} = g^G$ ,  $\text{НОД}(|\langle g \rangle|, \text{char } F) = 1$ . Тогда говорят об  $F$ -рациональности  $\mathcal{K}$ , коль скоро  $\chi(g) \in F$   $\forall \chi \in \text{Irr}(G)$ , или, эквивалентно, если  $\mathcal{K}^n = \mathcal{K}$   $\forall n$  с  $\sigma_n \in \text{Gal } F(\zeta)/F$ .

Пример 1. Знакопеременная группа  $A_5$  имеет пять классов сопряжённости элементов порядков 1, 2, 3, 5, 5. Пусть  $5A, 5B$  — два класса сопряжённости порядка 5. Если  $a \in 5A$ , то  $a^{-1} \in 5A$  и  $a^2, a^3 \in 5B$ , так что  $5a, 5B$  не  $\mathbb{Q}$ -рациональны. Отметим, что

$$\chi(5A), \chi(5B) \in \mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta), \quad \zeta^5 = 1.$$

Важность понятий сильной жёсткости и  $\mathbb{Q}$ -рациональности семейства  $\{\mathcal{K}_1, \dots, \mathcal{K}_m\}$  классов сопряжённости конечной группы  $G$  объясняется следующей фундаментальной теоремой, которую мы вынуждены принять без доказательства.

**Теорема 1** (Г.В. Белый, Дж. Томпсон). *Пусть  $G$  — конечная группа с тривиальным центром, обладающая рациональным сильно жёстким семейством. Тогда  $G \cong \text{Gal } F/\mathbb{Q}$  для некоторого расширения Галуа  $F/\mathbb{Q}$ .*

Если рациональности нет, то  $\mathbb{Q}$  в теореме заменяется на расширение

$$L = \mathbb{Q}(\text{Irr}(G)) = \mathbb{Q}(\chi(g) \mid \forall \chi \in \text{Irr}(G); g \in \mathcal{K}_1, \dots, \mathcal{K}_m) = \mathbb{Q}(\zeta).$$

Во всех известных случаях групп, близких к простым, для которых установлено свойство сильной жёсткости, семейство  $\{\mathcal{K}_1, \dots, \mathcal{K}_m\}$  является *тривиальным*, т.е.  $m = 3$ . В этом случае, очевидно,  $G$  — группа с двумя образующими. Теорема 1 делает актуальной задачу: выразить свойство сильной жёсткости на языке теории характеров, т.е. найти явные формулы для числа  $N(\mathcal{K}_1, \dots, \mathcal{K}_m)$ . Этим мы и займёмся, после чего рассмотрим примеры.

**2. Подсчёт решений.** Усреднение по группе и лемма Шура (гл. 3, § 4) дают

$$\frac{1}{|G|} \sum_{t \in G} \Psi(txt^{-1}) = \frac{\chi(x)}{\chi(e)} E$$

( $\chi = \chi_\Psi$  — характер неприводимого представления  $\Psi$  группы  $G$ ). Умножая это соотношение на  $\Psi(y)$  справа и переходя к следу, получим

$$\frac{1}{|G|} \sum_{t \in G} \chi(txt^{-1}y) = \frac{\chi(x)\chi(y)}{\chi(e)}.$$

Аналогично,

$$\frac{1}{|G|} \sum_{t_1 \in G} \Psi(t_1 x_1 t_1^{-1} t_2 x_2 t_2^{-1} y) = \frac{\chi(x_1)}{\chi(e)} \Psi(t_2 x_2 t_2^{-1} y),$$

$$\begin{aligned} \frac{1}{|G|^2} \sum_{t_1, t_2 \in G} \Psi(t_1 x_1 t_1^{-1} t_2 x_2 t_2^{-1} y) &= \frac{\chi(x_1)}{\chi(e)} \frac{1}{|G|} \sum_{t_2 \in G} \Psi(t_2 x_2 t_2^{-1} y) = \\ &= \frac{\chi(x_1) \chi(x_2)}{\chi(e)^2} \chi(y). \end{aligned}$$

Очевидная индукция по  $m$  даёт

$$\frac{1}{|G|^m} \sum_{t_1, \dots, t_m} \chi(t_1 x_1 t_1^{-1} \dots t_m x_m t_m^{-1} y) = \frac{\chi(x_1) \dots \chi(x_m)}{\chi(e)^m} \chi(y). \quad (2)$$

Пусть теперь  $\varphi$  — любая центральная функция (функция классов) на  $G$ . Тогда

$$\varphi = \sum_{\chi} c_{\chi} \cdot \chi, \quad c_{\chi} = (\varphi, \chi)_G.$$

Используя (2), введём в рассмотрение величину

$$\begin{aligned} I_m(\varphi) &:= \frac{1}{|G|^m} \sum_{t_1, \dots, t_m} \varphi \left( \left( \prod_{i=1}^m t_i x_i t_i^{-1} \right) y \right) = \\ &= \frac{1}{|G|^m} \sum_{\chi} \sum_{t_1, \dots, t_m} c_{\chi} \chi \left( \left( \prod_{i=1}^m t_i x_i t_i^{-1} \right) y \right) = \sum_{\chi} c_{\chi} \frac{\prod_{i=1}^m \chi(x_i)}{\chi(e)^m} \chi(y). \quad (3) \end{aligned}$$

Оценим  $I_m(\varphi)$  в случае, когда  $\varphi = \delta$  — функция Дирака:  $\delta(e) = 1$  и  $\delta(g) = 0 \quad \forall g \neq e$ . Очевидно,

$$\delta = \frac{1}{|G|} \sum_{\chi} \chi(e) \chi$$

(величина  $1/|G|$ , умноженная на характер регулярного представления). Стало быть,  $c_{\chi} = \chi(e)/|G|$ . Если  $x_1, \dots, x_m, y$  — заданные элементы из  $G$ , то

$$I_m(\delta) = \frac{1}{|G|^m} N'_m,$$

где  $N'_m = N(x_1, \dots, x_m, y)$  — число решений  $(t_1, \dots, t_m)$  уравнения

$$t_1 x_1 t_1^{-1} \dots t_m x_m t_m^{-1} y = e.$$

Таким образом, при помощи (3) находим

$$\begin{aligned} N'_m &= |G|^m I_m(\delta) = |G|^m \sum_{\chi} \frac{\chi(e)}{|G|} \frac{\chi(x_1) \dots \chi(x_m) \chi(y)}{\chi(e)^m} = \\ &= |G|^{m-1} \sum_{\chi} \frac{\chi(x_1) \dots \chi(x_m) \chi(y)}{\chi(e)^{m-1}}. \end{aligned}$$

Полагая  $y = e$ , получаем формулу

$$N_m = N(x_1, \dots, x_{m-1}, x_m) = |G|^{m-1} \sum_{\chi} \frac{\chi(x_1) \dots \chi(x_m)}{\chi(e)^{m-1}}. \quad (4)$$

Пусть  $\mathcal{K}_1, \dots, \mathcal{K}_m$  — классы сопряжённости с представителями  $x_1, \dots, x_m$ , и пусть  $c_i$  — порядок централизатора элемента из  $\mathcal{K}_i$ . Тогда, вспоминая об (1), приходим к выражению

$$N(\mathcal{K}_1, \dots, \mathcal{K}_m) = \frac{N_m}{c_1 \dots c_m}.$$

Применяя формулу (4) и замечая, что  $c_i = |G|/|\mathcal{K}_i|$ , получаем следующее утверждение.

**Теорема 2.** Число  $N(\mathcal{K}_1, \dots, \mathcal{K}_m)$  определяется формулой

$$N(\mathcal{K}_1, \dots, \mathcal{K}_m) = \frac{1}{|G|} |\mathcal{K}_1| \dots |\mathcal{K}_m| \sum_{\chi} \frac{\chi(x_1) \dots \chi(x_m)}{\chi(e)^{m-2}}, \quad (5)$$

где  $\mathcal{K}_i = x_i^G$  и  $\chi \in \text{Irr}(G)$ .  $\square$

Последняя теорема имеет разнообразные приложения. Например, её можно использовать для подсчёта числа подгрупп в  $G$ , изоморфных знакопеременной группе  $A_5$ . Действительно,

$$A_5 = \langle x, y, z \mid x^2 = y^3 = z^5 = e \rangle.$$

Задача сводится к нахождению числа решений уравнения  $xyz = e$ , где  $x, y, z$  принадлежат классам сопряжённости показателей 2, 3 и 5 соответственно. То же замечание применимо к  $S_4, A_4, D_n$  с аналогичным заданием образующими и соотношениями.

Жёсткость часто проверяется в два этапа.

1. Вычисляется  $|\tilde{\mathcal{S}}|$  по формуле (5) и таблице характеров группы  $G$ .

2. Вычисляется  $|\tilde{\mathcal{S}} - \mathcal{S}| = |\tilde{\mathcal{S}}| - |\mathcal{S}|$  путём нахождения всех  $m$ -семейств  $\{g_1, \dots, g_m\}$  в  $\tilde{\mathcal{S}}$ , не порождающих  $G$ ; для этого используют знание максимальных подгрупп группы  $G$ .

**Предложение 1.** Справедливы тождества:

- i)  $|\tilde{\mathcal{S}}(\mathcal{K}_1^n, \dots, \mathcal{K}_m^n)| = |\tilde{\mathcal{S}}(\mathcal{K}_1, \dots, \mathcal{K}_m)|$ ,  $\bar{n} \in U(Z_n)$ ;
- ii)  $|\mathcal{S}(\mathcal{K}_1^n, \dots, \mathcal{K}_m^n)| = |\mathcal{S}(\mathcal{K}_1, \dots, \mathcal{K}_m)|$ ,  $\bar{n} \in U(Z_n)$ .

**Доказательство.** Первое тождество следует из формулы (5), скомбинированной с формулой  $\chi(g^n) = \sigma_n(\chi)(g)$ .

Второе тождество доказывается индукцией по порядку  $|G|$  следующим образом. Для любой подгруппы  $H \subset G$  положим

$$\begin{aligned} \mathcal{S}^{(H)}(\mathcal{K}_1 \cap H, \dots, \mathcal{K}_m \cap H) &= \\ &= \{(g_1, \dots, g_m) \mid g_i \in \mathcal{K}_i \cap H, g_1 \dots g_m = e, \langle g_1, \dots, g_m \rangle = H\}. \end{aligned}$$

Вообще говоря,  $\mathcal{K}_i \cap H$  — не отдельный класс сопряжённости в  $H$ , а объединение некоторого числа таких классов. Формула

$$\tilde{\mathcal{S}} - \mathcal{S}(\mathcal{K}_1, \dots, \mathcal{K}_m) = \bigcup_{H \subset G, H \neq G} \mathcal{S}^{(H)}(\mathcal{K}_1 \cap H, \dots, \mathcal{K}_m \cap H)$$

приводит к индуктивному шагу.  $\square$

**3. Примеры жёсткости.** а) *Симметрическая группа  $S_n$ .* Ясно, что  $S_n (n \geq 3)$  содержит классы сопряжённости  $nA, 2A, \mathcal{K}$ , отвечающие циклам длины  $n, 2, n - 1$ . Утверждается, что тройка  $(nA, 2A, \mathcal{K})$  сильно жёсткая.

Действительно, данный  $n$ -цикл  $x \in nA$  задаёт циклическое упорядочение множества  $\{1, 2, \dots, n\}$ , т.е. ориентированный  $n$ -угольник. Композиция этой перестановки порядка  $n$  с транспозицией даёт  $(n - 1)$ -цикл ровно тогда, когда две переставляемые вершины стоят рядом. Следовательно, решения уравнения  $xyz = e$  с циклами  $x, y, z$  порядка  $n, 2, n - 1$  находятся в биективном соответствии с ориентированными  $n$ -угольниками с одним выделенным ребром. Любые две такие конфигурации могут быть переведены друг в друга одной перестановкой из  $S_n$ . Таким образом,  $|\tilde{\mathcal{S}}| = |G| = n!$ . В свою очередь  $\tilde{\mathcal{S}} = \mathcal{S}$ , поскольку  $\langle x, y, z \rangle = S_n$ . Как уже отмечалось, в  $S_n$  каждый класс сопряжённости рационален. Таким образом, в соответствии с теоремой 1 существует расширение Галуа  $F/\mathbb{Q}$  с  $\text{Gal } F/\mathbb{Q} \cong S_n$ . Разумеется, для нас это не новость (см. § 4), а лишь иллюстрация новых методов.

б) *Группа  $\text{PSL}(2, \mathbb{F}_p)$ .* При  $p > 3$  эта группа простая (теорема 4 в § 2 гл. 2). Все её комплексные характеристы известны, но мы ограничимся замечанием, что  $\text{PSL}(2, \mathbb{F}_p)$  содержит среди прочих по одному классу сопряжённости элементов порядка 2 и 3:  $2A, 3A$ . Имеются два класса  $pA, pB$  элементов порядка  $p$  с представителями — унипотентными матрицами  $\begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}$  и  $\begin{vmatrix} 1 & \alpha \\ 0 & 1 \end{vmatrix}$ , где символ Лежандра  $\left(\frac{\alpha}{p}\right) = -1$ . Сильная жёсткость тройки  $(2A, 3A, pA)$ , а также троек  $(2A, pA, pB)$  при  $\left(\frac{2}{p}\right) = -1$  и  $(3A, pA, pB)$  при  $\left(\frac{3}{p}\right) = -1$  проверяется непосредственно. Рациональности здесь, вообще говоря, не ожидается, как показывает рассмотренный ранее пример группы

$A_5 \cong \mathrm{PSL}(2, 5) := \mathrm{PSL}(2, \mathbb{F}_5)$ .

в) Простая группа  $\mathrm{SL}(2, 8) = \mathrm{SL}(2, \mathbb{F}_8)$  порядка  $504 = 2^3 \cdot 3^2 \cdot 7$ . Хорошим упражнением служит построение таблицы её неприводимых комплексных характеров:

.	$1A$	$2A$	$3A$	$7A$	$7B$	$7C$	$9A$	$9B$	$9C$
$\chi_1$	1	1	1	1	1	1	1	1	1
$\chi_2$	7	-1	-2	0	0	0	1	1	1
$\chi_3$	7	-1	1	0	0	0	$\alpha$	$\alpha'$	$\alpha''$
$\chi_4$	7	-1	1	0	0	0	$\alpha''$	$\alpha$	$\alpha'$
$\chi_5$	7	-1	1	0	0	0	$\alpha'$	$\alpha''$	$\alpha$
$\chi_6$	8	0	-1	1	1	1	-1	-1	-1
$\chi_7$	9	1	0	$\beta$	$\beta'$	$\beta''$	0	0	0
$\chi_8$	9	1	0	$\beta''$	$\beta$	$\beta'$	0	0	0
$\chi_9$	9	1	0	$\beta'$	$\beta''$	$\beta$	0	0	0

Здесь

$$\begin{aligned} \alpha &= -2 \cos \frac{2\pi}{9}, & \alpha' &= -2 \cos \frac{4\pi}{9}, & \alpha'' &= -2 \cos \frac{8\pi}{9}, \\ \beta &= 2 \cos \frac{2\pi}{7}, & \beta' &= 2 \cos \frac{4\pi}{7}, & \beta'' &= 2 \cos \frac{8\pi}{7}. \end{aligned}$$

По формуле (5) имеем

$$|\tilde{\mathcal{S}}(9A, 9B, 9C)| = \frac{504^2}{9^3} \left( 1 + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} + \frac{1}{7} - \frac{1}{8} + 0 + 0 + 0 \right) = 504 = \mathrm{SL}(2, 8).$$

Чтобы убедиться в жёсткости, достаточно проверить, что любой триплет  $(x, y, z) \in \tilde{\mathcal{S}}$  порождает  $\mathrm{SL}(2, 8)$ . Зададим поле

$$\mathbb{F}_8 = \{0, 1, \lambda^i \mid 1 \leq i \leq 6\}, \quad \lambda^3 = \lambda + 1.$$

Надо помнить, что  $\mathbb{F}_8$  — поле характеристики 2 и  $\mathbb{F}_8^* = \langle \lambda \rangle$ . В качестве элементов тройки возьмём матрицы

$$a = \begin{vmatrix} \lambda^2 + 1 & \lambda + 1 \\ \lambda + 1 & \lambda + 1 \end{vmatrix}, \quad b = \begin{vmatrix} \lambda^2 + \lambda + 1 & \lambda \\ \lambda + 1 & 1 \end{vmatrix}, \quad c = \begin{vmatrix} \lambda^2 & \lambda \\ \lambda^2 + \lambda + 1 & 1 \end{vmatrix}.$$

Легко проверяется, что  $a^9 = b^9 = c^9 = e$ ,  $abc = e$ . Степенями матрицы  $d = a^4b^2 = \mathrm{diag}(\lambda^{-1}, \lambda)$  исчерпываются все диагональные элементы группы  $\mathrm{SL}(2, 8)$ . Далее, получаются унипотентные матрицы

$$u = a^2b^4a^4b^2 = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix}, \quad \bar{u} = a^{-2}d^{-1}a^2d^{-1} = \begin{vmatrix} 1 & 0 \\ 1 & 1 \end{vmatrix}$$

и сразу же после этого — элемент  $w = u\bar{u}u = \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$ , играющий ключевую роль в разложении Брюа (см. доказательство теоремы 4 из

§ 2 гл. 2). Осталось получить стандартную борелевскую подгруппу, но детали вычислений мы опустим.

### УПРАЖНЕНИЯ

**1.** Пусть  $G, H$  — конечные группы с сильно жёсткими семействами

$$\tilde{S}(\mathcal{K}_1, \dots, \mathcal{K}_m), \quad \tilde{S}(\mathcal{K}'_1, \dots, \mathcal{K}'_{m'}).$$

Показать, что тогда

$$\tilde{S}(\mathcal{K}_i \times \mathcal{K}'_j \mid 1 \leq i \leq m, 1 \leq j \leq m')$$

— сильно жёсткое семейство в  $G \times H$ .

**2.** Пусть  $\sigma$  — внешний автоморфизм конечной группы, и пусть  $(\mathcal{K}_1, \dots, \mathcal{K}_m)$  — жёсткое семейство классов сопряжённости в  $G$ . Показать, что тогда  $\sigma(\mathcal{K}_i) \neq \mathcal{K}_i$  для некоторого  $i$ .

**3.** Показать, что в знакопеременной группе  $A_5$  с известными нам классами сопряжённости  $1A, 2A, 3A, 5A, 5B$  тройки

$$(2A, 3A, 5A), \quad (2A, 5A, 5B), \quad (3A, 5A, 5B)$$

являются сильно жёсткими. Отсюда следует, что  $A_5 \cong \text{Gal } F/\mathbb{Q}(\sqrt{5})$ .

**4.** Обозначим через  $K_1(z)$  число представлений элемента  $z$  конечной группы  $G$  в виде коммутатора, т.е. число решений уравнения  $z = xyx^{-1}y^{-1}$ . Показать, что

$$K_1(z) = |G| \sum_{i=1}^r \frac{\chi_i(z)}{\chi_i(e)}.$$

Более общо: если  $K_m(z)$  — число решений уравнения

$$z = (x_1 y_1 x_1^{-1} y_1^{-1})(x_2 y_2 x_2^{-1} y_2^{-1}) \dots (x_m y_m x_m^{-1} y_m^{-1}),$$

то

$$K_m(z) = |G|^{2m-1} \sum_i \frac{\chi_i(z)}{\chi_i(e)^{2m-1}}.$$

### § 7. Эпилог

7 ноября 2011 г. исполнится 200 лет со дня рождения Эвариста Галуа (1811–1832), одного из самых знаменитых математиков XIX столетия. Идеи Галуа проникли к настоящему времени в разные области математики, но и то, что обычно называют классической теорией Галуа, продолжает поражать воображение своим новаторством. Имевшиеся до Галуа разрозненные факты об алгебраических уравнениях были объединены и резко расширены им посредством теории групп — теории, также не существовавшей в его время. Были лишь отдельные примеры групп и простейшие понятия (у Лагранжа, Гаусса, Коши, Абеля), но отсутствовала даже какая-либо единная терминология. Введённые Галуа понятия *разрешимой группы*, *простой группы*, *нормальной подгруппы* остаются по сей день наиболее

употребительными в общей теории групп. Неумолимая логика развития привела Э. Галуа к конечным полям (поля Галуа, частично встречавшиеся у Гаусса) и к группам дробно-линейных преобразований над конечными полями. Он доказал простоту групп  $A_n$ ,  $n \geq 5$  (знакопеременные группы), и  $PSL(2, q)$ ,  $q \geq 4$ . Теоремы Галуа о примитивных группах перестановок, о транзитивных группах простой степени и о степенях представлений  $PSL(2, q)$  в качестве транзитивной группы перестановок можно считать прообразом общих классификационных результатов, полученных спустя полтора столетия. Условия разрешимости в радикалах алгебраических уравнений (с целыми рациональными коэффициентами) простой степени, выраженные на теоретико-групповом языке, отличаются полнотой и изяществом. И всё это было обдуманно и доказано Э. Галуа в возрасте от 16 лет до 21 года. Г. Вейль, сам внесший неоценимый вклад в математику, заметил (см. [8]): “Идеи Галуа, остававшиеся на протяжении нескольких десятилетий книгой за семью печатями, стали впоследствии оказывать всё более и более глубокое влияние на развитие всей математики; эти идеи содержатся в прощальном письме Галуа к другу, написанном им накануне смерти, постигшей его на дурацкой дуэли, когда ему не было ещё 21 года. По новизне и глубине идей, выраженных в этом письме, оно является, вероятно, самым выдающимся творением из всего, что когда-либо было написано рукой человека”. Короткая, полная загадок жизнь Э. Галуа с большим тиктом и симпатией описана в книге Л. Инфельда [13].

Общая оценка вклада Э. Галуа в математику дана также в замечательном историческом очерке Ф. Клейна [15]. В частности, Клейн пишет: “Без знакомства с “теорией Галуа” трудно оценить всё значение его достижений. Я хотел бы поэтому попробовать наметить в нескольких словах основной замысел этой теории, хотя в столь кратком изложении и нет возможности дать представление о всём её объёме. Прежде чем сделать это, я хотел бы отметить своеобразную роль, которую играет теория Галуа как предмет преподавания в наших университетах. Здесь происходит конфликт, одинаково прискорбный и для обучающих, и для обучаемых. Именно, с одной стороны, преподаватели, воодушевлённые исключительной гениальностью открытия и значительностью его глубоких результатов, особенно охотно читают курсы о теории Галуа; с другой стороны, как раз эта область представляет исключительные трудности для понимания среднего начинающего студента. Печальным результатом этого в большинстве случаев является то, что затраченные с особой любовью и воодушевлением усилия преподавателей проходят мимо большинства слушателей, не встречая, за редкими исключениями, никакого понимания. Известную роль в этом играют и особые трудности, которые представляет изложение теории Галуа”.

Высказанная выше мысль об особом месте теории Галуа пустила довольно глубокие корни, на что обратил внимание крупный теоретико-числовик А. Вейль. В предисловии к русскому переводу своей книги [9] он пишет: “Было время, когда теория Галуа рассматривалась как вещь трудная и абстрактная, предназначенная лишь для специалистов. Более того, я знал некоторых превосходных математиков моего поколения, которые открыто признавались в своём совершенном невежестве в теории Галуа и, кажется, даже гордились этим. Теперь все хорошо понимают, что это — один из “основных” разделов, с которым каждый серьёзный студент-математик должен познакомиться в первые же годы обучения”.

В последние годы большое внимание привлекла обратная задача теории Галуа, удовлетворительное решение которой (пока не существующее) требует далёких выходов в теорию чисел, алгебраическую геометрию и, естественно, в теорию групп, включая теорию представлений. Кажется, что ситуация, описанная Ф. Клейном, лишь усугубилась. Вместе с тем предмет, стоящий на стыке многих математических дисциплин, должен быть привлекательным для студентов, если на первых порах их внимание будет сосредоточено на элементах теории Галуа, не слишком отягощённой техникой, но достаточно продвинутой для формулировки интересных результатов. Изложение в гл. 5 преследовало именно эти цели. Прямая задача теории Галуа (вычисление группы  $\text{Gal}(f)$  для любого многочлена  $f \in \mathbb{Q}[X]$ ) и обратная задача (построение многочлена с заданной группой Галуа) ещё долго будут предметом серьёзных исследований, не говоря уже о том, что в более полном контексте теория Галуа приобрела общематематическое значение.

# Приложение

## НЕРЕШЁННЫЕ ЗАДАЧИ

---

**1. Классификация конечных простых групп.** Собственно говоря, эта классическая задача считается решённой. Ответ гласит, что каждая конечная простая группа (естественно, не циклическая простого порядка) изоморфна одной из следующих групп: знакопеременная, группа типа Ли, спорадическая. Никаких определений мы не даём, чтобы не увязнуть в деталях. Спорадических простых групп имеется всего 26 штук. К ним относится и упомянутый в преамбуле к гл. 2 монстр  $M$  (другое обозначение  $M = F_1$  — в честь первооткрывателей Нортон-Фишера). Общая ситуация прекрасно описана в книге Д. Горенстейна “Конечные простые группы. Введение в их классификацию” (М.: Мир, 1985). Обещанные несколько тысяч страниц доказательства пока не предъявлены, но активная работа в этом направлении ведётся. Если даже серьёзные пробелы не обнаружатся, широкой математической публике это доказательство будет недоступно. Ещё раз хочется сказать, что сила математики — в её единстве, и кто знает, на каком пути и какими средствами будут даны убедительные, легко проверяемые аргументы в пользу выводов, полученных ценой многолетних усилий.

Общее направление исследований по конечным простым группам определила знаменитая теорема Дж. Томпсона и У. Фейта (1962 г.) о разрешимости любой группы нечётного порядка. Доказательство заняло 255 с. журнального текста. В последующих работах нескольких математиков оно приобрело более прозрачную форму (см., например: *Bender H., Glauberman G. Local Analysis for the Odd Order Theorem.* — Cambridge Univ. Press, 1994), но так и не доведено хотя бы до 100 с. Одна из коварно простых переформулировок задачи заключается в следующем. Допустив существование в данном классе неразрешимой группы, мы должны получить группу  $G$  нечётного порядка, совпадающую со своим коммутантом. Но если  $G = G'$ , то согласно следствию теоремы 7 § 4 гл. 4 имеет место соотношение

$$|G| \cdot \prod_{i=1}^r K_i = \left( \prod_{i=1}^r |\mathcal{K}_i| \right) \sum_{j=1}^r K_j. \quad (*)$$

Соотношение  $(*)$ , полученное при помощи теории характеров, в случае групп нечётного порядка можно редуцировать по модулю 2 и рассмотреть над полем характеристики 2, где оно приобретает ещё более изящную форму:

$$\prod_{i=1}^r K_i = \sum_{j=1}^r K_j. \quad (**)$$

Надо “всего навсего” доказать, что на самом деле соотношения (\*), (\*\*), для групп нечётного порядка никогда не выполняются. Сделать это средствами одной лишь теории характеров невозможно.

**2. Регулярный автоморфизм.** Как отмечалось в [ВА I, гл. 4, § 2], группа  $\text{Aut}(G)$  и даже отдельный элемент  $\varphi \in \text{Aut}(G)$  могут служить источником важных сведений о группе  $G$ . Если

$$a \neq e \Rightarrow \varphi(a) \neq a,$$

то  $\varphi$  называется *регулярным автоморфизмом*. Важная теорема Дж. Томпсона о nilпотентности группы  $G$  с регулярным автоморфизмом простого порядка  $p$  привела к многочисленным следствиям и стимулировала интерес к возможной величине класса nilпотентности  $n$  группы  $G$ . При  $p = 2$  группа  $G$  абелева, а в общем случае доказано (А. Кострикин, В. Крекнин), что  $n = n(p) < p^p$ . На самом же деле гипотеза, идущая от Г. Хигмана, гласит, что

$$n(p) = \frac{(p^2 - 1)}{4}.$$

Эта гипотеза верна при  $p = 3, 5$  и как-будто (со ссылкой на компьютерные вычисления) при  $p = 7$ . Хорошо бы подтвердить эти вычисления и улучшить общую оценку. Гораздо более важна другая гипотеза — о разрешимости конечной группы с регулярным автоморфизмом любого порядка. Прямых подходов к её доказательству пока нет.

**3. Странная алгебра Ли.** Существует ли алгебра Ли  $L$  бесконечной размерности, все собственные подалгебры которой одномерны? Если да, то это означало бы, что  $L$  порождается любой парой непропорциональных элементов:

$$\dim \langle a, b \rangle_F = 2 \implies L = \text{Lie}(a, b).$$

Поле  $F$  можно считать произвольным, например, им может быть  $\mathbb{C}$ . В теории групп аналог такой странной алгебры Ли существует: в своё время А.Ю. Ольшанским был построен пример бесконечной  $p$ -группы, все собственные подгруппы которой циклические порядка  $p$  (простое число  $p$  считается достаточно большим).

**4. Проблема Бернсайда.** Пусть  $F_2 = Gr(x, y)$  — свободная группа с двумя образующими  $x, y$ , и пусть  $F_2^n$  — её нормальная подгруппа, порождённая  $n$ -ми степенями  $w^n$  всех элементов  $w \in F_2$ . Конечна или бесконечна “свободная” группа Бернсаайда  $B(n) = F_2/F_2^n$ ? Для  $n = 2, 3, 4, 6$  ответ положительный, для всех достаточно больших  $n$  ответ отрицательный. Значение  $n = 5$  наименьшее, для которого ответ неизвестен. Частичная переформулировка заключается в следующем.

Пусть

$$(x, y; 1) := (x, y) = xyx^{-1}y^{-1},$$

$$(x, y; s + 1) := ((x, y; s), y).$$

Найдутся ли такие элементы  $w_i(x, y)$  и целое число  $m$ , чтобы в  $F_2$  выполнялось соотношение

$$(x, y; 6) = \prod_{i=1}^m w_i(x, y)^5?$$

Если нет, то группа Бернсайда  $B(5)$  бесконечная; если да, то  $B(5)$  обладала бы интересным свойством энгелевости.

Для ориентировки напомним, что

$$(x, y; 1) = (xy)^2(y^{-1}x^{-1}y)^2(y^{-1})^2,$$

$$(x, y; 2) = (xyx^{-1}y^{-1}x^{-1})^3(xyx)^3(x^{-1}y^{-1})^3.$$

В  $B(4)$  выполнено соотношение

$$(x, y; 5) = \prod_{i=1}^m w_i(x, y)^4.$$

В 1981 г. при помощи ЭВМ Хавас нашёл такое соотношение с  $m = 250$ . Позднее А.В. Корлюков, комбинируя машинные и ручные расчёты, пришёл к соотношению с  $m = 28$ , причём проверка допускается без использования вычислительной техники. Каково наименьшее  $m = m(4)$  и что следует ожидать в интересующем нас случае  $n = 5$ ?

**5. Конечные группы полиномиальных автоморфизмов.** Пусть  $G$  — конечная подгруппа в группе  $\text{Aut}(\mathbb{C}^n)$  всех полиномиальных автоморфизмов. Будет ли  $G$  сопряжена в  $\text{Aut}(\mathbb{C}^n)$  с конечной подгруппой в  $\text{GL}(n, \mathbb{C})$ ? Для  $n = 2$  это так (теорема Гизатуллина—Данилова). При  $n \geq 3$  вопрос остаётся открытым (*Furushima Mikio// Tôhoku Math. J. — 1983. —V. 35, № 3. — P. 415–424*).

**6. Просто приводимые группы** (или *SR-группы* — по терминологии Е. Вигнера). Конечная группа  $G$  называется *SR-группой*, если

$$\sum_{g \in G} f(g)^3 = \sum_{g \in G} |C_G(g)|^2,$$

где

$$f(g) = \text{Card}\{x \in G \mid x^2 = g\}.$$

Коэффициентами разложения тензорного произведения любых двух неприводимых представлений *SR-групп* будут лишь нули и единицы, что важно для интерпретации некоторых физических задач (*Хамермеш М. Теория групп и её применение к физическим проблемам. — М.: Мир, 1966*). Класс *SR-групп* не пуст, как показывают примеры

любой элементарной абелевой 2-группы, обобщённой группы кватернионов  $Q_{2^n}$  и любой диэдральной группы. Дадим кое-какие пояснения. По определению

$$Q_{2^n} = \langle a, b \mid a^{2^{(n-1)}} = e, \quad b^2 = a^{2^{(n-2)}}, \quad ba^i = a^{-i}b \rangle, \quad n \geq 3.$$

Заметим, что

$$Z(Q_{2^n}) = \{e, a^{2^{(n-2)}}\}.$$

При  $n = 3$  получается обычная группа кватернионов. Прямые вычисления в  $G = Q_{2^n}$  показывают, что

$$\begin{aligned} \sum_g f(g)^3 &= (2^{n-1} + 2)^3 + (2^{n-2} - 1) \cdot 2^3 = \\ &= (2^{n-1} - 2)(2^{n-1})^2 + 2(2^n)^2 + 2^{n-1} \cdot 4^2 = \sum_g |C_G(g)|^2. \end{aligned}$$

Аналогично, если  $G = D_{2n+1}$ , то

$$\begin{aligned} \sum_g f(g)^3 &= (2n + 2)^3 + 2n \cdot 1^3 = \\ &= 2^2(2n + 1)^2 + 2n(2n + 1)^2 + (2n + 1)2^2 = \sum_g |C_G(g)|^2. \end{aligned}$$

Если  $G = D_{2n}$ , то

$$\begin{aligned} \sum_g f(g)^3 &= (2n + 2)^3 + (n - 1) \cdot 8 = \\ &= 2(2 \cdot 2n)^2 + (2n - 2)(2n)^2 + 2n \cdot 4^2 = \sum_g |C_G(g)|^2. \end{aligned}$$

Несложно проверяется, что симметрическая группа  $S_4$  является  $SR$ -группой, но  $S_5$  таковой уже не будет. Как выразить в общем принадлежность  $G$  к  $SR$ -классу в терминах структурных свойств самой группы  $G$ ?

**7. Обратная задача Галуа.** Говорят ещё “обратная задача теории Галуа”. Речь идёт о построении расширений Галуа поля рациональных чисел  $\mathbb{Q}$  с заданными группами Галуа. Первопроходцем был Д. Гильберт: его теорема о неприводимости утверждает, что достаточно реализовать заданную группу  $G$  в качестве группы Галуа расширения над функциональным полем  $\mathbb{Q}(x)$ . Раз это так, то на сцену выходят методы теории римановых поверхностей и алгебраической геометрии. Следующим поворотным пунктом оказалась замечательная

Теорема (И.Р. Шафаревич, 1954 г.) *Любая конечная разрешимая группа реализуется в качестве группы Галуа некоторого нормального расширения  $F/\mathbb{Q}$ .*

Его метод в основном теоретико-числовой.

Подходом, развитым в последние годы, является метод жёсткости, кратко изложенный в гл. 5 и в значительной мере приспособленный к простым или близким к ним группам. Первым жёсткость, не употребляя этого термина, эффективно использовал Г.В. Белый (Изв. АН СССР. Сер. матем. — 1979. — Т. 43, № 2. — С. 267–276) для реализации большинства линейных и проективных линейных групп в качестве групп  $\text{Gal}(E/L)$  с абелевым расширением  $L$  поля  $\mathbb{Q}$ . Термины жёсткости и рациональности, с необходимым обоснованием, были введены Дж.Томпсоном в работе (*Thompson J.// J. Algebra*. — 1984. — V. 89, № 2. — P. 337–499), где он показал, что монстр  $M = \text{Gal}(F/\mathbb{Q})$  для некоторого расширения Галуа  $F/\mathbb{Q}$ . Сам монстр  $M$  к тому времени уже прочно вошёл в теорию модулярных форм (благодаря фантастическим свойствам своих комплексных неприводимых характеров) и даже постучался в струнную теорию физиков. Несколько специальных конференций посвящены самому монстру (например: а) Moonshine, the Monster, and Related Topics: Research Conf., June 1994/ Eds Ch. Dong, G. Mason// Contemp. Math. — 1996. — № 193; б) Groups, Difference Sets, and the Monster// Eds K. Harada, L. Solomon et al. — B., N.Y.: de Gruyter, 1996). Свойства рациональной сильной жёсткости подробно обсуждаются в книгах [37–39, 41]. Всё новые и новые классические простые группы находят реализацию в качестве групп Галуа расширений над  $\mathbb{Q}$ . К сожалению, далеко не все простые группы обладают свойством рациональной жёсткости. Например,  $\text{PSL}(2, 29^2)$  этим свойством не обладает, хотя известно, что эта группа является группой Галуа над  $\mathbb{Q}$ . Более того, группы Сузуки  $\text{Sz}(q)$  порядков

$$q^2(q - 1)(q^2 + 1), \quad q = 2^{2n+1},$$

не обладают свойством рациональной жёсткости и не известно, являются ли они группами Галуа над  $\mathbb{Q}$ , по крайней мере при больших  $n$ . Стоит отметить, что  $\text{Sz}(q)$  занимают особое место в списке простых групп, поскольку только их порядки не делятся на 3.

Прямая и обратная задачи Галуа весьма трудоёмки в том смысле, что вычисление  $\text{Gal}(f)$  для явно заданного многочлена  $f \in \mathbb{Q}[X]$  или, напротив, поиск многочлена с предписанной группой Галуа  $G$  даже при сравнительно небольших  $\deg f$  и  $|G|$  требует больших усилий со стороны человека, вооружённого компьютером. Эта сторона деятельности отражена в книге [37]. Стоит попробовать прямыми вычислениями показать, что

$$\text{Gal}(X^7 - 7X + 3) \cong \text{PSL}(2, 7).$$

Причина трудностей отчасти обусловлена доказанным Ван дер Варденом (1933 г.) фактом, согласно которому “почти все” многочлены степени  $n$  имеют  $S_n$  в качестве своей группы Галуа над  $\mathbb{Q}$ .

Обратная задача Галуа имеет более широкую постановку как в известных нам рамках, так и в других математических теориях, например, в дифференциальной теории Галуа, где алгебраическое уравнение  $f(x) = 0$  заменено, скажем, на обыкновенное дифференциальное уравнение с коэффициентами в  $\mathbb{C}(z)$ . Обстоятельное обсуждение всего круга возникающих здесь проблем дано в докладе на семинаре Бурбаки: *Van Der Put M. Recent work on differential Galois theory// Séminaire N. Bourbaki. — June 1998. — Exp. 849.*

# ОТВЕТЫ И УКАЗАНИЯ К УПРАЖНЕНИЯМ

---

Номер **p.q.r** отсылает к упражнению **r** из § **q** главы **p**.

**1.1.3.**  $Q_8$  изоморфна группе этих матриц.

**1.1.4.** Нет.

**1.2.1.** Разложить  $G$  по  $H$  сначала в левые, а затем в правые смежные классы с теми же представителями.

**1.3.1.** Взять в качестве  $H$  стационарную подгруппу  $G_1$  точки  $1 \in \Omega$ , воспользоваться разложением (3) и положить  $\sigma(i) = g_i G_1$ .

**1.3.3.** Обратить внимание на то, что все элементы группы  $P$  имеют вид  $g = A^i B^j C^k$ , где

$$A = \begin{vmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad B = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{vmatrix}, \quad C = \begin{vmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix};$$

если  $g \notin Z(P)$ , то  $C_P(g) = \langle g \rangle Z(G)$ ,  $|C_P(g)| = p^2$ .

**1.3.4.** Если  $\sigma \in S_n$  и  $\pi = \pi_1 \dots \pi_m$ , то

$$\sigma \pi \sigma^{-1} = \sigma \pi_1 \sigma^{-1} \dots \sigma \pi_m \sigma^{-1};$$

далее,

$$\sigma(i_1 i_2 \dots i_k) \sigma^{-1} = (\sigma(i_1) \sigma(i_2) \dots \sigma(i_k))$$

для любого цикла  $(i_l, i_2, \dots, i_k)$  длины  $k$ .

**1.3.8.** В сумме  $\sum N(g)$  каждый элемент  $x \in \Omega$  подсчитывается  $|St(x)|$  раз. Стало быть, элементы, лежащие с  $x$  в одной орбите, вносят в  $\sum N(g)$  вклад, равный

$$(G : St(x)) \times |St(x)| = |G|.$$

**1.3.9. 1)** Если  $D(a)$  — группа, то  $e \in D(a)$ , так что  $ea = a^{-1}e$ , т.е.  $a^2 = e$  и  $D(a) = C(a)$ .

**2)** Если  $D(a)$  пусто, то  $E(a) = C(a) \cup D(a)$  — группа, так что считаем  $D(a)$  непустым множеством. Заметим, что  $xa = a^{-1}x \implies a^{-1}x^{-1} = x^{-1}a$ . Поэтому

$$x \in D(a) \iff x^{-1} \in D(a), \quad xa = a^{-1}x \iff ax = xa^{-1}.$$

Так как  $C(a)$  и  $D(a)$  замкнуты относительно взятия обратных, то таково же и множество  $E(a)$ .

Если  $x, y \in C(a)$ , то и  $xy \in C(a)$ . Если  $x, y \in D(a)$ , то

$$axy = x a^{-1} y = x y a,$$

т.е.  $xy \in C(a) \subset E(a)$ . Третья возможность:  $x \in D(a)$ ,  $y \in C(a)$ . В этом случае

$$axy = x a^{-1} y = x y a^{-1},$$

так что  $xy \in D(a) \subset E(a)$ . Остаётся заметить, что  $e \in C(a) \subset E(a)$ .

**1.4.9.** Подсчитать число элементов порядка 2 или воспользоваться результатом упр. 8.

**1.4.12.**  $aba = ba^2b = ba^{-1}b \implies ab^2 = aba \cdot a^{-1}b = ba^{-1}b \cdot a^{-1}b = ba^{-1} \cdot aba = b^2a$ . Сделать отсюда заключение, что  $ab = ba$  и, следовательно, с учётом других соотношений  $b = e$ .

**1.4.13.** Любая матрица  $A = (a_{ij})$  размера  $n \times n$  записывается в виде объединения столбцов  $(a_{ij}) = (A^{(1)}, \dots, A^{(n)})$ . Определим отображение  $f : S_n \rightarrow GL(n)$ , полагая

$$\pi \mapsto f(\pi) = (E^{(\pi 1)}, \dots, E^{(\pi n)}), \quad (*)$$

где  $E^{(i)}$  —  $i$ -й столбец единичной матрицы  $E$ . Таким образом,  $f(\pi)$  есть  $n \times n$ -матрица, в каждой строке и в каждом столбце которой стоит ровно одна единица, а остальные места заняты нулями (*матрица перестановки*). Легко сообразить, что  $f(\pi) \in GL(n)$ .

Пусть  $\sigma, \tau$  — произвольные перестановки,  $\pi = \sigma\tau$  — их произведение. По определению в  $i$ -й строке матрицы  $f(\sigma) = (a_{is})$  и в  $j$ -м столбце матрицы  $f(\tau) = (b_{kj})$  отличными от нуля элементами будут соответственно  $a_{i,\sigma^{-1}i} = 1$  и  $b_{\tau j,j} = 1$ . Поэтому для матрицы  $f(\sigma)f(\tau) = (c_{ij})$  условие  $c_{ij} \neq 0$  эквивалентно условию  $\sigma^{-1}i = \tau j$ , т.е.  $i = \sigma\tau j = \pi j$ , а это как раз и означает, что  $f(\sigma)f(\tau) = f(\sigma\tau)$ . Следовательно,  $f$  — гомоморфизм.

Свойство  $\text{Ker } f = e$  очевидно, поскольку непосредственно из  $(*)$  видно, что  $f(\pi) = E \implies \pi = e$ . Стало быть,  $f$  — мономорфизм.

Наконец, определитель — кососимметрическая функция своих столбцов. Поэтому  $\det f(\pi) = g(E^{(1)}, \dots, E^{(n)})$  — кососимметрическая функция аргументов  $E^{(1)}, \dots, E^{(n)}$ . Из  $(*)$ , а также из определения  $\varepsilon_\pi$  и действия  $S_n$  на  $g$  вытекает, что

$$\begin{aligned} \varepsilon_\pi \det f(\pi) &= \varepsilon_\pi \cdot g(E^{(1)}, \dots, E^{(n)}) = (\pi \circ g)(E^{(1)}, \dots, E^{(n)}) = \\ &= g(E^{(\pi 1)}, \dots, E^{(\pi n)}) = \det(E^{(1)}, \dots, E^{(n)}) = \det E = 1. \end{aligned}$$

Стало быть,  $\det f(\pi) = \varepsilon_\pi$ .

Случай  $n = 3$ :

$$\begin{aligned} e \mapsto \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad (12) \mapsto \begin{vmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{vmatrix}, \quad (13) \mapsto \begin{vmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{vmatrix}, \\ (23) \mapsto \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix}, \quad (123) \mapsto \begin{vmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{vmatrix}, \quad (132) \mapsto \begin{vmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{vmatrix}. \end{aligned}$$

**2.2.3.** Группа  $S_4$  без центра, а  $\text{SL}(2, 3)$  имеет центр порядка 2. Да, группы  $A_4$  и  $\text{PSL}(2, 3)$  изоморфны.

**2.2.4.** Группа  $G$  порядка  $pq$ ,  $p < q$ , обязательно имеет нормальную силовскую  $q$ -подгруппу, поскольку  $N_q = 1 + kq$  должно быть делителем  $G$ ,

а это возможно только при  $k = 0$ . Если и  $N_p = 1$ , то  $G$  — циклическая группа. При  $N_p = 1 + lp = q$  группа будет неабелевой.

**2.2.6.** Наиболее интересен случай  $|G| = 30$ . Прямая проверка с использованием теорем Силова показывает, что хотя бы одна из подгрупп  $G_p$  должна быть нормальной. В противном случае  $N_5 = 6$ ,  $N_3 = 10$ , и получается 24 элемента порядка 5, 20 элементов порядка 3, что явно абсурдно.

**2.3.9.** Применить теорему о согласованных базисах. В случае совпадения рангов доказать заодно, что  $(F_n^{ab} : A) = \det C$ , где  $C$  — матрица перехода от базиса в  $F_n^{ab}$  к базису в  $A$ .

**2.4.1.** Положим  $\Gamma_t = \log \sigma(t)$ . Тогда  $\Gamma_t$  будет кривой в  $M_n(\mathbb{R})$  с  $\sigma(t) = \exp(\Gamma_t)$ . Если  $\Gamma'_0 = A$ , то нужно показать, что  $\Gamma_t$  — прямая в  $M(\mathbb{R})$ , проходящая через 0, т.е  $\Gamma_t = tA$ . Зафиксировав  $t$ , будем иметь

$$\begin{aligned}\Gamma'_t &= \lim_{s \rightarrow 0} \frac{\Gamma_{t+s} - \Gamma_t}{s} = \lim_{s \rightarrow 0} \frac{\log \sigma(t+s) - \log \sigma(t)}{s} = \\ &= \lim_{s \rightarrow 0} \frac{\log(\sigma(t)\sigma(s)) - \log \sigma(t)}{s},\end{aligned}$$

поскольку  $\sigma$  — однопараметрическая подгруппа и  $t+s = s+t$ . Это показывает, что

$$\Gamma'_t = \lim_{s \rightarrow 0} \frac{\log \sigma(s)}{s} = \Gamma'_0.$$

Мы видим, что  $\Gamma'_t$  не зависит от  $t$ , являясь прямой. Итак, любой касательный вектор к  $GL(n, \mathbb{R})$  совпадает с производной в 0 некоторой однопараметрической подгруппы.

**2.5.2.** Пусть  $\mathcal{D}$  — дифференцирование алгебры Ли  $L(G)$ . Полагая  $c_t = = [(\exp(t\mathcal{D}))\mathbf{a}, (\exp(t\mathcal{D}))\mathbf{b}]$ , будем иметь

$$\begin{aligned}\frac{d}{dt} c_t &= [\mathcal{D}(\exp(t\mathcal{D}))\mathbf{a}, (\exp(t\mathcal{D}))\mathbf{b}] + [(\exp(t\mathcal{D}))\mathbf{a}, \mathcal{D}(\exp(t\mathcal{D}))\mathbf{b}] = \\ &= \mathcal{D}[(\exp(t\mathcal{D}))\mathbf{a}, (\exp(t\mathcal{D}))\mathbf{b}] = \mathcal{D}c_t.\end{aligned}$$

Но дифференциальное уравнение

$$\frac{d}{dt} c_t = \mathcal{D}c_t$$

с начальным условием  $c_0 = [\mathbf{a}, \mathbf{b}]$  обладает единственным решением

$$c_t = (\exp(t\mathcal{D}))[\mathbf{a}, \mathbf{b}].$$

Мы видим, что  $\exp(t\mathcal{D})$  — автоморфизм.

**3.1.2.** Да.

**3.2.1.** Продифференцировать равенство  $e^{i\alpha t} \overline{e^{i\alpha t}}$  по  $t$  и положить  $t = 0$ .

**3.3.1.** Посмотреть на доказательство теоремы 2 из § 2 гл. 1.

**3.3.2.** Используя сопряжённость всех элементов порядка 2, показать, что они располагаются в “букете” (см. рис. 6) из пяти

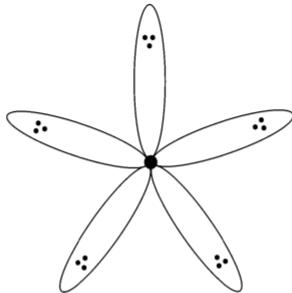


Рис. 6

попарно непересекающихся (точнее, пересекающихся по  $e$ ) сопряжённых силовских подгрупп порядка 4. Группа **I** действует на букете сопряжением. Это действие точно, поскольку **I** — простая группа (см. упр. 1).

**3.3.3.** Применить теорему о гомоморфизмах к случаю  $\Phi : \mathrm{SU}(2) \rightarrow \mathrm{SO}(3)$ .

**3.3.7.** Применить соображения, использованные при подсчете числа ожерелей (задача 2 в начале главы).

**3.4.1.** Переписать соотношения (4) и (5) в виде

$$|G|^{-1} \sum_g \psi_{j_0 j_0}(g) \varphi_{i_0 i}(g^{-1}) = \delta_{\Phi, \Psi} \frac{\delta_{j_0 j_0 i_0}}{\chi_\Phi(e)}.$$

Умножить обе части этого равенства на  $\psi_{k j}(h)$  и просуммировать по  $j$ , приняв во внимание равенство  $\sum_j \psi_{k j}(h) \psi_{j_0 j_0}(g) = \psi_{k j_0}(hg)$ . В получившемся соотношении

$$|G|^{-1} \sum_g \psi_{k j_0}(hg) \varphi_{i_0 i}(g^{-1}) = \delta_{\Phi, \Psi} \frac{\psi_{k i}(h) \delta_{j_0 i_0}}{\chi_\Phi(e)}$$

положить  $j_0 = k, i_0 = i$ , а затем суммированием по  $i$  и  $k$  перейти к характерам.

**3.4.3.** Пусть  $\Phi$  — неприводимое представление,  $h$  — элемент из  $G$ . В силу коммутативности группы  $\Phi(g)\Phi(h) = \Phi(h)\Phi(g) \forall g \in G$ . Положив  $\sigma = \Phi(h)$  в лемме Шура, получим  $\Phi(h) = \lambda_h \mathcal{E}$ . Это верно для любого  $h \in G$ . Для неприводимого  $\Phi$  остаётся единственная возможность — быть одномерным.

**3.4.5.** По условию  $B\Phi_g B^{-1} = \Psi_g$  для некоторой матрицы  $B = (b_{ij}) \in \mathrm{GL}(n, \mathbb{C})$ . Операция  $A \mapsto A^* = {}^t \bar{A}$ , применённая к  $B\Phi_g = \Psi_g B$ , даёт  $\Phi_g^{-1} B^* = B^* \Psi_g^{-1}$ , откуда  $\Phi_g^{-1} B^* B = B^* B \Phi_g^{-1}$ . По лемме Шура  $B^* B = \lambda \mathcal{E}$ . Далее,  $\lambda = \sum_{k=1}^n |b_{ki}|^2 = \mu \bar{\mu}$ ,  $\mu \in \mathbb{C}$  и  $C = \mu^{-1} B$  — искомая унитарная матрица.

**3.4.6.** Без ограничения общности считаем  $G$  матричной группой:  $G \subset \mathrm{GL}(n, \mathbb{C})$ , где  $n$  — степень представления. Пусть

$$C(G) = \{M \in M_n(\mathbb{C}) \mid MX = XM \quad \forall X \in G\}$$

— централизатор группы  $G$  в  $M_n(\mathbb{C})$ . Очевидно, что  $C(G)$  — подкольцо, содержащее  $Z(G)$ . По лемме Шура каждая матрица в  $C(G)$ , отличная от нулевой, невырожденная. Следовательно,  $C(G)$  — тело. Его центр  $K$  является полем и  $Z(G) \subseteq K$ . Таким образом,  $Z(G)$  — конечная подгруппа мультиликативной группы поля  $K$ . Как известно ещё из [ВА I], такая подгруппа всегда циклическая.

**3.4.7.** Решение короче формулировки упражнения. Нужно заметить, что

$$\chi_\Phi(g) = \text{tr } \Phi_g = \text{tr } C_g \Phi_g C_g^{-1} = \text{tr } \Psi_g = \chi_\Psi(g) \quad \forall g \in G,$$

т.е. характеры представлений  $\Phi$  и  $\Psi$  совпадают. Теперь достаточно применить следствие теоремы 2.

**3.5.2.** Из  $a^\tau(\chi_1\chi_2) = a^\tau(\chi_1)a^\tau(\chi_2)$  следует, что  $a^\tau$  — характер группы  $\widehat{A}$ . Так как  $(aa')^\tau = a^\tau(a')^\tau$ , то  $\tau$  — гомоморфизм  $A$  в  $\widehat{A}$ . Далее,

$$\text{Ker } \tau = \{a \in A \mid a^\tau(\chi) = \chi(a) = 1 \ \forall \chi \in \widehat{A}\} \implies \text{Ker } \tau = e,$$

а  $|\widehat{A}| = |\widehat{A}| = |A| \implies \tau$  — изоморфизм.

**3.5.7.** 5, 1, -1, 0, 0.

**3.6.2.** Сравнивая размерности, получить разложение в прямую сумму пространств

$$P_m = H_m \oplus (x^2 + y^2 + z^2)H_{m-2} \oplus (x^2 + y^2 + z^2)^2 H_{m-4} \oplus \dots$$

**3.6.4.** Ввиду простоты  $\text{SO}(3)$  нетривиальность  $\tau$  означала бы, что  $\tau$  — точное представление степени 2. Но, как видно из примера 3 п. 4 § 5 или из описания конечных подгрупп в  $\text{SU}(2)$  (см. § 3), даже ограничение  $\tau|_O$ ,  $O \cong S_4$  не может быть точным.

**4.1.1.** Очевидно, что  $J$  — собственный идеал в  $Q_M(\mathbb{Z})$ . Если  $c/d \notin J$ , то  $c \notin p\mathbb{Z}$ , и, следовательно,  $d/c \in Q_M(\mathbb{Z})$ . Это означает, что всякий идеал  $L$ , полученный из  $J$  добавлением хотя бы одного элемента  $c/d$ , содержит  $1 = c/d \odot d/c$  и, стало быть, совпадает с  $Q_M(\mathbb{Z})$ .

**4.2.8.** Рассмотреть примитивный корень  $\alpha$  степени 8 из 1 в алгебраическом замыкании  $\Omega_p$  поля  $\mathbb{F}_p$ . Так как  $\alpha^4 = -1$ , то  $\alpha^2 + \alpha^{-2} = 0$ ; кроме того,  $\alpha^5 = -\alpha$ ,  $\alpha^{-5} = -\alpha^{-1}$ , откуда  $\alpha^5 + \alpha^{-5} = -(\alpha + \alpha^{-1})$ . Полагая  $\beta = \alpha + \alpha^{-1}$ , будем иметь  $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = 2$ , так что

$$p \equiv \pm 1 \pmod{8} \implies \beta^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = \beta \implies$$

$$\implies 1 = \beta^{p-1} = (\beta^2)^{(p-1)/2} = 2^{(p-1)/2} \implies \left(\frac{2}{p}\right) = 1.$$

Аналогично,

$$p \equiv \pm 5 \pmod{8} \implies \beta^p = \alpha^p + \alpha^{-p} = \alpha^5 + \alpha^{-5} =$$

$$= -(\alpha + \alpha^{-1}) = -\beta \implies -1 = \beta^{p-1} = 2^{(p-1)/2} \implies \left(\frac{2}{p}\right) = -1.$$

**4.2.9.** Если  $n = 1$  и  $f(x) = \sum_{i=1}^m a_i x^i$ ,  $a_m \neq 0$ , то

$$f(xy) = \sum_{i=1}^m a_i x^i y^i = f(x) f(y) = f(x) \left( \sum_{i=1}^m a_i y^i \right),$$

где  $x, y$  — независимые переменные. Равенство коэффициентов при  $y^m$  показывает, что  $a_m x^m = f(x)a_m$  и, стало быть,  $f(x) = x^m$ . Если теперь в общем случае положить  $g(x) = f(x \cdot E)$ , то  $g(xy) = g(x)g(y)$ . Отсюда и из справедливости утверждения при  $n = 1$  вытекает, что  $g(x) = x^s$ . Так как  $X \cdot X^\vee = (\det X) \cdot E$ , то

$$f(X)f(X^\vee) = f((\det X)E) = g(\det X) = (\det X)^s.$$

Но  $f(X)$ ,  $f(X^\vee)$  и  $\det X$  — многочлены от  $x_{ij}$ ,  $1 \leq i, j \leq n$ , причём  $\det X$  неприводим (см. [BA I, гл. 5 § 3, упр. 7]). По теореме 4 о факториальности кольца многочленов любого числа переменных  $f(X) = c(\det X)^m$ ,  $c$  — константа, причём  $f(XY) = f(X)f(Y) \implies c^2 = c$ , а так как  $c \neq 0$ , то  $c = 1$ .

**4.4.2.** Ясно, что  $(1, 0)$  — двусторонняя единица в  $A \oplus A$ . Положим  $e = (0, 1)$ . По определению  $e^2 = -1$ . Так как  $(x, 0)e = (0, x)$ , то, отождествив элемент  $x \in A$  с элементом  $(x, 0) \in A \oplus A$ , придём к выражению  $(x, y) = x + ye$ . Операция сопряжения в  $A \oplus A$  задаётся формулой  $\overline{(x, y)} = (\bar{x}, -y)$ , т.е.  $\overline{x + ye} = \bar{x} - ye$ . Если теперь  $a = x + ye$ ,  $b = u + ve$ , то

$$\overline{ab} = \overline{xu + (ye)u + \bar{x}(ve) + (ye)(ve)} = \overline{ux} - \overline{u}(ye) - (ve)\bar{x} + (ve)(ye) = \overline{ba}.$$

Таким образом, операция сопряжения определена правильно. Непосредственно проверяются свойства

$$ea = \overline{ae}, \quad a(be) = (ba)e.$$

Всё это означает, что удвоение алгебры  $A$  некоммутативно, если операция сопряжения на  $A$  не является тождественной. Удвоение неассоциативно, если исходная алгебра  $A$  некоммутативна. Удвоение коммутативной и ассоциативной алгебры  $A$  ассоциативно. Эти замечания показывают, в частности, что восьмимерная алгебра Кэли  $\mathbb{Ca}$  неассоциативна.

**4.4.5.** Нет. По теореме 4 для любых двух абелевых групп одинаковых порядков строение их групповых алгебр над  $\mathbb{C}$  одно и то же. Гораздо более тонкие вопросы возникают при изоморфизме групповых колец:  $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ .

**4.4.6.** Воспользоваться следствием теоремы 3:  $\langle \Phi_g \mid g \in G \rangle = M_n(\mathbb{C})$ . Приходим к выводу, что  $\text{tr}(CX) = 0$  для любой матрицы  $X \in M_n(\mathbb{C})$ , т.е.  $C = 0$ .

**5.1.4.** Рассмотреть поле разложения  $F$  многочлена  $X^p - a$ . Пусть  $\theta \in F$  — один из корней, так что  $a = \theta^p$  и  $X^p - a = (X - \theta)^p$ . Если теперь  $X^p - a = u(X)v(X)$ , где  $u(X)$  — нормализованный многочлен над  $F$  положительной степени  $m < p$ , то в силу факториальности  $F[X]$  должно выполняться равенство  $u(X) = (X - \theta)^m$ . В частности,  $\theta^m, \theta^p \in F \implies \theta \in F$ .

**5.1.5.** Согласно предыдущему упражнению достаточно убедиться, что

равенство

$$X^p - Y = \left( X - \frac{g(Y)}{h(Y)} \right)^p$$

с  $g, h \in Z_p[Y]$  невозможно.

**5.2.1.** Согласно (8)  $X^d - 1 = \prod_{e|d} \Phi_e(X)$ . Поэтому

$$X^n - 1 = (X^d - 1) \prod_{s|n; s \neq d} \Phi_s(X) = (X^d - 1) \Phi_n(X) \prod_{s|n; s \neq d, n} \Phi_s(X).$$

Остается сослаться на (10).

**5.2.2.** Так как  $\Phi_n(X) = \prod(X - \varepsilon)$ , где  $\varepsilon$  пробегает примитивные корни, то при  $n > 1$  все  $\varepsilon$  не равны 1, и поэтому расстояние на комплексной плоскости от точки  $q$  до любого  $\varepsilon$  больше расстояния от  $q$  до 1. Стало быть,  $|\Phi_n(q)| = \prod(|q - \varepsilon|) > q - 1$  и  $q - 1$  никак не может делиться на  $\Phi_n(q)$ .

**5.2.7.** Перейти к уравнению  $x^2 + y^2 - z^2 = 0$  с  $x, y, z \in \mathbb{F}_p$ . По теореме Шевалле (см. упр. 4 из [ВА I, гл. 6, § 1]) общее число  $N$  решений этого уравнения делится на  $p$ . Пусть решений с  $xyz \neq 0$  не существует. Подсчитать тогда  $N$ , рассматривая отдельно два случая. Если не существует  $a \in \mathbb{F}_p$  с  $a^2 + 1 = 0$ , то решениями будут лишь

$$(0, 0, 0), (0, n, \pm n), (n, 0, \pm n), \quad n = 1, 2, \dots, p - 1,$$

и поэтому  $N = 4p - 3 \equiv 0 \pmod{p} \implies p = 3$ . Если  $a^2 + 1 = 0$  для некоторого  $a \in \mathbb{F}_p$ , то  $N = 6p - 5 \equiv 0 \pmod{p} \implies p = 5$ .

**5.2.8.** Вообще говоря, нет.

**5.3.2.** а)  $A_3$ ; б)  $S_3$ ; в)  $S_3$ ; г)  $Z_4$ ; д)  $D_4$ .

**5.3.1.** Над полем  $P(\zeta)$ ,  $\zeta^p = 1$ , многочлен  $X^p - a \in P[X]$  либо неприводим, либо распадается на линейные множители, когда все корни лежат в  $P(\zeta)$ . Предположим, что имеет место последнее и что  $u$  — один из корней. По теореме 4  $F/P$  будет расширением Галуа для любого  $F/P \subset P(\zeta)/P$ . В частности, минимальный многочлен  $f_u$  элемента  $u$  распадается в  $P(u)$  на линейные множители. Предположив, что  $u \notin P$ , т.е.  $\deg f_u \geq 2$ , рассмотрим другой его корень  $v \neq u$ . Тогда с точностью до выбора примитивного корня  $\zeta = u/v \in P(u)$  и  $P(u) = P(\zeta)$ . Это означает, что если  $X^p - a$  не имеет корней в поле  $P$ , то все его неприводимые множители одной и той же степени  $[P(\zeta) : P]$ , т.е.  $[P(\zeta) : P]$  делит простое число  $p$ . Но это исключается, поскольку  $1 < [P(u) : P] = [P(\zeta) : P] \leqslant p - 1$ . Итак, многочлен  $X^p - a$ , не имеющий корней в поле  $P$ , неприводим над  $P(\zeta)$ .

**5.4.1.**  $\theta + 1$ .

**5.5.3.** Предположив, что один из корней  $\alpha$  можно выразить через вещественные радикалы, мы должны заключить, что это справедливо и для остальных двух вещественных корней  $\beta, \gamma$ , поскольку они удовлетворяют квадратному уравнению с коэффициентами в поле  $P(\alpha)$ . Согласно теореме 13 порядок группы Галуа поля разложения нашего многочлена должен быть степенью двойки. Но это не так: порядок группы Галуа неприводимого многочлена степени 3 делится на 3.

**5.5.4.** а) Очевидно.

$$\text{б)} \sigma((\mathcal{L}(v))^n) = (\sigma(\mathcal{L}(v)))^n = (\zeta \mathcal{L}(v))^n = \mathcal{L}(v)^n \implies \mathcal{L}(v) \in P.$$

в) В качестве базиса поля  $F$  над  $P$  можно взять  $(1, u, u^2, \dots, u^{n-1})$ .

Положим  $u_j = \sigma^j(u)$  и допустим на времена, что

$$\mathcal{L}(u^i) = u_0^i + \zeta^{-1} u_1^i + \dots + \zeta^{-(n-1)} u_{n-1}^i = 0$$

для  $i = 0, 1, \dots, n-1$ . В таком случае строки матрицы  $(u_j^i)$ ,  $0 \leq i < j \leq n-1$ , были бы линейно зависимы, а её определитель  $\det(u_j^i) = \prod_{k>l} (u_k - u_l)$  равнялся бы нулю. Но это не так, поскольку все элементы  $u_0, u_1, \dots, u_{n-1}$  попарно различны.

**5.6.2.** Действительно, предположим обратное. Тогда  $(g_1, \dots, g_m) \in S \implies (\sigma g_1, \dots, \sigma g_m) \in S$ . Так как  $G$  действует транзитивно на  $S$  внутренним сопряжением, то найдётся  $g \in G$ , для которого  $\sigma g_i = gg_i g^{-1} \forall i$ . Но  $\langle g_1, \dots, g_m \rangle = G$  и, следовательно,  $\sigma$  — внутренний автоморфизм, вопреки предположению.

**5.6.3.** Чтобы доказать сильную жёсткость указанных троек, проще всего вычислить мощность  $|\tilde{S}|$  в каждом случае, используя формулу (5) и известную нам таблицу неприводимых комплексных характеров

.	1A	2A	3A	5A	5B
$\chi_1$	1	1	1	1	1
$\chi_2$	3	-1	0	$\lambda$	$\lambda'$
$\chi_3$	3	-1	0	$\lambda'$	$\lambda$
$\chi_4$	4	1	-1	0	0
$\chi_5$	5	1	-1	0	0

Здесь  $\lambda = (1 + \sqrt{5})/2$ ,  $\lambda' = (1 - \sqrt{5})/2$ . Результат вычислений:

$$|\tilde{S}(2A, 3A, 5A)| = \frac{60^2}{4 \cdot 3 \cdot 5} (1 + 0 + 0 + 0 + 0) = 60,$$

$$|\tilde{S}(2A, 5A, 5B)| = \frac{60^2}{4 \cdot 5 \cdot 5} \left(1 + \frac{1}{3} + \frac{1}{3} + 0 + 0\right) = 60,$$

$$|\tilde{S}(3A, 5A, 5B)| = \frac{60^2}{(3 \cdot 5 \cdot 5)} \left(1 + 0 + 0 + \frac{1}{4} + 0\right) = 60.$$

Легко проверяется также, что любая тройка в  $\tilde{S}$  порождает  $A_5$ .

**5.6.4.** Очевидные замечания:  $K_1(z)$  — целое число, и поэтому  $\overline{K_1(z)} = K_1(z)$ ;  $K_1$  — центральная функция. Далее рассуждаем, как в тексте, т.е. по лемме Шура имеем равенство

$$\frac{1}{|G|} \sum_{x \in G} \Psi_i(xyx^{-1}) = \lambda_i E,$$

где  $\Psi_i$  — представление с характером  $\chi_i$ ,  $\lambda_i = \chi_i(y)/\chi_i(e)$ . Из уравнения

$$\frac{1}{|G|} \sum_{x \in G} \Psi_i(xyx^{-1}y^{-1}) = \lambda_i \Psi_i(y^{-1})$$

переходом к следу и последующим суммированием по  $y$  получаем, используя соотношения ортогональности,

$$\frac{1}{|G|} \sum_s^r K_1(g_s) |g_s^G| \chi_i(g_s) = \frac{1}{\chi_i(e)} \sum_y \chi_i(y) \overline{\chi_i(y)} = \frac{|G|}{\chi_i(e)}$$

( $g_s$  — представители классов сопряжённости, записываемые в виде коммутатора). Умножаем на  $\overline{\chi_i(z)}$  и суммируем по  $i$ :

$$\frac{1}{|G|} \sum_{s=1}^r K_1(g_s) |g_s^G| \sum_{i=1}^r \chi_i(g_s) \overline{\chi_i(z)} = |G| \sum_i \frac{\overline{\chi_i(z)}}{\chi_i(e)}.$$

Но в левой части равенства стоит  $K_1(z)$ , поскольку  $\sum_{i=1}^r \chi_i(g_s) \overline{\chi_i(z)} = 0$ , если  $g_s^G \neq z^G$  и  $|C(z)|$  в противном случае. Таким образом,

$$K_1(z) = \overline{K_1(z)} = |G| \sum_i \frac{\chi_i(z)}{\chi_i(e)}.$$

Теперь более или менее ясно, как получить выражение для  $K_m(z)$ .

# МЕТОДИЧЕСКИЕ ЗАМЕЧАНИЯ

---

Так как лекционных часов и семинарских занятий, отводимых на освоение изложенного в [ВА III] материала, слишком мало, то приходится ориентироваться на некий каркас, оснащая его по мере возможности разными деталями. Каркас, именуемый учебной программой, подвержен эволюции, вкусам лектора, а в целом отвечает уровню студенческой восприимчивости.

Рассказ о соответствии между линейными группами Ли и касательными к ним алгебрами Ли (гл. 2 § 4), опирающийся на материал из [ВА II, гл. 7 § 1] и в какой-то мере нужный геометрам (инициирован он по их просьбе), получился довольно схематичным из-за явного дефицита топологических сведений. Гораций был бы недоволен... (см. предисловие к [ВА I]). И всё-таки сопоставления типа “алгебра Ли  $\rightarrow$  группа Ли”, “многочлен  $\rightarrow$  его группа Галуа”, “произвольное ассоциативное кольцо  $\rightarrow$  модуль над этим кольцом” крайне полезны, поскольку они служат яркой иллюстрацией единства алгебры как большого раздела математики.

В условиях механико-математического факультета МГУ им. М.В. Ломоносова упомянутый выше каркас алгебры третьего семестра применялся несколько раз. Теория Галуа потихоньку отошла в область спецкурсов. Собственно, глава 5 и написана для одного из таких спецкурсов, причём рассчитанного на эффективное использование теории характеров.

## ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ (без теории характеров)

1. Разбиения на смежные классы и теорема Лагранжа.
2. Подгруппы циклической группы.
3. Конструкция факторгруппы и основная теорема о гомоморфизмах групп.
4. Первая теорема об изоморфизме.
5. Коммутант группы и теорема об абелевых факторгруппах.
6. Центр и теорема о факторгруппе по центру.
7. Понятие разрешимой группы. Разрешимость конечной  $p$ -группы,  $S_3$  и  $S_4$ .
8. Теорема о гомоморфном образе прямого произведения. Примеры.
9. Действия групп: стабилизаторы точек, длины орбит.
10. Действие сопряжением. Классы сопряжённости. Теорема о центре конечной  $p$ -группы.
11. Первая теорема Силова (существование).
12. Вторая теорема Силова (сопряжённость).
13. Простота группы  $A_5$ .
14. Простота группы  $SO(3)$ .

15. Конечно порождённая абелева группа без кручения свободна. Понятие ранга.
16. Теорема о существовании согласованных базисов свободной абелевой группы конечного ранга и её подгруппы.
17. Теорема о строении конечно порождённой абелевой группы как следствие теоремы о согласованных базисах.
18. Прямое доказательство теоремы о строении конечных абелевых  $p$ -групп.
19. Основная теорема о конечных абелевых группах: инвариантные множители, элементарные делители, примеры.
20. Эквивалентные множества матриц. Лемма Шура и её следствия.
21. Теорема о неприводимой матричной группе с конечным центром.
22. Теорема Машке о полной приводимости конечных матричных групп.
23. Матричное представление конечной группы над  $\mathbb{C}$ . Примеры.
24. Геометрический язык теории представлений. Примеры линейных представлений. Переход к матричным представлениям.
25. Каждая неабелева конечная группа имеет неприводимое представление степени  $> 1$  над любым полем нулевой характеристики.
26. Описание всех неприводимых комплексных представлений конечной абелевой группы. Теорема двойственности.
27. Теорема о числе одномерных комплексных представлений конечной группы.
28. Каждое комплексное представление конечной группы эквивалентно унитарному.
29. Действие линейной группы степени  $n$  на однородных формах от  $n$  переменных. Понятие об инвариантах линейной группы. Примеры.
30. Идеалы колец. Факторкольцо.
31. Основная теорема о гомоморфизмах для колец. Кольца главных идеалов.
32. Алгебры над полем: ассоциативные алгебры и алгебры Ли. Примеры. Гомоморфизмы алгебр.
33. Идеалы в алгебре многочленов. Простота матричной алгебры.
34. Гомоморфные образы алгебры многочленов. Поля алгебраических чисел.
35. Поле разложения многочлена. Примеры над  $\mathbb{Q}$  и над  $\mathbb{F}_p$ .
36. Существование конечного поля любого порядка  $q = p^n$ .
37. Единственность конечного поля заданного порядка.
38. Автоморфизмы конечного поля.
39. Алгебры с делением. Алгебра кватернионов.
40. Теорема Фробениуса.

ПРОГРАММА КУРСА ВЫСШЕЙ АЛГЕБРЫ  
(3-й семестр, 1995 г.)

1. Порядок элемента и порядок циклической группы. Изоморфизм циклических групп одинакового порядка. Полное описание подгрупп циклической группы.
  2. Разложение группы в объединение левых (правых) смежных классов по её подгруппе. Теорема Лагранжа и её следствия (2 часа).
  3. Нормальная подгруппа. Факторгруппа. Теоремы о гомоморфизмах и об изоморфизме. Прямые произведения групп (5 часов).
  4. Действия групп. Орбиты и стабилизаторы. Классы сопряжённых элементов и центр группы. Примеры:  $S_n$  и  $A_n$  (2 часа).
  5. Понятие простой группы. Простота  $A_n$ ,  $n > 4$ , и  $\mathrm{SO}(3)$  (2 часа).
  6. Теоремы Силова (2 часа).
  7. Свободные абелевы группы конечного ранга и их подгруппы. Периодические абелевы группы. Строение конечно порождённых абелевых групп (4 часа).
  8. Кольца, алгебры, факторалгебры. Присоединение корня многочлена к полю. Поле разложения многочлена. Конечные поля (5 часов).
  9. Алгебры с делением. Алгебра кватернионов. Теорема Фробениуса (2 часа).
  10. Линейные представления групп и алгебр. Инвариантные подпространства. Неприводимые и вполне приводимые представления. Матричная реализация. Теорема Машке. Представления конечных абелевых групп (3 часа).
  11. Модули. Лемма Шура. Теорема плотности. Структура простой конечномерной ассоциативной алгебры (3 часа).
  12. Линейные группы Ли. Классические группы. Алгебры Ли. Касательная алгебра Ли группы Ли. Экспоненциальное отображение (4 часа).
- Общее количество лекционных часов — 34 (на практике меньше). При необходимости часть лекционного материала переносится на семинарские занятия.

### ИЛЛЮСТРАТИВНЫЙ МАТЕРИАЛ К ТЕОРИИ ПРЕДСТАВЛЕНИЙ

Многое можно пояснить, не прибегая к теории характеров.

**Задача 1.** Требуется установить, что неприводимое комплексное представление  $(\Phi, V)$ ,  $\dim V = n > 1$ , симметрической группы

$$S_3 = \langle a, b \mid a^3 = e, b^2 = e, bab^{-1} = a^2 \rangle, \quad a = (123), \quad b = (12),$$

с точностью до эквивалентности единственно.

Положим  $\Phi(a) = \mathcal{A}$ ,  $\Phi(b) = \mathcal{B}$  и выберем в  $V$  базис, в котором  $B = \mathrm{diag}(-1, \dots, -1, 1, \dots, 1)$ . Так как  $Z(S_3) = e$ , то  $B$  имеет в качестве

собственных значений как  $-1$ , так и  $+1$ . Пусть  $\mathcal{B}v = v$ . Очевидно,  $\mathcal{A}v \neq v$ , поскольку  $n > 1$ , т.е.  $w = \mathcal{A}v - v \neq 0$ . С другой стороны,

$$(\mathcal{A}^2 + \mathcal{A} + \mathcal{E})w = (\mathcal{A}^2 + \mathcal{A} + \mathcal{E})(\mathcal{A} - \mathcal{E})v = (\mathcal{A}^3 - \mathcal{E})v = 0.$$

Утверждается, что  $\langle w, \mathcal{A}w \rangle$  —  $\Phi(G)$ -инвариантное подпространство (которое должно совпадать с  $V$  в силу неприводимости). Действительно,  $\mathcal{A}$ -инвариантность установлена. Далее,

$$\mathcal{B} \cdot \mathcal{A}w = \mathcal{B}(\mathcal{A}^2 - \mathcal{A})v = (\mathcal{A} - \mathcal{A}^2)\mathcal{B}v = (\mathcal{A} - \mathcal{A}^2)v = -\mathcal{A}w,$$

$$\mathcal{B}w = \mathcal{B}\mathcal{A}v - \mathcal{B}v = \mathcal{A}^2\mathcal{B}v - v = (\mathcal{A}^2 - \mathcal{E})v = (\mathcal{A} + \mathcal{E})w.$$

Значит, в базисе  $(w, \mathcal{A}w)$  имеем

$$A = \begin{vmatrix} 0 & -1 \\ 1 & -1 \end{vmatrix}, \quad B = \begin{vmatrix} 1 & 0 \\ 1 & -1 \end{vmatrix}.$$

Мы однозначно восстановили  $(\Phi, V)$ . В частности,  $n = 2$ .

**Задача 2.** Та же проблема для группы кватернионов: имеем точное неприводимое представление  $(\Phi, V)$  и операторы  $\mathcal{A}, \mathcal{B}$  на  $V$ , порождающие  $Q_8$  и связанные соотношениями

$$\mathcal{A}^4 = \mathcal{E}, \quad \mathcal{B}^2 = \mathcal{A}^2 = -\mathcal{E},$$

$$\mathcal{B}\mathcal{A}\mathcal{B}^{-1} = \mathcal{A}^{-1} = -\mathcal{A}.$$

Выбираем в  $V$  базис, относительно которого

$$B = \text{diag}(i, \dots, i, -i, \dots, -i).$$

Так как  $\Phi$  точное, то в качестве собственных значений выступают  $+i$  и  $-i$ . Пусть  $v$  — собственный вектор, для которого  $\mathcal{B}v = iv$ . Соотношения

$$\mathcal{A}^2v = -v, \quad \mathcal{B}(\mathcal{A}v) = -\mathcal{A}\mathcal{B}v = -i(\mathcal{A}v)$$

и неприводимость  $(\Phi, V)$  показывают, что  $V = \langle v, \mathcal{A}v \rangle$ , причём

$$A = \begin{vmatrix} 0 & -1 \\ 1 & 0 \end{vmatrix}, \quad B = \begin{vmatrix} i & 0 \\ 0 & -i \end{vmatrix}.$$

Представление однозначно восстановлено.

**Задача 3.** Знакопеременная группа  $A_4$  определяется заданием

$$A_4 = \langle a, b, c \mid a^2 = b^2 = (a, b) = e = c^3; \quad cac^{-1} = b, \quad cbc^{-1} = ab \rangle$$

Точность и неприводимость представления  $(\Phi, V)$  позволяют выбрать в  $V$  базис, относительно которого

$$C = \mathcal{F}_c = \text{diag}(1, \dots, \zeta, \dots, \zeta^{-1}).$$

Без ограничения общности выбираем  $0 \neq f \in V$ , для которого  $\mathcal{C}f = \zeta f$ ,  $\zeta \neq 1$ ,  $\zeta^3 = 1$ . Если  $\mathcal{A}f = f$ , то

$$\mathcal{B}f = \mathcal{C}\mathcal{A}\mathcal{C}^{-1}f = \mathcal{C}\mathcal{A}\zeta^{-1}f = f$$

— противоречие с неприводимостью  $\Phi$ . Значит,  $u = \mathcal{A}f - f \neq 0$ . Аналогично,  $v = \mathcal{B}f - f \neq 0$ ,  $w = \mathcal{B}\mathcal{A}f - f \neq 0$ . Имеем

$$\mathcal{C}\mathcal{A}f = \mathcal{C}\mathcal{A}\mathcal{C}^{-1}\mathcal{C}f = \mathcal{B}\zeta f = \zeta \mathcal{B}f,$$

$$\mathcal{CB}f = \mathcal{C}\mathcal{B}\mathcal{C}^{-1}\mathcal{C}f = \mathcal{A}\mathcal{B}\zeta f = \zeta\mathcal{A}\mathcal{B}f,$$

$$\mathcal{C}\mathcal{A}\mathcal{B}f = \mathcal{A}\mathcal{C}f = \zeta\mathcal{A}f.$$

Поэтому  $\mathcal{C}u = \zeta v$ ,  $\mathcal{C}v = \zeta w$ ,  $\mathcal{C}w = \zeta u$ . Далее,  $\mathcal{A}u = -u$ ,  $\mathcal{A}v = \mathcal{A}\mathcal{B}f - \mathcal{A}f = (\mathcal{A}\mathcal{B}f - f) - (\mathcal{A}f - f) = w - u$ ,  $\mathcal{A}w = \mathcal{B}f - \mathcal{A}f = v - u$ ,  $\mathcal{B}u = \mathcal{A}\mathcal{B}f - \mathcal{B}f = w - v$ ,  $\mathcal{B}v = -v$ ,  $\mathcal{B}w = \mathcal{A}f - \mathcal{B}f = u - v$ .

Получаем  $\dim V = 3$  и однозначно определённые матрицы

$$A = \begin{vmatrix} -1 & -1 & -1 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix}, \quad B = \begin{vmatrix} 0 & 0 & 1 \\ -1 & -1 & -1 \\ 1 & 0 & 0 \end{vmatrix}, \quad C = \begin{vmatrix} 0 & 0 & \zeta \\ \zeta & 0 & 0 \\ 0 & \zeta & 0 \end{vmatrix}.$$

# ПРЕДМЕТНЫЙ УКАЗАТЕЛЬ

- Автоморфизм регулярный 249  
Алгебра над полем 167  
— ассоциативная с делением 170,  
  172  
— конечная 173  
— градуированная 169  
— групповая 175  
— конечной группы 175, 177  
— кватернионов 15  
— обобщённых 183  
— Кэли 183  
— Ли 79, 184, 187  
— странная 249  
— группы Ли 79  
— над полем 168  
— центральная простая 169  
Аннулятор 161  
Антиавтоморфизм 16
- Базис абелевой группы 61  
— нормальный расширения Галуа  
  224, 227  
Башня расширений 190
- Вектор касательный 76  
— старший 186, 187  
Высота соотношения 62  
Вес вектора 186
- Группа абелева элементарная 73  
— внешних автоморфизмов 45  
— внутренних автоморфизмов 26  
— Галуа 207  
— движений пространства 30  
— дизэдра 43  
— заданная образующими и соот-  
ношениями 43
- Группа кватернионов 44  
— обобщённая 183  
— конечно определённая 43  
— Ли линейная 75  
— мультипликативная 15, 154  
— нильпотентная 49  
— полиномиальных автоморфиз-  
мов 250  
— преобразований 23  
— простая 50  
— просто приводимая 250  
— разрешимая 48  
— специальная линейная 10  
— ортогональная 10  
— свободная 42  
— свободная абелева 64  
— транзитивная 28  
— унитарная 10  
— характеров абелевой группы 121  
—  $U(Z_n)$  154, 158
- Группы бинарные 108  
— кристаллографические 127  
— правильных многогранников 105  
— просто приводимые 250
- Действие группы на множестве 26  
— сдвигом 27  
— сопряжением 26  
Действия эквивалентные 31  
Делители абелевой группы инва-  
риантные 71  
— элементарные 71  
Дифференциал гомоморфизма 179  
Дифференцирование алгебры Ли 82  
— произвольной алгебры 184  
Длина орбиты 25  
Длина слова 41

- Жёсткость набора** 230  
 — сильная 239  
 — рациональная 239
- Закон взаимности квадратичный** 159  
 — двойственности для конечных абелевых групп 125
- Задание группы** 43
- Задача Галуа обратная** 251
- Запись несократимая** 41
- Идеал кольца** 142
- Идеал максимальный** 148, 151
- Идеалы кольца многочленов** 144
- Идемпотенты групповой алгебры** 178
- Изоморфизм групп Ли** 74  
 — полей разложения 194  
 —  $G$ -пространств 88, 91
- Инварианты группы диэдра** 137  
 — группы  $S_n$  137, 138  
 — линейной группы 136, 140
- Инвариантное подмножество** при действии группы 31  
 — подпространство 88
- Инварианты конечной абелевой группы** 71
- Индекс подгруппы** 21
- Кватернионы** 15
- Класс нильпотентности** 49  
 — сопряжённых элементов 26
- Классификация простых групп** 248
- Классы вычетов по модулю идеала** 144
- Клетка жорданова** 89
- Кольцо гауссовых чисел** 150  
 — главных идеалов 151  
 — евклидово 150  
 — классов вычетов 143, 144  
 — локальное 150  
 — многочленов 153  
 — с делением 170  
 — факториальное 153  
 — характеров 133  
 — целых элементов 166  
 — эндоморфизмов 160
- Коммутант группы** 37
- Коммутатор элементов** 37
- Константы структурные** 178
- Кратность веса** 186  
 — вхождения 101  
 — полюса 103
- Кривые в матричных группах** 76  
 — дифференцируемые 76
- Кручение абелевой группы** 61, 64
- Лемма Артина** 208  
 — Дедекинда–Артина 219
- Логарифм** 81
- Матрица эрмитова** 96
- Матрицы перестановок** 46
- Многочлен гармонический** 128  
 — круговой 104, 212  
 — минимальный элемента 192  
 — неприводимый 196, 198  
 — сепарабельный 196
- Модуль** 159
- Монстр** 48, 252
- Независимость алгебраическая** 226
- Нормализатор подгруппы** 26
- Норма элемента расширения** 230
- Нули характеров** 181
- Образующие свободные** 41  
 — группы 43
- Ожерелье** 85
- Оператор линейный ортогональный** 96  
 — унитарный 96
- Орбита** 24
- Параметризация групп** 10
- Подгруппа борелевская** 52  
 — кручения 68  
 — Ли 75  
 — нормальная 19  
 — производная 37, 48  
 — сопряжённая 25  
 — стационарная 24  
 — унипотентная 52
- Подгруппы Силова** 55
- Подпредставление** 90

Подпространство дополнительное 90  
 — инвариантное 90  
 — устойчивое 90  
 Показатель группы 72  
 Поле разложения многочлена 146  
 Полюс вращения 103  
 Представитель смежного класса 19  
 Представление вполне приводимое 91, 99  
 — дуальное 131  
 — контрагredientное 131  
 — линейное 16  
 — неприводимое 91  
 — неразложимое 90  
 — регулярное 93  
 — точное 86  
 — тривиальное 90  
 — унитарное 96  
 Пересечение идеалов 148  
 Подмодуль 159  
 — без кручения 162  
 — конечного типа 165  
 — кручения 162  
 — периодический 161  
 — простой (неприводимый) 163  
 — над  $\mathfrak{sl}(2)$  184  
 — свободный 163  
 — циклический 161  
 Поле конечное 198  
 — круговое 204  
 — совершенное 196  
 — циклотомическое 204  
 Представление алгебры 170  
 Представления неприводимые 91  
 — абелевой группы 121  
 — группы  $A_4$  124  
 — группы  $A_5$  126  
 — кватернионов 125  
 — группы  $S_4$  124  
 — групп SU(2), SO(3) 127, 129  
 Проблема Бернсайда 249  
 Прогрессия арифметическая 228  
 Произведение групп прямое 39, 40  
 — полупрямое 40  
 Произведение идеалов 149  
 Произведение тензорное представлений 132  
 — пространств 132

Пространство евклидово 96  
 — касательное 77  
 — однородное 30  
 — представления 87  
 — эрмитово 96

**Р**азложение Брюа 53  
 Размерность алгебры 168  
 Разрешимость в радикалах 235, 236  
 Ранг свободной группы 41  
 Расслоение 30  
 Расширение полей алгебраическое 192  
 — — Галуа 209  
 — — нормальное 209  
 — — с абелевой группой Галуа 229  
 — вещественное 237, 238  
 — радикальное 235  
 — циклическое 231, 233  
 — — конечное 192  
 Рациональность класса 239  
 Ряд композиционный 54  
 — нижний центральный 49  
 — нормальный 54

**С**имвол Лежандра 158  
 След элемента расширения 230  
 Слово в алфавите 41  
 — пустое 41  
 Согласованность базисов 65  
 Соотношение минимальное 62  
 Соотношение ортогональности второе 121  
 — — первое 114  
 Соответствие Галуа 210, 211  
 Соотношения 41  
 Стабилизатор точки 24  
 Степень представления 86  
 — примитивного элемента 191  
 — прямая группы 40  
 — расширения поля 191  
 Ступень разрешимости 48  
 Сумма идеалов 148  
 — квадратов чисел 152  
 — прямая представлений 90

- Таблица характеров 120  
Тело 14, 170  
Теорема Артина 220  
— Артина–Шрайера 234  
— Белого–Томпсона 240  
— Бернсайда 177, 181  
— Брауера 135, 218  
— Веддербарна 173  
— Гильберта 231, 233  
— Дедекинда 219  
— Дирихле 228  
— китайская об остатках 155  
— Лагранжа 21  
— Машке 99  
— Фробениуса 172  
— Фробениус–Штикерльбергера 69  
— Шафаревича 251  
— Штайзера 231, 232  
— (лемма) Шура 109  
— Эйлера 156  
Теоремы Силова 55, 56  
Трисекция угла 214  
Триплет жёсткий 240
- У**двоение куба 214  
Углы Эйлера 11  
Удвоение алгебры 183  
Уравнение Лапласа 83
- Ф**акторалгебра 168  
Факторгруппа 32  
Факторкольцо 143  
Факторпредставление 90  
Факторы инвариантные 72  
— композиционные 54  
Функция центральная 113  
Функция Эйлера 203  
Форма эрмитова 96  
Формула обращения Мёбиуса 201,  
    203  
— Витта 207
- Х**арактер обобщённый 133  
— представления 111
- Ц**ентр группы 26
- Ч**асть периодическая группы 68
- Э**квивалентность представлений 87  
— топологическая 11, 14  
Экспонента группы 72  
Элемент кольца целый 166  
— примитивный расширения 190,  
    196  
Элементы сопряжённые 26

Учебное издание

*КОСТРИКИН Алексей Иванович*

**ВВЕДЕНИЕ В АЛГЕБРУ**

Часть III  
**ОСНОВНЫЕ СТРУКТУРЫ**

Редактор *E.Ю. Ходан*  
Оригинал-макет *H.H. Андреева*

ЛР № 071930 от 06.07.99. Подписано в печать 27.05.04.  
Формат 60×90/16. Бумага офсетная. Печать офсетная.  
Усл. печ. л. 17. Уч.-изд. л. 18,7. Заказ №

Издательская фирма «Физико-математическая литература»  
МАИК «Наука/Интерпериодика»  
117997, Москва, ул. Профсоюзная, 90  
E-mail: fizmat@maik.ru, fmlsale@maik.ru  
<http://www.fml.ru>

Отпечатано с готовых диапозитивов в ПФ «Полиграфист»  
160001, г. Вологда, ул. Челюскинцев, 3  
Тел.: (8172) 72-55-31, 72-61-75, факс: (8172) 72-60-72  
E-mail: form.pfp@votel.ru <http://www.vologda/~pfpv>